CAPÍTULO I

La mayoría de las ideas fundamentales de la ciencia son esencialmente sencillas y, por regla general pueden ser expresadas en un lenguaje comprensible para todos."

Albert Einstein

INFORMÁTICA FORENSE

1.1. ¿Qué es la informática forense?

1.2. Importancia de la informática forense

1.3. Objetivos de la informática forense

1.4. El proceso forense

1.5. Delitos informáticos

1.6. Tipificación de los delitos informáticos

1. INFORMÁTICA FORENSE

La tecnología ha avanzado rápidamente y con esta también la forma en que se opera los medios informáticos, ahora la información es almacenada de forma automática en la computadora, obviamente de forma muy diferente a como se almacenaba en épocas no muy lejanas, en papel, sin embargo esto nos conlleva a ciertas ventajas y desventajas.

La ventaja es que podemos tener un mejor manejo y disposición de la información, pero a su vez también se transforma en desventaja, en especial cuando la información es manipulada por personas no autorizadas.

Es aquí donde interviene la informática forense, que sirve para contrarrestar y detectar delitos a la información.

1.1. ¿QUÉ ES LA INFORMÁTICA FORENSE?

Hasta este punto es fácil imaginarse que la informática forense tiene que ver con los programas o aplicaciones que se utilizan en la medicina forense, pero en realidad de lo que se trata es de la investigación penal, con el fin de resolver problemas online.

Con el auge de las computadoras y la TI, la seguridad informática está cada vez más afectada, lo que ha favorecido de alguna manera la implementación de una serie de acciones que refuerzan la seguridad, sin embargo no han sido suficientes ya que los delincuentes informáticos encuentran nuevas formas para continuar con sus acciones.

La informática forense surgió o dio sus primeros pasos aproximadamente hace 25 años en Estados Unidos, cuando el FBI se dio cuenta que los criminales empezaron a usar la tecnología para cometer sus crímenes.

En 1984 el FBI inicio un programa llamado el Programa de Medios Magnéticos que dio origen al CART, un equipo de análisis computacional. En 1988 Michael Anderson un agente del IRS (servicio de rentas

internas), armó un grupo de especialistas y se reunieron con 3 compañías involucradas en la recuperación de datos, compañías que luego se convirtieron en Symantec.

En una de estas reuniones se crearon las clases de Especialistas de Recuperación de Evidencia Computacional, en 1988 y 1989 en el centro de entrenamiento federal FLETC, y también se creó la IACIS, Asociación Internacional de Especialistas en la Investigación Computacional.

Entre 1993 y 1995 junto con el Departamento de Hacienda de Canadá se formó el programa CIS para incluir a todas las agencias de la tesorería estadounidense en el entrenamiento. Al mismo tiempo se formó la IOCE[1], Organización Internacional en Evidencia Computacional, cuyo propósito es proveer un foro internacional para el intercambio de la información relacionada con la investigación computacional y la informática forense.

Para ese entonces la informática forense ya se había consolidado como un campo vital en el área de la investigación, y que a medida que la tecnología avanzaba de forma acelerada así tenían que hacerlo las organizaciones encargadas de la informática forense.

Para el 2003 el CART trabajaba en 6500 casos y estaba examinando 782 Terabytes de datos.

Actualmente las compañías de Software producen software forense más robusto y los agentes de la ley y militares entrenan a más personal para responder a los crímenes que involucren tecnología.

La informática forense está adquiriendo gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y al uso que se hace de la misma; la computadora y los sistemas informáticos son fundamentales dentro de esta sociedad moderna y por lo tanto favorecen al crecimiento de una organización.

[1]IOCE, INTERNATIONAL ORGANIZATION ON COMPUTER EVIDENCE: http://www.ioce.org

Lastimosamente estas mismas herramientas están siendo utilizadas para cometer delitos, pero igual que un crimen en la dimensión física deja evidencias, aquí también se deja evidencias del crimen, pero dichas evidencias quedan almacenadas de forma digital, en la mayoría de los casos dicha información no se puede leer o recolectar por medios comunes o mecanismos tradicionales. Es de aquí que nace el estudio de la informática forense, que provee el conocimiento y los instrumentos para estudiar y solucionar este nuevo tipo de delitos.

Incluso es posible resaltar su carácter científico, ya que tiene sus fundamentos en las leyes de la física, de la electricidad y del magnetismo, por ejemplo podemos destacar que es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer y recuperar aunque haya sido eliminada.

Si a todo esto se le aplica un método científico, con procedimientos estrictos, en donde se aplique la recolección, análisis y validación de todo tipo de pruebas digitales, puede fácilmente ayudar a resolver varios crímenes.

1.1.1. Orígenes

Con el auge de las computadoras y la TI, la cantidad de información ha crecido casi de forma exponencial, el mismo hecho de que ahora la información se almacena digitalmente cambia también la forma de obtener evidencia que luego servirá como pruebas para futuras investigaciones.

Es necesario obtener pruebas de manera eficiente y útil, debe aparecer el forense del mundo digital al igual que existe un forense en el mundo físico.

Es importante señalar que la informática forense no nace con el internet porque al inicio no existían las redes, se empieza investigando los virus informáticos en los años 90 con la técnica denominada ingeniería inversa que se puede decir es el inicio de la informática forense.

Pero con la apertura de las redes cambia la forma de delinquir, ya que la cantidad de redes interconectadas facilita los delitos informáticos, en este punto ya existen delitos que son propios solo de internet, muy brevemente se puede decir que en internet la gente miente, roba, falsifica, escucha, ataca, destruye y hasta organiza asesinatos y actos terroristas, un ejemplo muy cercano es el de la guerrilla colombiana.

La ciencia de la informática fue creada para cubrir todo este tipo de necesidades que se estaban presentando y para aprovechar al máximo este nuevo tipo de evidencia que se estaba generando constantemente.

En los años 90 las autoridades no eran capaces de cubrir todos los delitos que se estaban cometiendo a través de la TI, ya sea por falta de personal e infraestructura calificada para este tipo de trabajo.

Un ejemplo muy claro de esto son las estadísticas que muestra el FBI en este periodo sobre el número de intrusiones, casos cerrados y casos abiertos.

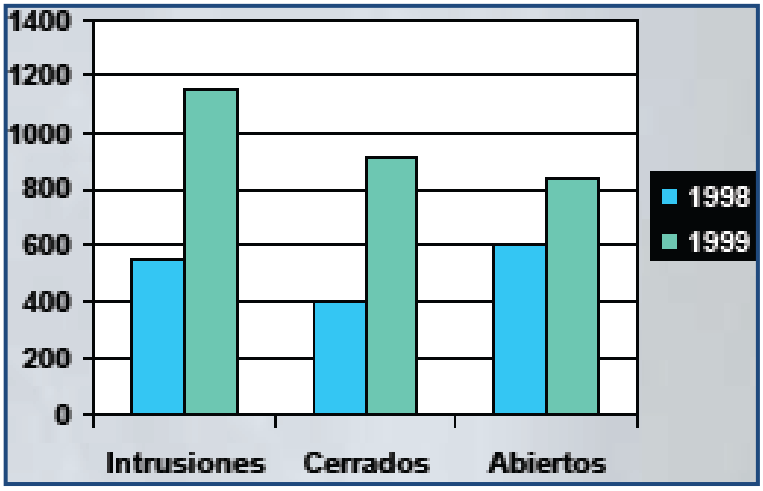

Figura 1.1. Intrusiones, casos cerrados y abiertos por el FBI

1.1.2. Situación actual de la Informática Forense

Las intrusiones en su mayoría no se detectan, o se detectan pero ya es demasiado tarde o simplemente no se quieren investigar.

La mayoría de investigaciones están relacionadas con:

- Pornografía infantil.
- Derechos de autor.
- Envío de información, mails perdidos.
- Acciones dañinas llevadas a cabo por empleados, ex empleados o personas externas.
- Solo en aquellos casos en que vale la pena la inversión se realiza una investigación forense, porque la investigación puede no llevar a nada concluyente, las conclusiones no llevan a la captura del delincuente o sencillamente este ya no se encuentra al alcance.

1.2. IMPORTANCIA DE LA INFORMÁTICA FORENSE

La informática forense se puede definir como una disciplina de las ciencias forenses que en la medida de lo posible procura hacer dos cosas fundamentales, descubrir e interpretar la información que se encuentra dentro de medios informáticos.

El valor de la información en nuestra sociedad y en las empresas es cada vez más importante para el desarrollo de la organización, partiendo de este aspecto, la importancia de la informática forense, sus usos y objetivos adquieren mayor trascendencia.

Un ejemplo muy claro de la informática forense se puede encontrar en los equipos de cómputo encontrados cuando el ejército Colombiano realizó el ataque al campamento de las FARC en territorio ecuatoriano, y en donde murió Raúl Reyes, demuestran la importancia de la información contenida en dichos equipos y que pueden desatar un escándalo político en toda Latinoamérica, siempre y cuando la información que se extraiga de los mencionados dispositivos se realice en base a técnicas forenses reconocidas a nivel mundial y con el debido protocolo de manejo de evidencia.

Si se aplicaron de forma correcta las técnicas de informática forense, la captura de información de los tres equipos encontrados puede estar

disponible para los equipos de informática forense de todos los países que puedan verse perjudicados.

Como podemos notar la evidencia que se obtenga es de gran importancia y de carácter criminalístico, puede ser copiada con exactitud y compartida para ser revisada por todo el mundo y de forma conjunta, por los especialistas de informática forense, de esta forma pueden dar sus resultados de manera abierta y sin ocultar nada.

Por tanto la informática forense nos puede contar en este caso la historia, la del comando guerrillero que fue atacado y abatido en otro país, contar una historia que ya no pueden contar los que fueron abatidos en dicho ataque. Se puede obtener información como, quien estuvo a cargo de los equipos, historial de manejo de los equipos, si tenían conexión satelital, información financiera, histórica, informativa, mediática, proyectos, planes a futuro, estructura organizativa, etc.

Por el contrario si la extracción de la información no fue obtenida con los procedimientos de informática forense, toda la información que se presente carecerá de valor y lógicamente su veracidad puede ser cuestionada.

Poco a poco los crímenes informáticos, su prevención y procesamiento se vuelven cada vez más importantes, la informática forense es muy importante, en este siglo y en cualquier fecha del mismo debido a que se ha abierto un mundo digital, donde es de gran importancia poder conducirse en ese mundo cibernético de tecnologías de información y comunicación para el desarrollo.

1.3. OBJETIVOS DE LA INFORMÁTICA FORENSE

La informática forense en estos tiempos digitales es muy importante, pero la importancia real proviene de sus objetivos, que son la recolección, comparación, análisis y evaluación de datos procedentes de cualquier medio informático, de tal forma que sea como prueba dentro de un tribunal de justicia.

La frase clave es “que pueda ser usado como prueba dentro de un tribunal de justicia”, es esencial tener en mente esta frase el momento que se comienza una investigación informática forense, ya que de esta forma se penalizará a los delincuentes en base a las regulaciones legales de cada país.

1.4. EL PROCESO FORENSE

Para que la investigación forense tenga validez es necesario que cumpla con ciertas normas y leyes, ya sea a nivel legal o corporativo. En este sentido la ciencia forense provee de ciertas metodologías básicas que contemplan el correcto manejo de la investigación y de la información.

A continuación se enuncian siete guías existentes a nivel mundial de mejores prácticas en computación forense.

1.4.1. RFC3227

El “RFC 3227: Guía Para Recolectar y Archivar Evidencia” (Guidelines for Evidence Collection and Archiving), escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal. Su estructura es:

a) Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.
b) El proceso de recolección: transparencia y pasos de recolección.
c) El proceso de archivo: la cadena de custodia y donde y como archivar.

1.4.2. Guía de la IOCE

La IOCE, publicó “Guía para las mejores prácticas en el examen forense de tecnología digital” (Guidelines for the best practices in the forensic examination of digital technology). El documento provee una serie de estándares, principios de calidad y aproximaciones para la detección prevención, recuperación, examinación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte.

Su estructura es:

a) Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo).
b) Determinación de los requisitos de examen del caso.
c) Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).
d) Prácticas aplicables al examen de la evidencia de digital.
e) Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación.
f) Priorización de la evidencia.
g) Examinar la evidencia: protocolos de análisis y expedientes de caso.
h) Evaluación e interpretación de la evidencia
i) Presentación de resultados (informe escrito).
j) Revisión del archivo del caso: Revisión técnica y revisión administrativa.
k) Presentación oral de la evidencia.
l) Procedimientos de seguridad y quejas.

De toda esta estructura se puede rescatar en general 4 fases principales:

1) Recolección de la evidencia sin alterarla o dañarla.
2) Autenticación de la evidencia recolectada para asegurar que es idéntica a la original.
3) Análisis de los datos sin modificarlos.
4) Reporte final.

A continuación se estudia cada una de estas etapas que básicamente explican el manejo de la evidencia en una investigación.

Figura 1.2. Metodología forense según IOCE

1.4.2.1. Fase 1. Recolección De La Evidencia

El principio básico de cualquier investigación forense es tratar de congelar la escena del crimen, esto con el fin de preservar la evidencia frente a variaciones posteriores.

Cualquiera se puede imaginar que esto se puede hacer con simplemente desconectar el cable de alimentación eléctrica de la computadora, pero con esto solo se asegura los datos del disco duro,

mientras que los datos de la memoria RAM se perderían por completo, al igual que los procesos en ejecución y las conexiones de red.

Esta pérdida puede ser o no aceptable dependiendo de las circunstancias que se presenten en cada ataque, pero si es el caso, apagar de esta forma la computadora antes de recolectar los datos volátiles que se había mencionado puede representar pérdida de evidencia vital para la investigación; adicionalmente que posiblemente desconectar el cable de alimentación eléctrica puede ocasionar algún daño en el hardware y perder incluso la evidencia del disco duro.

Frente a todo lo que se ha dicho, decidir si se deja corriendo el sistema, si se desconecta el cable de alimentación eléctrica o se apaga de forma normal es una de las decisiones más difíciles dentro de la informática forense. Cada caso es diferente y cada investigador debe tener la flexibilidad necesaria para poder adaptarse a cada caso y tomar la decisión más adecuada. Sea cualquiera la decisión que se tome, está debe documentarse detalladamente en cada una de sus acciones, ya que estos documentos pueden ayudar luego a explicar el tipo de ataque que se presentó en ese momento.

La recolección inicial de la evidencia debe hacerse de manera tal que no afecte los datos que se encuentran en el sistema original, este debe ser sin lugar a dudas el principio básico de toda investigación. Basándose en este principio existen dos alternativas: realizar toda la investigación sobre el dispositivo que se cree fue afectado, pero en modo de solo lectura; la segunda opción o alternativa es realizar una copia idéntica del dispositivo original, y realizar el estudio forense sobre esta copia de la evidencia original.

La segunda opción es la más aconsejable ya que tiene la ventaja de que se trabaja sobre una copia de respaldo como si fuese la evidencia original, igual aquí se puede trabajar en modo solo lectura, además de que ahora existen un sinnúmero de herramientas tanto de software como

de hardware que ayudan a sacar estas imágenes o copias con diferentes niveles de confiabilidad.

Algo importante de tomar en cuenta es la realización de una cadena de custodia adecuada, esto con el fin de proteger la evidencia cuando las personas tengan acceso a ella. Este proceso consiste en documentar donde se encuentra almacenada la evidencia, que persona se encuentra o estuvo a cargo de la evidencia, porque motivo y en que periodo de tiempo tuvo acceso. Con esto se disminuye la posibilidad de que alguien modifique la evidencia o plante evidencia que desvié el rumbo de la investigación.

1.4.2.2. Fase 2: Autenticación De La Evidencia

Los diferentes dispositivos de almacenamiento se deterioran muy lentamente, pero los datos que contienen los mencionados dispositivos pueden variar rápidamente y como consecuencia cambiará también su significado.

Por esto es que se hace difícil demostrar que la evidencia recolectada es la misma que dejo el atacante, la cadena de custodia es uno de los métodos que se puede utilizar para asegurar que ningún cambio accidental o deliberado ha sido introducido en la evidencia.

Una técnica criptográfica basada en software que permite caracterizar numéricamente y de forma universal un archivo y todos los datos de un disco duro son las denominadas funciones hash como MD5. Las funciones hash lo que hacen es calcular y almacenar el valor hash para cada archivo, permitiendo así comprobar que los datos con los que se está trabajando son idénticos a los originales.

1.4.2.3. Fase 3: Análisis

El proceso de análisis tiene como objetivo encontrar todos los datos que tengan un valor probativo en la investigación, y lo más importante que aporten información para poder reconstruir el incidente. El análisis puede realizarse sobre cualquier sistema operativo siempre y cuando se cumpla

la denominada regla de oro en el manejo de evidencia: en cualquier acción que se realice no se debe dañar la evidencia.

No existe una metodología exacta para realizar una reconstrucción de un ataque informático, en su lugar lo que se debe hacer es un razonamiento en el que se estudia cada pieza de evidencia disponible, para luego encontrar el vínculo entre cada una de estas piezas, se crean hipótesis acerca de cómo se creó la evidencia, y se realizan pruebas para confirmar o contradecir esta hipótesis. Con estos pasos o proceso se puede reconstruir el ataque de forma muy aproximada a lo que en realidad ocurrió. En la ciencia forense el investigador no puede estar totalmente seguro de lo que ocurrió en un ataque, ya que sólo posee una limitada cantidad de información. Por lo tanto, solo se puede presentar explicaciones posibles basadas en la limitada cantidad de información que brinda la evidencia.

Las piezas de evidencia digital contienen información relativa a las acciones del atacante en el sistema, dichas piezas se encuentran dispersas en todo el sistema y pueden ser de distinta índole, pueden ser archivos de configuración del sistema, archivos borrados del sistema de archivos pero aún presentes en la superficie del disco duro, bitácoras de ingresos y salidas del disco duro, muchas veces manipuladas para ocultar el ingreso del atacante, archivos ocultos en carpetas de usuario que pueden ser programas de tipo exploit[2], historiales de comandos ejecutados, procesos que se encuentren en ejecución dentro de la memoria del sistema, archivos personales de usuarios en ubicaciones propias para los archivos del sistema o en ubicaciones restringidas. La mayoría de los archivos que se ha mencionado deben examinarse con herramientas de software especiales, en especial archivos que ya fueron eliminados del sistema o que se encuentran en memoria.

Como se ha expuesto existe un gran volumen de información que debe ser analizada, por tanto se debe organizar la búsqueda de manera

[2]Término con el que se denomina en el entorno "hacker" a un método concreto de usar un error de algún programa (bug) para entrar en un sistema informático.

adecuada, siguiendo un orden y análisis. Primero recolectar y estudiar los datos contenidos en memoria, luego recuperar los archivos borrados, continuar con el estudio de los archivos de configuración, las bitácoras del sistema y los archivos de usuario. Dependiendo de la experiencia del investigador algunos de estos pasos o análisis se pueden hacer al mismo tiempo. Lo más importante dentro de todo esto es la documentación de cada acción que se haya tomado en la investigación, con el fin de poder explicar el proceso de análisis ante cualquier instancia en cualquier momento.

1.4.2.4. Fase 4: Reporte Final

Como se dijo en el párrafo final de la fase anterior es necesario documentar las acciones realizadas. Se debe mencionar cual es el software y el número de versión que se utilizó para el análisis y la recolección de la evidencia; así como los métodos que se usaron para dichas tareas y por qué se decidió proceder de una u otra forma. La decisión del investigador debe fundamentarse en sus conocimientos, habilidad, circunstancias del caso y lo más importante su papel de neutralidad dentro del caso.

El reporte final debe estar fundamentado con base en las notas que se hicieron a lo largo de todo el proceso investigativo, debe ser detallado de forma extensa pero siempre haciendo hincapié en lo que es relevante para la investigación; lo que sí es importante es que el documento debe especificar la ubicación lógica que ocupa cierta evidencia relevante dentro del documento, en el caso de datos borrados y recuperados, se debe especificar donde se encontraba exactamente, incluyendo información como el cilindro, cabeza y sector del dispositivo físico; por ejemplo se puede decir que el archivo se encontraba en el cilindro 8, cabeza 4 y sector 7 y por el contrario sería incorrecto decir que se encontraba en C:\ en el caso de ser un sistemas Windows.

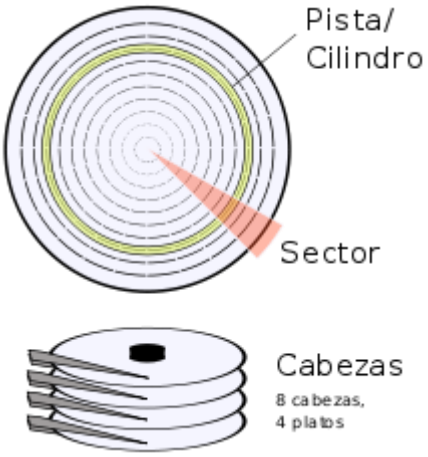

Figura 1.3. Cilindro, Cabeza y Sector

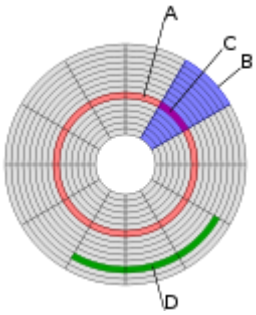

Figura 1.4. Pista (A), Sector (B), Sector de una pista (C), Clúster (D)

1.4.3. Investigación en la Escena del Crimen Electrónico

El Departamento de Justicia de los Estados Unidos de América, publicó “Investigación En La Escena Del Crimen Electrónico” (Electronic Crime Scene Investigation: A Guide for First Responders). Esta guía se enfoca más que todo en identificación y recolección de evidencia. Su estructura es:

a) Dispositivos electrónicos (tipos de dispositivos que pueden encontrar y cuál puede ser la posible evidencia).
b) Herramientas para investigar y equipo.
c) Asegurar y evaluar la escena.
d) Documentar la escena.
e) Recolección de evidencia.
f) Empaque, transporte y almacenamiento de la evidencia.
g) Examen forense y clasificación de delitos.

h) Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

1.4.4. Examen Forense de Evidencia Digital

Otra guía del Departamento de Justicia de los Estados Unidos, es "Examen Forense de Evidencia Digital" (Forensic Examination of Digital Evidence: A Guide for Law Enforcement). Esta guía está pensada para ser usada en el momento de examinar la evidencia digital. Su estructura es:

Desarrollar políticas y procedimientos con el fin de darle un buen trato a la evidencia.

a) Determinar el curso de la evidencia a partir del alcance del caso.
b) Adquirir la evidencia.
c) Examinar la evidencia.
d) Documentación y reportes.
e) Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).

1.4.5. Computación Forense - Parte 2: Mejores Prácticas (Guía Hong Kong)

El ISFS, Information Security and Forensic Society (Sociedad de Seguridad Informática y Forense) creada en Hong Kong, publicó "Computación Forense - Parte 2: Mejores Prácticas" (Computer Forensics – Part 2: Best Practices). Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la corte. Su estructura es:

a) Introducción a la computación forense.
b) Calidad en la computación forense.
c) Evidencia digital.
d) Recolección de Evidencia.
e) Consideraciones legales (orientado a la legislación de Hong Kong).

f) Anexos.

1.4.6. Guía de buenas prácticas para Evidencia basada en Computadores (Guía Reino Unido)

La ACPO, Association of Chief Police Officers (Asociación de Jefes de Policía), del Reino Unido, mediante su departamento de crimen por computador, publicó “Guía de Buenas Prácticas para Evidencia basada en Computadores” (Good Practice Guide For Computer Based Evidence). La policía creó este documento con el fin de ser usado por sus miembros como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia. Su estructura es:

a) Los principios de la evidencia basada en computadores.
b) Oficiales atendiendo a la escena.
c) Oficiales investigadores.
d) Personal para la recuperación de evidencia basada en computadores.
e) Testigos de consulta externos.
f) Anexos (legislación relevante, glosario y formatos)

1.4.7. Guía para el Manejo de Evidencia en IT (Guía Australia)

Estándares de Australia (Standards Australia) publico en agosto de 2003 “*Guía Para El Manejo De Evidencia En IT*” (HB171:2003 *Handbook Guidelines for the management of IT evidence*). Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital.

Detalla el ciclo de administración de evidencia de la siguiente forma:

a) Diseño de la evidencia.
b) Producción de la evidencia.
c) Recolección de la evidencia.

d) Análisis de la evidencia.
e) Reporte y presentación.
f) Determinación de la relevancia de la evidencia.

1.5. DELITOS INFORMÁTICOS

Es obvio que la informática tiene una gran influencia sobre la vida diaria de las personas y de las organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las comunicaciones, transacciones comerciales, educación, investigación, salud, defensa nacional, etc., son solo algunos aspectos que dependen cada día más de la tecnología y como se desarrolla ésta.

Pero junto al avance de la tecnología y su estrecho vínculo con las áreas sociales, también ha surgido una serie de ilícitos denominados delitos informáticos.

No hay una definición universal para delito informático pero varios han sido los autores que han intentado conceptualizarlo en base a las realidades de sus propios países.

"Delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático" (departamento de investigación de la Universidad de México, 2002).

El tratadista penal italiano Carlos Sarzana, en su obra Criminalitá e tecnología, dice "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

Nidia Callegari, especialista en derecho informático, mexicana, define el delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

María de la Luz Lima dice que el delito electrónico "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización

hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

El doctor Rodolfo Herrera Bravo en la ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile en agosto de 1998, sostiene que delito informático es "toda acción típica antijurídica dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software, de un sistema de tratamiento automatizado de la información".

Según el mexicano Téllez Valdez, “un delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, estafa, fraude, falsificación, sabotaje, pero siempre que involucre la informática como medio para realizar la ilegalidad”.

El mismo Julio Téllez Valdez[3] menciona que los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco, en tanto que solo determinadas personas con ciertos conocimientos pueden llegar a cometerlas.
- Son acciones ocupacionales en cuanto a que muchas veces se realizan cuando el sujeto está trabajando.
- Son acciones de oportunidad ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas ya que casi siempre producen beneficios de más de cinco cifras a aquellos que las realizan.

[3]TÉLLEZ VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996 Pág. 103-104

- Ofrecen posibilidades de tiempo y espacio ya que en milésimas de segundo y sin una presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la falta de regulación.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Tienden a proliferar cada vez más, por lo que requieren de una urgente regulación.

Julio Téllez Valdez clasifica a los delitos informáticos en base a dos criterios:

1. Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

   Ejemplos:

   - Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, etc.
   - Variación de la situación contable.
   - Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
   - Alteración del funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, etc.
   - Intervención de líneas de comunicación de datos o teleprocesos.
2. Como fin u objetivo: se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

Ejemplos:

- Instrucciones que producen un bloqueo parcial o total del sistema.
- Destrucción de programas por cualquier método.
- Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.
- Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.

María Luz Lima en su libro delitos electrónicos publicado en 1984, presenta la siguiente clasificación de delitos electrónicos:

- Como Método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
- Como Medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
- Como Fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

1.6. TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS

Las Naciones Unidas reconocen los delitos informáticos de la siguiente manera:

Fraudes cometidos mediante manipulación de computadoras	
Delitos	**Características**
Manipulación de los datos de entrada	Este tipo de fraude informático conocido también como sustracción de datos, 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.
La manipulación de programas	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.
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 a partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y

	de las tarjetas de crédito.
Fraude efectuado por manipulación informática	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.

Tabla 1.1. Fraudes mediante computadoras

Falsificaciones Informáticas	
Delitos	**Características**
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 a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias 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.

Tabla 1.2. Falsificaciones informáticas

Daños o modificaciones de programas o datos computarizados	
Delitos	**Características**
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o

	modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.
Acceso no autorizado a Sistemas o Servicios	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático.
Piratas informáticos o Hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden

	emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
Reproducción no autorizada de programas informáticos de protección Legal.	Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Tabla 1.3. Daños o modificaciones de programas o datos computarizados

Ahora bien, pocos son los países que disponen de una legislación adecuada que permita enfrentarse a los delitos mencionados, entre ellos tenemos a los siguientes:

- Alemania: A partir del 1 de agosto de 1986, adoptó la Segunda Ley contra la Criminalidad Económica.
- Austria: Ley de reforma del Código Penal del 22 de diciembre de 1987.
- Francia: La Ley 88/19 del 5 de enero de 1988 sobre el fraude informático.

- Estados Unidos: en 1994 modificó el Acta de Fraude y Abuso Computacional que se había creado en 1986, para crear el Acta Federal de Abuso Computacional.

1.6.1. Legislación Ecuatoriana

En el caso de la legislación Ecuatoriana en abril del 2002 y luego de largas discusiones por parte de los honorables diputados, fue aprobada la Ley de Comercio Electrónico, Mensaje 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, Capítulo III 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 se concluye que el dueño de la acción penal y de la investigación tanto pre-procesal 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 contará 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 del Ministerio Público, en tal virtud cualquier resultado de dichas investigaciones se incorporarán en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudarán posteriormente al representante del Ministerio Público a emitir su dictamen correspondiente.

Ahora 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 auxiliará 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 sus Jueces y Magistrados 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 incluir 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.

1.7. BIBLIOGRAFÍA

[1] Computación forense, análisis de "cadáveres" virtuales**.** Tomado de: http://cxo-community.com.ar/index.php ?option=com_content& task= view&id=291&Itemid=45

[2] Herramientas para computación forense control y adquisición de evidencia digital. Tomado de: http://www.mono grafias.com/trabajos 74/herramientas-computacion-forense-control-digital/herramientas-computacion-forense-control-digital.shtml

[3] Cyber Investigations (FBI). Tomado de: http://www.fbi.gov/cyberin vest/cyberhome.htm

[4] Objetivos de la informática forense. Tomado de: http://www. informaticaforense.com/criminalistica/faqs/general/cuales-son-los-objetivos-de-la-informatica-forense.html

[5] RFC 3227 Traducción al español. Tomado de: http://www.normes-internet.com/normes.php?rfc=rfc3227&lang=es

[6] Cano Martínez Jeimy José. (2006) Buenas prácticas en la administración de la evidencia digital. Tomado de: http://gecti. uniandes.edu.co/docs/doc_gecti_7_06.pdf

[7] Michael G. Noblett, Recovering and Examining Computer Forensic Evidence. Tomado de: http://www.fbi.gov/hq/lab/fsc/backissu /oct2000 /computer.htm

[8] Scientific Working Group on Digital Evidence: Standards and Principles. Tomado de: http://www.fbi.gov/hq/lab/fsc/backissu/ april2000/swgde.htm

[9] Handbook Guidelines for the management of IT evidence. Tomado de: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

[10] IOCE, Guidelines for the best practices in the forensic examination of digital technology. Tomado de: http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html

[11] INFORMATION SECURITY AND FORENSICS. Computer forensics.Part2: Best Practices. Tomado de: http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf

[12] DELITOS Y TECNOLOGÍA DE LA INFORMACIÓN. Tomado de: http://www.delitosinformaticos.com/delitos/delitosinformaticos2.shtml

[13] CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS. Tomado de: http://www.angelfire.com/la/LegislaDir/Carac.html

[14] Acurio del Pino, Delitos informáticos. Tomado de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf