UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

EL PERITAJE INFORMÁTICO COMO MEDIO DE PRUEBA EN EL DELITO DE PROGRAMAS DESTRUCTIVOS, REGULADO EN EL CÓDIGO PENAL

XILONÉ AYESTAS GALO

GUATEMALA, JULIO DE 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

EL PERITAJE INFORMÁTICO COMO MEDIO DE PRUEBA EN EL DELITO DE PROGRAMAS DESTRUCTIVOS, REGULADO EN EL CÓDIGO PENAL

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

XILONÉ AYESTAS GALO

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, julio de 2016

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	Lic.	Gustavo Bonilla
VOCAL I:	Lic.	Luis Rodolfo Polanco Gil
VOCAL II:	Licda.	Rosario Gil Pérez
VOCAL III:	Lic.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Jhonathan Josué Mayorga Urrutia
VOCAL V:	Br.	Freddy Noé Orellana Orellana
SECRETARIO:	Lic.	Fernando Antonio Chacón Urizar

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis" (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C. A.

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 21 de octubre de 2015.

Atentamente pase al (a) Profesional, **OTTO RENE ARENAS HERNÁNDEZ**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **XILONÉ AYESTAS GALO**, con carné **200119043**, intitulado **EL PERITAJE INFORMÁTICO COMO MEDIO DE PRUEBA EN EL DELITO DE PROGRAMAS DESTRUCTIVOS, REGULADO EN EL CÓDIGO PENAL.**

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

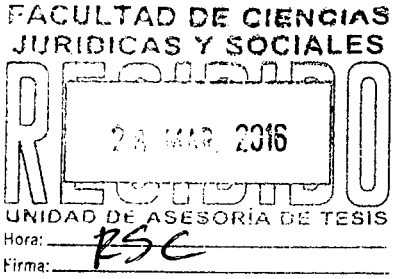
DR. BONERGE AMILCAR MEJÍA ORELLANA
Jefe(a) de la Unidad de Asesoría de Tesis

Fecha de recepción 15 / 01 / 2,016. f)

Asesor(a)
(Firma y Sello)
LIC. OTTO RENE ARENAS HERNÁNDEZ
ABOGADO Y NOTARIO

Lic. Otto René Arenas Hernández
Abogado y Notario
9 Av. 13-39 zona 1
Teléfono: 54120813
Guatemala C.A.

Guatemala 5 de febrero de 2016



Doctor
Bonerge Amilcar Mejía Orellana
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

Distinguido Doctor Mejía Orellana:

De conformidad con el oficio emitido por la Unidad de Asesoría, me permito manifestarle que en la calidad de asesor de tesis de la estudiante **XILONÉ AYESTAS GALO** quien desarrollo el tema intitulado, **"EL PERITAJE INFORMÁTICO COMO MEDIO DE PRUEBA EN EL DELITO DE PROGRAMAS DESTRUCTIVOS, REGULADO EN EL CÓDIGO PENAL".** Al respecto le manifiesto lo siguiente:

a) De la revisión practicada al trabajo de tesis relacionado, se puede establecer que el mismo cumple con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, relativos al contenido científico y técnico de la tesis en virtud, asimismo, que el presente trabajo llena las expectativas por dicho normativo, al haberse empleado dichos lineamientos al desarrollarse la investigación del caso

b) En este trabajo de investigación científica se utilizó el método deductivo, que en virtud del análisis de los hechos que aparecen en la investigación se originaron argumentos sobre las observaciones efectuadas que llegaron a conclusiones particulares. Asimismo, se utilizó el método histórico, pues en la investigación se analizaron situaciones pasadas y acontecimientos históricos que son parte del tema. Se utilizaron técnicas bibliográficas, citas textuales y de paráfrasis, que ayudaron a plasmar el marco teórico. En definitiva el trabajo de tesis se ajusta a los requerimientos científicos y técnicos que se deben cumplir de conformidad con la norma respectiva, la metodología y técnicas de investigación utilizadas.

c) Se observó que en toda la tesis se emplearon técnicas de redacción, ortografía y gramática adecuadas para este tipo de trabajos, así como de fondo y forma según lo establecido por la Real Academia de la Lengua Española.

Lic. Otto René Arenas Hernández
Abogado y Notario
9 Av. 13-39 zona 1
Teléfono: 54120813
Guatemala C.A.

d) La Contribución Científica lo constituye el proyecto de reforma al Reglamento de Organización y Funcionamiento del INACIF con el objeto de implementarse los protocolos y personal capacitado para el procesamiento, levantamiento y análisis de evidencia para el combate de los programas destructivos que les permita combatir este tipo de delincuencia.

e) En la conclusión discursiva se puede establecer que el estudiante realizó hallazgos dentro de la investigación, mismos que a mi consideración y criterio son adecuados y oportunos para el contexto en el que se desarrolló la misma, y del mismo modo, la conclusión discursiva de dicho trabajo son congruentes con el trabajo final realizado.

f) En la bibliografía utilizada se constató que en el desarrollo y culminación del informe final de la tesis, se utilizó doctrina de autores nacionales y extranjeros, así como haber realizado análisis tanto de la legislación interna como de legislación de otros países, lo cual, a mi criterio, es totalmente adecuado.

En conclusión y en virtud de haberse cumplido con las exigencias del suscrito asesor, derivadas del examen del trabajo en los términos anteriormente expuestos e individualizados y por las razones expresadas, así como haber cumplido con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, resulta procedente aprobar el trabajo de tesis relacionado, realizado por la estudiante **XILONÉ AYESTAS GALO**, y en consideración, conferirse la opinión que merece, debiendo continuar su trámite administrativo legal correspondiente a efecto se emita orden de impresión y se señale día y hora para la discusión en el correspondiente examen público, así también **DECLARO** que no tengo parentesco dentro de los grados de ley con el estudiante. En tal virtud, emito **DICTAMEN FAVORABLE** aprobando el trabajo de tesis asesorado.

Atentamente.

Lic. Otto René Arenas Hernández
Abogado y Notario
Colegiado 3805

LIC. OTTO RENE ARENAS HERNANDEZ
ABOGADO Y NOTARIO

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 02 de junio de 2016.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante XILONÉ AYESTAS GALO, titulado EL PERITAJE INFORMÁTICO COMO MEDIO DE PRUEBA EN EL DELITO DE PROGRAMAS DESTRUCTIVOS, REGULADO EN EL CÓDIGO PENAL. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

WELM/srrs.

Lic Daniel Mauricio Tejeda Ayestas
Secretario Académico

Lic. Avidán Ortíz Orellana
DECANO

DEDICATORIA

A DIOS: Por la vida y por la existencia misma, por darme las fuerzas y para seguir adelante para hacer este sueño realidad.

A MI MADRE: Por su incalculable amor y sacrificio, por sentar en mi las bases de la responsabilidad y deseos de superación, por enseñarme que nada es imposible y por creer en mis triunfos los cuales le dedico.

A: La Tricentenaria Universidad de San Carlos de Guatemala.

A: La Facultad de Ciencias Jurídicas y Sociales, por el honor y gran orgullo de ser egresado de tan prestigiosa casa de estudios la cual me formó académicamente haciendo de mi un nuevo profesional apasionado por el derecho.

PRESENTACIÓN

Esta investigación se refiere peritaje informático como medio de prueba en el delito de programas destructivos, regulado en el Código Penal, para ello se tomó como base el periodo histórico comprendido de los años 2010 a 2014, siendo esta una investigación cualitativa.

Se analizaron las causas que impiden que actualmente el Ministerio Público investigue correctamente los delitos informáticos en Guatemala especialmente el delito de programas destructivos, el cual debe estar orientado en función de una correcta actuación en relación a su investigación, en la obtención de los diferentes medios de prueba que el INACIF como ente que se encarga de la prueba cientifica aporte.

El enfoque con el que se desarrolló la investigación fue eminentemente jurídico-penal, en cuanto a que el Ministerio Público en el ejercicio de la acción penal pierde valiosos medios de investigacion y prueba, ya que el INACIF no presta servicios de informatica forense como medio de prueba en el proceso penal. El aporte del presente trabajo será el fortalecimiento del trabajo de investigación realizado por el Ministerio Público, mediante la puesta en marcha del laboratorio de informática forense, para la obtención de medios de prueba válidos y fehacientes en la investigación del delito de programas destructivos, regulado en el Código Penal, siendo la prueba pilar fundamental de la justicia como unica instancia para la consolidación del Estado de derecho.

COMPROBACIÓN DE LA HIPÓTESIS

Se comprobó la hipótesis a través del método inductivo, debido que el Ministerio Público para poder realizar su labor debe de contar con herramientas científicas que le ayuden a resolver los casos que se le presentan a través de la prueba científica que garantiza la Constitución Política de la República de Guatemala, en la legislación guatemalteca. El INACIF no cuenta con el laboratorio de informática forense, quedando en resumidas cuentas, el Ministerio Público sin herramientas para resolver los hechos delictivos, para ello se recolecto material bibliográfico referente a la prueba científica y el laboratorio informática forense.

Por lo anterior, es importante implementar el laboratorio de informática forense, los protocolos y personal capacitado para el procesamiento, levantamiento y análisis de evidencia para el combate de los programas destructivos que les permita combatir este tipo de delincuencia, comprobando la hipótesis planteada.

ÍNDICE

Pág.

CAPÍTULO IV

INTRODUCCIÓN

El propósito de realizar la presente investigación, fue efectuar un análisis doctrinario, legal, y practico relativo a la necesidad de crear un acuerdo del Consejo Directivo del Instituto Nacional de Ciencias Forenses de Guatemala, que implemente el laboratorio de informática forense y aplicación del protocolo de recolección, preservación, manejo y análisis de la evidencia digital para combatir el delito de programas destructivos y así garantizar el acceso a la justicia a través de la prueba pericial.

El Instituto Nacional de Ciencias Forenses es la única institución que presta el servicio forense, lamentablemente a la fecha no se ha implementado el laboratorio de informática forense. La hipótesis fue comprobada, ya que con la creación del acuerdo del Consejo del Instituto Nacional de Ciencias Forenses, que regula el laboratorio de informática forense y el protocolo de recolección, preservación, manejo y análisis de la evidencia digital; se garantiza el acceso a la justicia a través del servicio forense que presta la institución. Los objetivos fueron alcanzados, al determinar la importancia de que exista un acuerdo del Consejo Directivo el cual debe crear el protocolo para el manejo de evidencia digital.

La tesis se dividió en cuatro capítulos: el primer capítulo, se señaló lo que es la evidencia, definición, evidencia digital, escena del crimen de la evidencia digital, indicios, cadena de custodia; el segundo capítulo, se refiera a la informática forense, definición, validez jurídica de la evidencia digital, programas destructivos, virus, clases de virus; el tercer capítulo se desarrollaron conceptos tales como delitos informáticos, naturaleza y objeto, delito programas destructivos, elementos del delito de programas destructivos, sujeto activo, sujeto pasivo; el cuarto capítulo se refiere a las instituciones que participan en la obtención del peritaje informático, Ministerio Público, Instituto Nacional de Ciencias Forenses de Guatemala, peritaje informático como medio de prueba en el delito de programas destructivos, regulado en el Código Penal, legislación comparada, proyecto de creación del protocolo para el análisis de evidencia informática.

Los métodos utilizados fueron: El analítico, el inductivo, con el cual se obtuvieron propiedades generales a partir de las propiedades singulares, enfocando el tema de manera particularizada o individual, tanto en aspectos doctrinarios, como legales y prácticos, para poder concluir en razonamientos generalizados relacionados la legislación guatemalteca para la creación del laboratorio de informática forenses y del protocolo de recolección, preservación, manejo y análisis de la evidencia digital a través de un acuerdo del Consejo Directivo del Instituto Nacional de Ciencias Forenses de Guatemala. Y por último el deductivo. Las técnicas utilizadas son: La bibliográfica, en la cual se obtuvo material bibliográfico y documental en cuanto a la prestación del servicio forense, utilizando para esto leyes, textos, documentos, diccionarios jurídicos, enciclopedias; técnica de fichas, se procedió a tabular los datos obtenidos de la investigación en fichas para su posterior transcripción al trabajo final.

Es de vital importancia que exista un acuerdo del Consejo Directivo del Instituto Nacional de Ciencias Forenses de Guatemala, que implemente el laboratorio de informática forense y del protocolo de recolección, preservación, manejo y análisis de la evidencia digital como método idóneo de investigación del Ministerio Público para el esclarecimiento de los delitos informáticos.

CAPÍTULO I

1. La evidencia

Evidencia física, indicio o material sensible significativo, denominado a todo objeto, huella o elemento íntimamente relacionado con un presunto hecho delictuoso, cuyo estudio permite reconstruirlo, identificar a su autor y establecer su comisión.

1.1. Definición

Evidencia: "Viene del latín evidente. Certeza clara, manifiesta de una cosa: la evidencia es un axioma (principio o sentencia tan claro que no necesita explicación)".[1]

"Es la que puede ser encontrada tanto en el lugar de los hechos y en el cuerpo de la víctima o del victimario, como en las áreas relacionadas, ya sean próximas o distantes".[2]

"Elemento físico que se recauda como consecuencia de un acto delictivo los cuales pueden servir de evidencia para esclarecer los hechos de una investigación".[3] "La evidencia tiene forma, se puede ver, tocar, oler, pesar, medir; es tangible".[4]

---

[1] Diccionario ilustrado. **Pequeño Larousse.** Pág. 573.
[2] Moreno González, L. Rafael. **Introducción a la criminalística.** Pág. 67.
[3] **Manual de Procedimientos del Sistema de cadena de custodia.** Pág. 41.
[4] Benítez, Mendizábal, Arkel. **La escena del crimen.** Pág. 39.

La evidencia física, está determinada por la utilidad en la verificación de que un crimen ha sido cometido, identificando a la persona o personas que lo cometieron, y exonerando a toda otra persona que pueda estar bajo sospecha. Evidencia es todo indicio que una vez analizado se comprueba que pertenece al hecho presuntamente delictivo.

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 evidencias 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 lo tanto el rol que cumpla el sistema informático determinara donde debe ser ubicada y como deber 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. Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de 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, programas almacenados y mensajes de datos transmitidos usando el sistema informático.

1.2. Evidencia digital

La evidencia digital se constituye en todos aquellos datos e información histórica y presente almacenada en archivos lógicos para que se pueda procesar mediante algoritmos abiertos y auditables, con la finalidad de ser expuestos de manera muy sencilla ante los tribunales de justicia, siendo la evidencia digital el conjunto de datos en formato binario, esto se comprende en los archivos, su contenido o referencias a éstos, que se encuentren en los soportes físicos o lógicos de un sistema comprometido por un incidente informático.

En relación a la información que es encontrada en los dispositivos de almacenamiento o en las piezas de almacenamiento de 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 o memoria solida (como las memorias flash y dispositivos *usb*) y los dispositivos ópticos (como los discos compactos y *dvd*).

Como se ha mencionado anteriormente la evidencia digital se puede encontrar en una gran cantidad de dispositivos, tales como computadoras de escritorio, computadoras personales, *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 podemos encontrar evidencia digital, en datos que no están organizados como archivos sino que 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 quedar almacenados temporalmente en los archivos de intercambio o en la misma memoria *ram*.

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.

Es importante mencionar que este tipo de evidencias deben ser recuperadas casi de inmediato. La información residente en los medios de almacenamiento electrónico puede ser borrada, cambiada o eliminada sin dejar rastro, lo cual limita la labor del investigador forense para identificar y encontrar elementos claves para esclarecer los hechos relevantes de una investigación.

De esto 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.

Aquí se presenta 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 criminalísticos comunes, se debe utilizar mecanismos diferentes a los tradicionales.

Es aquí donde radica la necesidad de utilizar los procedimientos técnicos legales y la rigurosidad científica que pone a disposición de los investigadores la informática forense a fin de descubrir a los autores y cómplices del delito informático cometido bajo cualquier circunstancia.

Como consecuencia la falta de información especializada en esta área de investigación científica, la inexistente práctica y capacitación en la obtención, recolección, documentación y posterior análisis e interpretación de la evidencia digital, pueden dar como resultado una sentencia condenatoria contra un inocente y se deje libre a un culpable, situación que no puede permitirse en un proceso penal, es por tanto

necesarios que los entes encargados de la investigación, es decir el Ministerio Publico, la Policía Nacional Civil tengan conocimiento profundo en la materia, además deben de estar preparados para afrontar el reto de capacitar y entrenar al personal necesario para que combatan de forma óptima no solo los delitos informáticos sino también con otra clase de delitos, aprovechando así las ventajas de utilizar la informática forense y la evidencia digital dentro de los procesos penales, así mismo los jueces al momento de dictar sus resoluciones deben tomar en cuenta la informática jurídica ya que es un área que está en constante cambio y crecimiento.

1.3. Escena del crimen de la evidencia digital

Es el espacio abierto o cerrado, de mueble o inmueble, donde se ha cometido una presunta conducta punible, cuyo análisis o inspección además comprende sus alrededores, pues en la periferia generalmente se encuentran elementos materiales probatorios o evidencias físicas.

Es el lugar donde los hechos sujetos a investigación fueron cometidos, los rastros y restos que quedan en la víctima y victimario y en algunos casos en personas (testigos, cómplices, encubridores, coautores o cualquier otra persona) presenciales de los hechos u omisiones.

La escena del crimen es el lugar donde ha ocurrido un hecho con características de delito y que requiere de una investigación criminalística para su esclarecimiento.

Por lo que se comprende que la escena del crimen es el lugar donde ocurrió un hecho ilícito, y que es necesaria la intervención de investigadores para la búsqueda de indicios para el esclarecimiento de lo ocurrido.

La investigación es el componente más complejo del proceso, e involucra un gran número de actividades. Esta etapa de investigación debe tener clara la premisa de que es importante, desde el principio hasta el fin, mantener la cadena de custodia; por consiguiente, la documentación será la pieza fundamental del proceso.

De igual manera esto puede ser dividido en diversos momentos que pueden ser:

-Asegurar la escena del crimen y su respectiva documentación.

-Evaluar la escena del crimen.

-Aislar la escena del crimen: Se debe realizar un proceso de observación de la escena y en caso de ser posible delimitar la escena física.

-Realizar las entrevistas preliminares de tal manera que se indague por la información y sobre todo de la escena bajo investigación, de igual manera, es necesario que estas actividades estén debidamente documentadas.

-Documentación de la escena del crimen: Es necesario crear un registro completo y detallado para la investigación, buscando mantener la cadena de custodia que es de vital importancia para el proceso. Para este caso es posible el uso de:

- Toma de fotografía y/o video de la escena.

- Documentación de los componentes de la escena, describiendo cada uno de ellos.

- Etiquetar todos y cada uno de los componentes de la escena.

-Recolección de la evidencia digital: Fase de mucho cuidado en la que los especialistas deben prestar mucha atención a la forma como la evidencia es recolectada, de tal manera que no afecten la integridad de la información que es almacenada a través de un medio digital o fuente donde se encuentra la información. Es necesario que se documente el estado en el que se encuentra el medio tecnológico, indispensable documentar si se encuentra apagado o encendido el medio tecnológico, puesto que de cada uno de estos estados se debe realizar una acción en particular. Tomar en caso de ser necesario la información más volátil del sistema, entre ellas están la información de la memoria y los procesos que se están ejecutando en caso de estar prendida la máquina y en operación normal.

-Almacenamiento, transporte y embalaje de los indicios: Es necesario poseer las condiciones necesarias para el almacenamiento y transporte de los medios digitales, dado que condiciones como la humedad, la temperatura, las corrientes eléctricas y los

campos magnéticos pueden alterar los medios de almacenamiento y por ende, la información que allí se encuentra almacenada. En ellos es necesario garantizar: - etiquetado y marcado de los indicios identificados, con el objetivo de poder replicar en un ambiente controlado para su posterior análisis.

Guardar los medios tecnológicos en embalajes que eviten los problemas con la estática. - No transportar los indicios por largos períodos de tiempo, en este aspecto que salga de la escena del crimen directo para el laboratorio donde se realizara su posterior análisis. - Se debe almacenar en un ambiente adecuado para ello, como son los laboratorios que se dispongan para investigar y analizar los componentes tecnológicos definidos.

Para evitar la contaminación del lugar y poder documentar la condición original del escenario, todo el personal que interviene debe hacer el máximo esfuerzo para poder mantener asegurada y protegida dicha escena. El aseguramiento requiere conservar en forma original el espacio físico donde aconteció el hecho con la finalidad de evitar cualquier alteración, manipulación, contaminación, destrucción, pérdida o sustracción de los elementos, rastros o indicios que en el lugar se localicen.

La protección inicial de la escena del crimen implica mantener de inmediato la intangibilidad del espacio físico en el que pudieran hallarse elementos, rastros o indicios vinculados con el suceso.

Una escena del crimen es caracterizada frecuentemente con un espacio físico delimitado de alguna manera, por paredes, por un área más extensa o simplemente delimitadas por el suelo, en función de esta característica se dice que la escena es cerrada, abierta o mixta. Un componente electrónico puede hallarse en cualquiera de estas escenas, cuando se encuentra en escena abierta se puede asumir que el dispositivo electrónico se halla en una escena virtual cerrada, con esa misma lógica de los opuestos complementarios, cuando la escena física es cerrada por ejemplo, delimitada por un edificio u oficina se puede asumir que la escena virtual será abierta o mixta en el supuesto de que exista algún tipo de red.

Cuando se sospecha o se tiene certeza de la ocurrencia de un hecho anormal, se debe bloquear el uso y acceso a todos los dispositivos, medios electrónicos, magnéticos u ópticos que puedan estar comprometidos.

Si en una escena física se procede con el acordonamiento del lugar, en casos de escenas que comprendan ordenadores se debe tomar en cuenta que éstos pueden estar conectados a redes, por lo tanto se aislara de la forma más eficiente y así evitar cualquier tipo de contaminación. Consideremos, por ejemplo una oficina probablemente un puesto de trabajo puede contener algunos, o todos los dispositivos siguientes:

a) Un ordenador de sobremesa o móvil

b) Teléfono móvil;

c) Agenda electrónica

d) Memorias *flash*

e) Discos compactos (*Cd* o *Dvd*)

f) Impresora

g) Teléfono / fax que puede tener memoria de grabación

h) Dispositivos *USB*, de diferentes tipos

Tales son estos dispositivos que pueden llegar a manejar y almacenar información variada y valiosa para el caso en investigación, por tal motivo es muy importante ser metódico en todos los procedimientos a realizar, comenzando con un buen acordonamiento de la escena y de esta manera asegurando los dispositivos que posteriormente van a ser analizados.

En caso de las computadoras, si en la pantalla se ve algo que podría perderse y si esta se apaga, es recomendable redactar un acta donde se exponga y se describa todo lo que se muestra en dicha pantalla, de la misma manera documentarlo por medio de fotografía y video para que de esta manera quede constancia de lo que se está realizando.

Una de las mejores maneras de aislar la escena electrónica del hecho es quitar la alimentación de forma inmediata, en caso de ordenadores personales se quitará la energía eléctrica sin apagar vía sistema operativo, en caso de un ordenador portátil se apagará quitando la batería o en su defecto por el botón de energía, se debe tomar en cuenta que lo que se llega a perder es poco comparado con la protección que se logra.

La escena del delito informático es idéntica a la física en los cuidados requeridos, no se deben utilizar, encender o apagar los dispositivos dado que estaría contaminando las evidencias, tenga en cuenta que con el solo hecho de conectar una memoria (*USB*) modifica la escena del delito introduciendo elementos ajenos al hecho en investigación.

1.4. Indicios

La voz indicio proviene de indicium, a su vez derivado del latín indicere, que significa indicar, señalar, mostrar, hacer, conocer algo, etc. Se entiende también como un signo o señal, rastro o huella. Los griegos lo denominaban termaria, si era equivocada, y semela si era inequívoco.

En el Diccionario de idioma español de la Real Academia Española de la lengua nos indica que "indicio es el fenómeno que permite conocer o inferir la existencia de otro no percibido".[5]

[5] www.rae.es, fecha de consulta: 12/01/2016

"La importancia de los indicios estriba en que cualquiera de ellos puede resultar o ser la clave en determinado caso".[6]

"Es el que puede ser encontrado tanto en el lugar de los hechos y en el cuerpo de la víctima o del victimario, como en las áreas relacionadas, ya sean próximas o distantes".[7] "Es todo objeto, instrumento, huella, rastro, marca o señal que se produce durante la ejecución de un delito".[8]

Indicios son las características más frecuentes en el lugar de los hechos; indicios es todo aquel material significativo, sensible susceptible de mayor investigación; relacionado con un hecho supuestamente delictivo, cuyo estudio permite reconstruirlos, identificar a sus autores y establecer su comisión.

1.5. Cadena de custodia

Es el mecanismo que garantiza la autenticidad de los elementos probatorios recogidos y examinados, esto significa que las pruebas corresponden al caso investigado sin que se dé lugar a confusión, adulteración, perdida, ni sustracción alguna. Por lo tanto, toda persona que participe en el proceso de cadena de custodia debe velar por la seguridad, integridad y conservación de dichos elementos.

---

[6] López Calvo, Pedro y Gómez Silva, Pedro, **Investigación criminal y criminalística**. Pág. 15.
[7] Moreno González, L. Rafael. **Ob. Cit**. Pág. 21
[8] *Morales Trujillo, Luis Javier y otros.* ***CCI Criminalística, criminología e investigación***, *Pág. 164*

La cadena de custodia de la prueba, encuentra su fundamento en el debido proceso. De tal manera, que desde ese punto de vista se define como: "El procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene como fin no viciar el manejo".[9]

Es un procedimiento de seguridad para garantizar que el perito informático reciba del responsable de la investigación, los elementos de prueba en el mismo estado en que fueron reunidos en el lugar del hecho, igualmente que sean devueltos al responsable de la investigación en la misma situación, de forma que al ser presentados ante el tribunal se pueda comprobar su autenticidad y no existan dudas sobre la misma.

Toda transferencia de custodia debe quedar consignada en las hojas del registro de la cadena de custodia, indicando fecha, hora, nombre y firma de quien recibe y de quien entrega.

Para Javier Badilla la cadena de custodia se define en los siguientes términos: "Es el procedimiento de control que se aplica al indicio material relacionado con el delito, desde su localización por parte de una autoridad, hasta que ha sido valorado por los órganos de administrar justicia".[10]

---

[9] Arbulora Valverde, Arístides, **La cadena de la custodia**. Pág. 3
[10] Badilla, Javier. **Procesamiento de la escena del crimen**. Pág. 23

Es aquel registro escrito que lleva detalladamente el manejo de la evidencia, así como las personas que han tenido contacto con alguna pieza desde el momento de su recolección hasta el momento en que la misma se presente al tribunal que conoce del caso, objeto de la investigación, la cual es de suma importancia en virtud de garantizar que el objeto que se está presentando como evidencia tiene relación con los hechos que se investigan.

La Cadena de Custodia es el conjunto de requisitos que cuando sea procedente deben observarse para demostrar la autenticidad de los objetos y documentos relacionados a un hecho delictivo que inicia a partir de la recolección de los indicios, embalaje, transporte, análisis y su custodia, hasta su valoración en el juicio.

Para que la cadena de custodia tenga validez y pueda ser utilizada sin objeciones en un juicio, debe satisfacer, ciertos requerimientos:

Que el indicio haya sido recolectado, embalado y etiquetado adecuadamente. La preservación adecuada; el transporte adecuado; y la entrega apropiada de la misma.

Dentro del desarrollo de cada una de las etapas de la cadena de custodia, los responsables de recibir los elementos materiales e indicios deben corroborar que estos objetos sean enviados junto con el respectivo formato de cadena de custodia, asimismo, se debe realizar la revisión del embalaje de los mismos a fin de observar si presenta alguna alteración o modificación tanto en el embalaje como en los rótulos, etiquetas, el sellado y firmado.

En caso de descubrir alguna alteración en los rótulos o en el embalaje, el responsable deberá comunicarlo de manera inmediata al jefe y a la autoridad competente, dejando constancia escrita en el formato de cadena de custodia.

Es aquel registro escrito que lleva detalladamente el manejo de la evidencia, así como las personas que han tenido contacto con alguna pieza desde el momento de su recolección hasta el momento en que la misma se presente al tribunal que conoce del caso, objeto de la investigación, la cual es de suma importancia en virtud de garantizar que el objeto que se está presentando como evidencia tiene relación con los hechos que se investigan.

CAPÍTULO II

2. La informática forense

Fue Soleiman, un comerciante árabe, quien sugirió que a los prestatarios se les ordenará mediante un proyecto de ley colocar su huella digital en el documento que iba a ser entregado a la entidad crediticia. Como prueba, el proyecto de ley fue reconocido como una validación legal de la deuda existente.

En 1978 se empiezan a reconocer en la ciudad de Florida en Estados Unidos los crímenes de sistemas informáticos relacionados con la computadora denominados "Computer Crimes Act", en casos de sabotaje, copias no autorizadas, modificación de datos y ataques similares.

En 1987 se crea la asociación dedicada a la investigación de crímenes tecnológicos denominada "High Tech Crime Investigation Association", en la cual se agrupan a profesionales tanto de agencias gubernamentales como compañías privadas para centralizar conocimiento e impartir cursos. John C. Smith detalla la historia de esta organización aún vigente en su página web.

El auge de las nuevas tecnologías nos está llevando a niveles inimaginables que solamente se podían ver en las películas o programas de ficción. La infraestructura de cámaras de televigilancia colocadas en las urbes ha permitido controlar e informar sobre el tráfico, niños desaparecidos, congestionamientos e incluso para dar

información sobre un hecho delictivo. El uso y proliferación de sistemas de telefonía móvil y la vasta red que esta posee, permite comunicaciones sin límites y nos brindan un medio sofisticado de enlace comunicacional a nivel de empresas o a nivel persona.

Debido a hechos que han marcado y estremecido el acontecer nacional se ha visto cómo un grupo de personas de las fuerzas de seguridad, investigadores y terceros expertos en temas de seguridad, con la combinación de las tecnologías que se mencionaron, han podido dar con personas que cometen delitos. A esta nueva ciencia se le conoce como Informática Forense y tiene como objetivo tomar, cuidar, analizar, preservar y presentar a partir de una fuente digital -cámaras, celulares, computadoras, videos, audio, etcétera- la evidencia cruda que servirá como un resultado incriminatorio sobre un hecho delictivo.

La Informática Forense tiene varias ramas y una de ellas se conoce como la Video Forensia, la cual a través de técnicas de interpolación de imágenes y utilizando software especializado, permite por medio de imágenes o videos, hacer acercamientos y detallar con una excepcional precisión un número de matrícula, un rostro, colores de un vehículo y todo el entorno sobre el ambiente que se esta trabajando.

Uno de los muchos beneficios de la informática es que tiene la capacidad de conectar a personas de todas partes del mundo con intereses comunes. A los ojos de algunos, la naturaleza del mundo cibernético es más un lugar espacio peligroso que real, especialmente para niños. De acuerdo al experto en seguridad de software, "cuando (comunicación inapropiada adulto-niño) sucede en la vida real, tu sabes que es lo que

está sucediendo"[11] No es lo mismo cuando se trata de esta comunicación por medio del ciberespacio. En el internet, los padres quizás no se imaginan que sus hijos estén hablando con una persona mayor. Y así no solo con menores de edad, también personas adultas pueden estar cayendo en los engaños que el mundo cibernético nos ofrece.

Esta técnica ha permitido la captura en estos últimos meses de personas implicadas en delitos de alto impacto, debido a la gran ayuda de los sistemas de cámaras de la Empresa Municipal de Transito, centros comerciales, estaciones de venta de combustible y hasta en residencias; que permiten tener una fuente de investigación sobre los hechos, además un histórico de días, meses y años que permiten consultar la información antigua y utilizarla como evidencia.

Es difícil precisar el inicio de la informática forense o el comienzo del campo para el caso, pero la mayoría de los expertos coincide en que la informática forense comenzó a desarrollarse hace más de 30 años en los Estados Unidos, cuando la policía y los investigadores militares comenzaron a ver que los delincuentes obtenían ayudas técnicas en la comisión de sus delitos, esto hace latente la necesidad de que los encargados de las investigaciones se tecnifiquen.

El campo de la informática forense se inició en la década de 1980, poco después que las computadoras personales se convirtieran en una opción viable para los

---

[11] *McCurdy, Jessica,* ***Computer Crime****, Pág. 23.*

consumidores.

A comienzo de los años 90, la Oficina Federal de Investigación de los Estados Unidos observó que las pruebas o evidencias digitales tenían el potencial de convertirse en un elemento de prueba tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por examen genético. Para ello, mantuvo reuniones con diferentes organizaciones en su ámbito y a finales de los años 90 se creó la Organización Internacional para Cooperación en Evaluación con la intención de compartir información e investigar sobre las prácticas de informática forense en todo el mundo, por tal motivo ha ido expandiéndose y en constante cambio y desarrollo para encontrarse siempre en la vanguardia tecnológica.

En cuanto al sistema de telefonía, muy usado por personas anónimas que creen poder esconderse en estos y realizar amenazas, cuando la realidad es que estos equipos dejan una traza o huella sobre cada celda por la cual se mueven, además de que el registro en el celular nos permite tener un enfoque claro de qué sucedió realizando una serie de comparaciones que dan como resultados una bitácora o cronología que compromete al equipo del cual se efectuaron las llamadas o enviado los mensajes de texto.

Vale la pena destacar que en Guatemala hay un grupo de expertos que están trabajando a favor de la defensa de la seguridad ciudadana y son los peritos forenses digitales.

2.1. Definición

Para dar una definición propia es necesario hacer referencia de lo que algunos autores indican, entre ellas están "los sistemas transaccionales que permiten la realización de operaciones sobre el contenido de bases de datos".[12]

Según el autor Carlos Gispert "Es la ciencia de la información automatizada, todo aquello que tiene relación con el procesamiento de datos, utilizando las computadoras y/o los equipos de procesos automáticos de información".[13]

En principio se puede definir a la informática forense como, una ciencia forense que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos 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.

En consecuencia la informática forense se puede decir que es un proceso metodológico de recolección de evidencia para su posterior análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido en los órganos jurisdiccionales en materia penal, para que los mismos sean medios de prueba para condenar o absolver a una persona que sea juzgada por algún delito informático.
Siendo la informática forense las técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar

---

[12] Cristobal Pareja, Angel Andeyro, Manuel Ojeda. **Introducción a la Informática**. Pág. 104.
[13] Carlos Gispert, **Diccionario Enciclopédico**. Pág. 1,488.

datos que sean válidos dentro de un proceso legal. Por tal razón la informática forense es una disciplina auxiliar de la justicia, ya que por medio de ella se puede determinar mediante técnicas científicas y analíticas todo lo relacionado a la informática en busca de la evidencia digital.

Según la Oficina Federal de Investigación de los Estados Unidos, la informática forense, es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio de computación.

Computación forense, que entendemos por disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para esclarecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

2.2. Validez jurídica de la evidencia digital

Se puede decir que el término evidencia digital abarca cualquier información en formato digital que pueda establecer una relación entre un delito informático y su autor. Desde el punto de vista del derecho probatorio, la evidencia digital puede ser comparable con un documento como prueba legal. Con el fin de garantizar su validez probatoria, los documentos, y por ende la evidencia digital, deben cumplir con algunos requerimientos, estos son:

- Autenticidad: La autenticidad consiste en satisfacer a un tribunal en que, los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa.

- Precisión: La precisión se refiere a que debe ser posible relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación ante un tribunal en un proceso penal. Adicionalmente, los procedimientos deben ser seguidos por alguien que pueda explicar, en términos comprensibles, cómo fueron realizados y con qué tipo de herramientas se llevaron a cabo.

- Suficiencia: La suficiencia se refiere a que la evidencia digital debe de ser completa, que por sí misma y en sus propios términos muestra el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

2.3. Programas destructivos

Los programas destructivos funcionan de manera similar a la destrucción de registros ya que puede ser convertido mediante virus, gusanos, bombas lógicas o cronológicas, los cuales fueron analizados anteriormente. Dentro de los programas destructivos existen varios tipos de comandos dañinos. Clasificación de los múltiples métodos que

afectan el software:

a) Datos engañosos: es el más seguro y eficaz método utilizado por los delincuentes informáticos, el cual consiste en la alteración de los datos de entrada al computador, a través de manipulaciones difíciles y casi imposibles de detectar; los datos son ingresados con omisiones o agregaciones que los alteran en su sentido y contenido.

b) Caballo de Troya: es otro método de sabotaje muy utilizado, mediante el cual se introduce una serie de órdenes en la codificación de un programa con el propósito de que éste realice funciones no autorizadas.

c) La técnica salami: es muy utilizada en las instituciones en que hay un continuo movimiento de dinero y consiste en la sustracción de pequeñas cantidades activas de diferentes procedencias, logrando a través de él un redondeo en las cuentas.

d) Superzapping: es el manejo de programas de uso universal, la copia y la reproducción que evita el pago de los derechos de propiedad.

e) Bombas lógicas: son programas ejecutados en momentos específicos o bajo determinadas condiciones; son rutinas a posteriori según circunstancias de tiempo, de fecha, pago, etc.

f) Recogida de residuos: es la recogida de información residual impresa en papel o

magnética en memoria, después de la ejecución de un trabajo, con ella se puede establecer la situación de una empresa, los niveles de renta, etc., en fin, todos los datos que se encuentren en el papel y que quedan como borradores.

g) Suplantación: consiste en lograr el acceso a áreas que son controladas por medios electrónicos o mecánicos.

h) Simulaciones y modelos: fundamentalmente consiste en utilizar el computador para planificar y controlar un delito, mediante el uso de técnicas de simulación y modelos.

i) Puertas con trampas: es la utilización de interrupciones en la lógica del programa, en la fase de desarrollo para su depuración y uso posterior con fines delictivos.

j) Pinchar líneas de teleproceso: es la intervención en las líneas de comunicación para lograr el acceso y posterior manipulación de los datos que son transmitidos.

k) Ataques asincrónicos: es el aprovechamiento de funcionamientos asincrónicos de un sistema operativo, basado en los servicios que puede realizar para los distintos programas de ejecución.

l) Filtración de datos: consiste en filtrar o sacar los datos de un sistema por sustracción o copia, como ocurre al duplicar una cinta.

Esta conducta delictiva se puede realizar de diversas maneras y no es necesaria la presencia física del autor, ya que lo puede hacer a distancia con un simple acceso a internet, lo puede hacer a través de la distribución de freeware, lo puede hacer a través de la alteración de programas y a través del engaño con productos de computación.

El Código Penal Salvadoreño menciona que Sujeto activo, puede ser cualquiera, que tenga conocimientos en informática y computación y el sujeto pasivo, puede ser cualquiera que posea un ordenador.

El tipo subjetivo del presente delito contiene un elemento consistente en la finalidad de vulnerar la privacidad y propiedad del sujeto pasivo.

Dicho tipo subjetivo realizado por el sujeto activo se refleja en la conducta típica contenida dentro de la legislación guatemalteca como lo menciona el Artículo 274 G del Código Penal de Guatemala que menciona que "al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación."

La consecuencia de la conducta típica resulta en los ordenadores o computadores dañados por los programas con fines de alteración o funcionamiento irregular en perjuicio del propietario, siendo entonces estos el objeto material del delito. De dicha cuenta es fácil observar que el bien jurídico protegido es la propiedad privada y la información contenida en los ordenadores.

2.4. Virus

"Hoy se denomina virus al software dañino que, una vez instalado en una computadora (ordenador), puede destruir los datos almacenados. Estos virus se conocen específicamente como virus informáticos".[14]

Un virus es un programa que en poco más de uno o dos Kbytes consiguen realizar acciones inimaginables; desde mostrar diversos mensajes o gráficos en pantalla hasta formatear el disco duro o hacernos perder todos los datos en él guardados.

Un virus de computadora, por definición, es un programa -o código- que se replica añadiendo una copia de sí mismo a otro archivo ejecutable. Un virus particularmente se da cuando el usuario trabaja sin protección antivirus y muchas veces no se percata de que su sistema está invadido, hasta que ve los resultados que pueden ir desde anuncios inocuos hasta la pérdida total del sistema.

2.5. Clases de virus

Existen una variedad de virus en función de su forma de actuar o de su forma de infectar clasificados de la siguiente manera.

- Acompañante: Estos virus basan su principio en que MS-DOS, ejecuta el primer archivo COM y EXE del mismo directorio. El virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar.

[14] http://definicion.de/virus-informatico/ consultado el 21/01/2016

Después de ejecutar el nuevo archivo COM creado por el virus y cede el control al archivo EXE.

- Archivo: Los virus que infectan archivos del tipo *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS e incluso BAT. Este tipo de virus se añade al principio o al final del archivo. Estos se activan cada vez que el archivo infectado es ejecutado, ejecutando primero su código vírico y luego devuelve el control al programa infectado pudiendo permanecer residente en la memoria durante mucho tiempo después de que hayan sido activados.

Este tipo de virus de dividen en dos:

-Virus de sobreescritura Se escriben dentro del contenido del fichero infectado, haciendo que pueda quedar inservible. Se ocultan por encima del fichero de tal forma que la única manera de desinfectarlo es borrar dicho archivo, perdiendo así su contenido.

-Virus de acción directa: Que son aquellos que no se quedan residentes en memoria y se replican en el momento de ejecutar el fichero infectado y los virus de sobrescrita que corrompen el fichero donde se ubican al sobrescribirlo.

- Bug-Ware: Es el término dado a programas informáticos legales diseñados para realizar funciones concretas. Debido a una inadecuada comprobación de errores

o a una programación confusa causan daños al hardware o al software del sistema.

Muchas veces los usuarios finales aducen esos daños a la actividad de virus informáticos. Los programas bug-ware no son en absoluto virus informáticos, simplemente son fragmentos de código mal implementado, que debido a fallos lógicos, dañan el hardware o inutilizan los datos del computador el término bug fue asociado a interferencias y malfuncionamiento desde mucho tiempo antes de que existieran los ordenadores modernos, siendo Thomas Edison uno de los primeros en acuñar este significado. Si bien fue una mujer, Grace Murray Hopper, quién en 1945 documentó el primer bug informático.

Bug, traducido literalmente del inglés como bicho, adquiere otro significado cuando hablamos de informática. Esta otra acepción se refiere a elementos y circunstancias en el software o hardware, involuntarios e indeseados, que provocan un malfuncionamiento. A lo largo de los años este término se ha popularizado y hoy día se utiliza comúnmente para referirse a los errores en los programas informáticos.

La relación con la seguridad informática es directa, ya que muchas de las vulnerabilidades que día a día vemos en hispasec están asociadas a "bugs".

Grace Murray Hopper (1906-1992), graduada en matemáticas y física por el Vassar College, y doctora en matemáticas por la universidad de Yale, ha pasado a

la historia por ser una innovadora programadora durante las primeras generaciones de ordenadores.

En el año de 1943, en el período de la segunda guerra mundial, decidió incorporarse a la marina de los Estados Unidos de América. Fue destinada al laboratorio de cálculo Howard Aiken en la Universidad de Harvard, donde trabajó como programadora en el Mark I.

El 9 de septiembre de 1945 el grupo de trabajo de Aiken y Grace se encontraba en la sala del Mark II intentando averiguar por qué el ordenador no funcionaba adecuadamente.

Tras un examen concienzudo lograron detectar que la culpable era una polilla de dos pulgadas que se había colado entre los contactos de unos de los relés del Mark II. Más tarde, Grace registraría el incidente en el cuaderno de bitácoras, pegó la polilla que causó el problema y anotó debajo la frase First actual case of bug being found.

Cada vez que algún ordenador daba problemas ellos decían que tenía bugs (bichos o insectos). Años más tarde Grace también acuñaría el término debug para referirse a la depuración de programas.

Además de los fines militares, única razón de ser de los primeros ordenadores, cuentan que Grace fue de las primeras personas en buscar utilidades civiles a la informática.

Entre sus muchos méritos destaca la creación del lenguaje Flowmatic, el desarrollo del primer compilador, o su trabajo en la primera versión del lenguaje COBOL.

"Los virus informáticos pueden borrar información, saturar una red, exhibir carteles molestos o apagar la computadora, entre otras posibilidades. Para proteger un equipo de infecciones y eliminar virus, existen los llamados antivirus, que son programas especialmente creados para combatir al software malicioso".[15]

Grace continuó con sus avances en computación y tuvo numerosos reconocimientos a lo largo de su carrera. Entre otros, recibió el premio Hombre del Año en las Ciencias de Cómputos por la Data Processing Management Association. Fue la primera mujer nombrada Distinguished fellow of the British Computer Society, y la primera y única mujer almirante en la marina de los Estados Unidos hasta la fecha.

La informática forense es una disciplina de la criminalística relativamente nueva ya que tuvo sus inicios aproximadamente hace 30 años en los Estos Unidos de América, y a la fecha no han sido regulados los delitos informáticos en nuestro ordenamiento jurídico penal, por lo que las personas que cometen este tipo de hechos no pueden ser sometidos a investigación, quedando en la impunidad, debido a la falta de tipos penales que encuadren su accionar, esperando que en un futuro no muy lejano se realice la reforma en el Código Penal y así poder regular las conductas que vallan encaminadas con hechos relacionados a la informática, ya que de hecho se cuenta con una gran variedad de técnicas y métodos criminalísticos que podrían coadyuvar en las

[15] http://definicion.de/virus-informatico/ consultado el 22/01/2016

investigaciones judiciales, las cuales podrían ser encaminadas exclusivamente para el manejo, obtención, preservación y conservación de indicios informáticos, capacitando al personal idóneo, con conocimientos generales en informática y así facilitar el adiestramiento en la ciencia de la informática forense, la cual tiene sus fundamentos en las leyes de la física, electricidad y magnetismo, dando así validez jurídica a la evidencia digital recolectada en la escena del crimen, y cumpliendo con los requerimientos necesarios para que aquella sea aceptada como un medio de prueba en el desarrollo del debate.

CAPÍTULO III

3. Delitos informáticos

El aspecto principal de la informática, radica en que "la información se ha convertido en un valor económico de primera magnitud. Desde la antigüedad el hombre ha tratado de encontrar medios para guardar información relevante, para poderla usar posteriormente, desde la era pre-Gutenberg, que se caracterizaba por la transmisión de las informaciones de forma manual o personal, por medio de los individuos que generaban la misma, pasando por la era de la impresión, la era eléctrica-analógica, hasta la era digital que brinda la posibilidad de transmitir la información, a bajo costo, con facilidad y en forma rápida, la cual se encuentra almacenada electrónicamente, de forma bidireccional e interactiva desde cualquier parte del mundo a cualquier destino, recurriendo a una variedad de tecnologías; se puede observar la evolución de la información y el valor que ésta tiene".[16]

Como señala Camacho Losa, "En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia".[17]

---

[16] Magliona Markovicth Claudio Paúl, López Medel Macarena, **Delincuencia y Fraude Informático**, pág.43
[17] Camacho Losa Luis, **El Delito informático**, pág. 12

El término delito informático se acuñó a finales de los años noventa, a medida que *Internet* se expandió por toda Norteamérica. Después de una reunión en *Lyon* Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado "G8" con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados en *internet*. Según López Manrique "El Grupo de *Lyon* utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos".[18]

Al parecer todos los estudiosos de la materia están de acuerdo, en pensar que el surgimiento de este tipo de crímenes está íntimamente ligado al desarrollo de la tecnología informática. Las computadoras se han utilizado para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato. Para los autores chilenos Marcelo Huerta y Claudio Líbano "este fenómeno ha obligado al surgimiento de medidas legislativo penales en los estados industriales donde hay conciencia de que en los últimos años, ha estado presente el fenómeno delictivo informático".[19]

Se puede mencionar que es un término relativamente nuevo, y que se ha desarrollado por el avance de las tecnologías, teniendo su origen en la expansión de la Internet, por lo que fue necesario crear una denominación para referirse a los tipos de delitos que surgieron con el avance informático, de acuerdo a lo señalado por la autora citada, se puede indicar que los delitos informáticos tienen su origen con el surgimiento de la

[18] Yuri Vladimir López Manrique. **Computación forense: una forma de obtener evidencias para combatir y prevenir delitos informáticos**. Pág. 1
[19] Huerta Marcelo y Líbano Claudio, **Delitos informáticos**, pág. 4.

Internet y fue por ello que se vislumbró la necesidad de denominar de alguna manera a las conductas ilícitas, realizadas a través de un ordenador.

La legislación Guatemalteca regula algunos delitos informáticos en el código penal, como también en la ley de derechos de autor y derechos conexos, y la ley de propiedad industrial, así mismo protege los derechos humanos en el ámbito cibernético.

Los delitos informáticos según nuestra legislación penal se circunscriben a siete acciones antijurídicas punibles de acuerdo al Artículo 274 en sus literales "A", "B", "C", "D", "E", "F", "G" del Código Penal, los cuales son:

1. "Destrucción de registros informáticos

2. Alteración de programas.

3. Reproducción de instrucciones o programas de computación.

4. Registros prohibidos.

5. Manipulación de información.

6. Uso de información.

7. Programas destructivos."

Es por ello que debe de regularse la forma como se utiliza el internet en Guatemala, pues a diferencia de otros países en Guatemala existe una libertad sobre su uso, limitándose únicamente regular los derechos respecto a cualquier violación y penas para quien cometiera delitos contra los bienes jurídicos tutelados pero estos generalizan los hechos, y habiendo tanta libertad respecto a esto, como lo explica el doctor, no tiene sentido hablar de libertad si, nuestra propia normativa no puede limitar sus propias fronteras.

Dicha ley establece normas especiales tendientes a la regulación de los delitos informáticos, suficientes para prevenir, controlar y sancionar las conductas de cibercrimen que no tiene límites fronterizos, ni normas que los limiten, pretendiendo limitar a los criminales y proteger de toda violación a los titulares de derechos o a aquellos que se ven afectados por los cibercriminales.

La iniciativa conceptualiza lo que es delito informático, documento, pornografía infantil, sistema informático, tarjeta inteligente y tecnología de información, su ámbito de aplicación, los superpuestos en los que se está ante un acceso sin autorización, el daño que se puede provocar en el ámbito informático, espionaje. Una de las cosas que cabe resaltar es que dicha iniciativa planteaba crear una unidad de investigación especializada en los delitos informáticos, lo cual hubiera sido muy ventajoso para Guatemala, pues habría un ente encargado de velar por el cumplimiento estricto de la ley y encargado de la investigación del tema.

El profesor español Romeo Casabona define a la criminalidad informática como "la realización de una forma de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software".[20]

Delincuencia informática y abuso informático, es un conjunto de conductas merecedoras de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están relacionados íntimamente con ésta, pudiendo mostrar varias formas de daños de distintos bienes jurídicos.

El delito informático o cibernético para el profesional Carlos Sarzana, es "aquel delito que abarca cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena o como mero símbolo".[21]

De lo antes descrito se pueden diferenciar dos clases de delitos informáticos: a) Ataques pasivos: divulgación del contenido de mensajes ajenos, análisis de información de terceros. Y b) Ataques activos: utilización de *passwords* ajenos, modificación de mensajes y/o archivos.

---

[20] Romeo Casabona, Carlos María. **Poder informático y seguridad jurídica**.pág.26
[21] www.dtj.com.ar/publicaciones.html. Consultado el 25/01/2016.

El delito informático es "la realización de una acción que reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades".[22]

Casabona señala que "En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo no se puede hablar de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadoras, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del hecho delictivo o merecedor de serlo, presenta siempre características semejantes, la computadora es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el hardware, el software, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información".[23]

Como define Carlos Resa, "el crimen organizado no existe como tipo ideal, sino como un grado de actividad criminal o como un punto del 'espectro de legitimidad".[24] En este contexto es el crimen organizado que a través de los años se ha ido transnacionalizando su actividad y por ello se habla de delincuencia transnacional.

---

[22] http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf, (consultado el 25/01/2016).
[23] Romeo Casabona, Carlos María. **Ob.Cit.** pag.12.
[24] Resa Nestares Carlos, **Crimen organizado transnacional: definición, causas y consecuencias**, pág.47

Dentro de esta definición de crimen organizado, la gama de actividades que puede ejecutar un determinado grupo de crimen organizado puede ser extensa, variando en cada caso según diversas variables internas y externas a la organización, y combinar uno o más mercados, expandiéndose asimismo por un número más o menos limitado de países, aunque en tiempos recientes existe una fuerte tendencia a la concentración empresarial en cada vez menos grupos de un mayor número de campos de la ilegalidad. Su repertorio de actividades incluye el delito de cuello blanco y el económico (en donde se encontrarían los delitos informáticos), pero supera a éste último en organización y control, aunque los nexos de unión entre ambos modelos de delincuencia tienden a fusionarse y el terrorismo y el ciberterrorismo pueden llegar a formar parte de sus acciones violentas en ciertas etapas o momentos.

3.1. Naturaleza y objeto

El objeto se enmarca en las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física.

Conductas dirigidas a causar daños en el *hardware* o en el *software* de un sistema. Programación de instrucciones que producen un bloqueo total al sistema.

Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han evolucionado hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se puede diferenciar dos grupos de casos: las

conductas dirigidas a causar destrozos físicos y los métodos dirigidos a causar daños lógicos.

Como fin las conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla. La clasificación de estos delitos es muy amplia, por una parte son conductas criminales que se valen de las computadoras como método o medio, y por otro lado están las que van dirigidas a efectuar daños tanto externos como internos a las computadoras, por consiguiente es de suma importancia prestarle la debida atención ya que de una u otra forma podemos ser víctimas de nuestra información o de nuestro propio equipo de cómputo.

La naturaleza de los delitos informáticos es eminentemente jurídico penal ya que dichas conductas están reguladas en las leyes en metería penal.

3.2. Delito programas destructivos

El Decreto número 33-96 del Congreso de la República de Guatemala en el Artículo 19 adiciona el Artículo 274, literal "G" del Código Penal, el cual establece: "Programas destructivos. Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación".

En este caso se protege, de los programas destructivos fundamentalmente dos elementos de los sistemas de información, que son:

- Los registros

- Los programas de ordenador (software)

En el ambiente informático y de las tecnologías de la información y las comunicaciones, existen programas denominados virus electrónicos, virus digitales o programas perjudiciales. Los virus se definen como, "los programas de ordenador que tienen por objeto introducirse en los sistemas informatizados para causar algún daño a la información, al sistema operativo, a los programas en general y se considera que algunos pueden llegar a dañar el hardware".

Estos programas perjudiciales han causado pérdidas patrimoniales a nivel mundial que se calculan en millones de dólares de los Estados Unidos de América. En Guatemala ha tenido consecuencias de factor económico considerable, pero no existen estadísticas o estudios al respecto para los usuarios.

Existen otros tipos de programas informáticos perjudiciales, algunos dañan a la propia computadora, mientras que otros utilizan la computadora para atacar otros elementos de la red; algunos programas (llamados bombas lógicas) pueden permanecer inactivos hasta que se desencadena por algún motivo, como por ejemplo, una fecha determinada, causando graves daños modificando o destruyendo datos. Otros

programas parecen benignos, pero cuando se activan, desencadenan un ataque perjudicial (a los denominados caballos de Troya); otros programas (denominados gusanos) no infectan programas con virus, pero crean réplicas de ellos mismos, estas crean a su vez nuevas replicas y de ese modo se termina por invadir el sistema. Por esta razón las personas que utilizan los sistemas de información deben de protegerse según el nivel de riesgo, con un programa antivirus; los niveles de seguridad dependen de la información y de la interconexión con otras redes.

En cuanto al hecho ilícito es importante determinar si existe responsabilidad penal o no, en virtud que el artículo 274, literal "G" del Código Penal establece "al que distribuye o pusiere en circulación.". Cuando una persona crea el virus informático no tiene responsabilidad penal, porque el simple hecho de crear un programa destructivo no constituye un delito.

Cuando éste se distribuye o se pone en una u otras computadoras, en una red interna, externa o el internet, es cuando concurren todos los elementos de tipificación del delito, aunque este no logre el daño que se tiene propuesto en virtud de detección y eliminación por un antivirus o no ingresa a la red por medio de un firewall.

Destrucción de registros informáticos: El Decreto número 33-96 del Congreso de la República de Guatemala, en el Artículo 13 adiciona el Artículo 274, literal "A" el cual establece: "Destrucción de registros informáticos. Será sancionado con prisión de seis meses a cuatro años y multa de doscientos a dos mil quetzales, el que destruye, borrare o de cualquier modo inutilizarse registros informáticos.

La pena se elevará en un tercio cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial".

El bien jurídico tutelado se define como registro informático, que consiste en la base de datos creada por el sistema informático utilizada para la toma de decisiones. El Artículo 274, literal "A" del Código Penal establece el que: "destruyere, borrare o de cualquier modo."; destruir información se refiere a que el sujeto responsable del hecho destruya la información lo que equivale a cambiar su naturaleza de tal forma que no pueda recuperarse por medios electrónicos (el original instalado).

Al establecer borrare, se refiere a eliminar de forma física en los dispositivos almacenamiento la información. La frase o de cualquier modo, deja a una variedad de posibilidades, que puede ejemplificarse en el caso que con intención se grabe información sobre la existente, o utilice algún dispositivo para afectar el acceso a los registros informáticos.

Es importante agregar que aunque la victima cuente con una copia de seguridad de la información (backup) no es causa para eximir de responsabilidades al sujeto activo. El Artículo 274, literal "A" del Código Penal también divide los registros en privados y públicos, considerando como un agravante cuando es contra los registros públicos.

En ausencia de legislación que determine que debe de entenderse por registro públicos se interpreta que se refieren a los registros a cargo de la administración pública y que contienen datos personales.

Otro criterio establece que se refiere a la naturaleza de los datos o información, es decir que los registros serán públicos aun cuando sean almacenados, procesados y/o automatizados por un ente privado.

3.3. Elementos del delito de programas destructivos

Siguiendo la metodología de otros módulos y en el ámbito técnico del análisis de los ilícitos a través de la teoría del delito, el elemento descriptivo apreciado a través de la vista u otros sentidos de esta clase de delitos lo sería la computadora, las bases de datos o registros informáticos o bien los bienes materiales e intelectuales afectados a través de un sistema informático u ordenador para citar algunos.

Con respecto al elemento normativo aparecen cuando los tipos acuden a valoraciones jurídicas o éticas. Normalmente el tipo se vale de descripciones para individualizar programas, pero en ocasiones lo hace mediante estas remisiones a elementos de carácter valorativo.

Debe entenderse entonces que tal elemento se aprecia intelectualmente, en el caso en particular de los delitos informáticos es necesario auxiliarse de la informática u otra ciencia para comprenderlos, en ese sentido dentro de los elementos normativos de este tipo de ilícitos tenemos los daños producidos a los equipos, a los programas o bases de datos, la pérdida patrimonial, la indemnidad sexual y de otros bienes jurídicos tutelados contenidos en la legislación.

3.4. Sujeto activo

La doctrina generalmente se refiere a dos clases de sujetos: el que realiza o comete el delito y que recibe el nombre del sujeto activo, ofensor, agente o delincuente; el segundo que es quien sufre las consecuencias del mismo y que recibe el nombre de sujeto pasivo, ofendido o víctima.

El sujeto activo del delito según las legislaciones modernas es el que realiza la acción, el comportamiento descrito en la ley. Al ser la acción un acaecimiento dependiente de la voluntad, no puede ser atribuida ni por consiguiente realizada, sino por una persona humana. Es entonces el sujeto activo del delito "quien comete o participa en su ejecución, el que comete directamente es sujeto activo primario y el que participa es sujeto activo secundario".[25]

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y puede ocurrir que por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que la diferencia entre sí es la naturaleza de los delitos cometidos.

---

[25] Reyes Calderón, José Rodolfo, **Derecho Penal, parte general.** Pág. 52

En forma más concreta en cuanto a la característica del sujeto activo del delito informático, es quien realice un hecho delictivo a través de medios informáticos y que poseen ciertas características que tienen que ver con los medios de comunicación e Internet, los sujetos activos en este tipo de delito, concretamente tienen habilidades para el manejo de los *TICS* y por lo general se encuentran en lugares estratégicos donde se maneja información o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

De esta forma, la persona que ingresa en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes de delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática pero si de una actividad punible, en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

3.5. Sujeto pasivo

Sujeto pasivo o víctima del delito informático, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos

las victimas pueden ser individuos, instituciones, gobiernos, etcétera, que usan sistemas automatizados de información generalmente conectados a otros.

El sujeto pasivo del delito según las legislaciones actuales es el que sufre las consecuencias del delito. Es entonces el sujeto pasivo del delito "el titular del interés jurídicamente protegido, atacado por el delito, o puesto en peligro".[26]

En primer término se debe distinguir que sujeto pasivo o víctima del delito es quien soporta las consecuencia del hecho delictivo que comete el victimario ya sean personas jurídica o naturales, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los "delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las

[26] *Muñoz Conde, Francisco.* ***Manual de derecho penal parte general.*** *Pág. 1*

autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada cifra oculta o cifra negra.

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento, entre otros.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

La determinación del sujeto pasivo es importante, toda vez que a través de su identificación podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos.

Los tipos de delitos informáticos a los que se encuentran sometidas todas la personas tanto individuales como jurídicas, que son blanco de las conductas ilícitas que producen personas que tiene los conocimientos técnicos y profesionales para poder, por decirlo así saquear cuentas bancarias, cometer estafas, inyectar virus a equipos computarizados, clonar programas informáticos, etcétera, quedando totalmente desprotegidas por la falta de legislación especializada en aspectos informáticos, ya que nuestro ordenamiento jurídico penal, apenas cuenta con siete Artículos que regulan algunas conductas que describen acciones que lesionan la intimidad de las personas y el desarrollo de instituciones públicas o privadas.

CAPÍTULO IV

4. Las instituciones que participan en la obtención del peritaje informático

En el mundo digital, es un poco difícil puesto que el tratamiento de la información se distribuye, se prestan servicios a usuarios móviles, y la inter operatividad de los sistemas es una condición básica. Los enfoques tradicionales de la seguridad son sustituidos por soluciones innovadoras basadas en las nuevas tecnologías.

Estas soluciones implican el uso del cifrado y las firmas digitales, de nuevos instrumentos de autenticación y de control del acceso, y de filtros de software de todo tipo. Garantizar infraestructuras de información segura y fiable, no sólo exige la aplicación de diversas tecnologías, sino también su correcto despliegue y su uso efectivo, siendo el Ministerio Público el ente encargado de la persecución penal y quien obtiene de primera mano la evidencia digital, quien se auxilia del Instituto Nacional de Ciencias Forenses de Guatemala para el procesamiento y análisis del peritaje informático por lo tanto estas dos instituciones son las instituciones que participan en la obtención de dicha evidencia.

4.1. Ministerio Público

En el nuevo proceso penal guatemalteco se han delimitado con precisión cuales son las atribuciones del órgano jurisdiccional, pues antes de la entrada en vigencia del Código Procesal Penal, los jueces de materia penal no solamente se limitaban a juzgar, sino

también eran participantes activos en la investigación, siendo en esos momentos de la historia un proceso totalmente inquisitivo y esencialmente escrito.

El actual Código Procesal Penal le brinda al Ministerio Público una serie de facultades especiales, colocándole dentro del orden jurídico nacional como un órgano de persecución de los criminales, en consecuencia se viene a convertir en el acusador oficial del Estado y por ende en el encargado de ejercer la acción y la persecución penal.

La acción penal es la facultad de provocar la actividad de la jurisdicción penal mediante la declaración de un órgano público o privado, según esta facultad se ha conferido a dichos órganos privados exclusivamente delitos de acción privada o en concurso con el órgano público acción pública; es decir, mediante una oferta o proposición de actuar la voluntad de la ley aplicable al caso.

Según el Artículo 251 de la Constitución Política de la República de Guatemala, le corresponde al Ministerio Público el ejercicio de la acción penal. Este ejercicio es en el entendido de que la violación al bien jurídico tutelado encuadre perfectamente con el principio de legalidad.

En consecuencia puede establecerse que la acción penal es la obligación que tiene el Ministerio Público actuando acorde al principio de objetividad de ser el órgano acusador del Estado. Mientras que la persecución penal es la obligación que tiene el Ministerio

Público de investigar y recabar los medios de prueba para determinar si procede el ejercicio de la acción penal.

4.2. Instituto Nacional de Ciencias Forenses de Guatemala

Ésta institución fue creada debido a que con anterioridad el servicio médico forense estaba afecto al Organismo Judicial, los laboratorios de criminalística operaban en forma dispersa, no llenaban las expectativas que en la actualidad el sistema de justicia necesitaba para probar los hechos tipificados como delito.

La prueba pericial que aporta el Instituto Nacional de Ciencias Forenses de Guatemala es el medio por el cual personas ajenas a las partes, que poseen conocimientos especiales en alguna ciencia, arte o profesión y que han sido precisamente designadas en un proceso determinado, perciben, verifican hechos y los ponen en conocimiento del juez, y dan su opinión fundada sobre la interpretación y apreciación de los mismos, a fin de formar la convicción del magistrado, siempre que para ellos se requieran esos conocimientos.

El Instituto Nacional de Ciencias Forenses de Guatemala –INACIF- es una institución auxiliar de la administración de justicia que presta el servicio de investigación, emitiendo peritajes técnicos científicos, aplicando los avances que la tecnología y la metodología actualmente ofrece a las ciencias forenses modernas, es una entidad que está en permanente desarrollo científico y tecnológico, en especialidades se encuentra a nivel de estándares mundiales en las ciencias forenses.

"Es creado con el Decreto número 32-2006 del Congreso de la República de Guatemala del ocho de septiembre de dos mil seis, como resultado de la necesidad de contar con medios de prueba válidos y fehacientes en los procesos judiciales. Cuenta con la cooperación de expertos y peritos en ciencias forenses que aplican los avances tecnológicos, metodológicos y científicos de la medicina legal y criminalística, como elementos esenciales en la investigación criminal y de cualquier otra naturaleza".[27]

Dicha institución tiene como misión fundamental "convertir los indicios en elementos útiles al sistema de justicia, mediante la realización de análisis técnico científicos en materia forense y estudios médico legales apegados a la objetividad, transparencia y autonomía, fundamentados en ciencia arte y basados en el trabajo en equipo".[28]

El Instituto Nacional de Ciencias Forenses de Guatemala a través de los dictámenes técnico científicos tiene como visión primordial "fortalecer mediante la mejora continua de sus procesos, en una institución del sector justicia autónoma, independiente y confiable; que busca mediante el esfuerzo conjunto, servir a la sociedad guatemalteca en forma efectiva y eficiente en el ámbito de la investigación científica forense".[29]

Para realizar un peritaje la institución necesita en principio la solicitud del juez o del fiscal, ya que la institución no puede actuar de oficio, según el artículo 5, el cual indica: "El INACIF no podrá actuar de oficio y realizará los peritajes técnico científicos conforme la presente Ley.".

---

[27] http://www.inacif.gob.gt/index.php?option=com (consultado el 26/01/2016)
[28] http://www.inacif.gob.gt/index.php?option=com_content&view=article&id=59&Itemid=80 (Consultado el 26/01/2016)
[29] **Ibíd.**

Asimismo, la Ley Orgánica establece que los servicios en materia de peritajes los suministrará a requerimiento de los jueces o tribunales en materia penal, auxiliares o agentes fiscales, la defensa técnica tanto privada o pública y las demás partes lo realizarán a través del Ministerio Público, sin embargo, si este último no realiza el requerimiento, los interesados en realizar alguna pericia pueden acudir al órgano jurisdiccional que está a cargo del proceso.

Para solicitar un peritaje, el ente investigador o el órgano jurisdiccional deberán indicar el objetivo técnico de la pericia, fijando cuáles serán los temas sobre los cuales versará el análisis sobre determinado indicio enviado al laboratorio. Al respecto, el Artículo 230 del Código Procesal Penal señala: "La orden de peritaje fijará con precisión los temas de la peritación.".

A través del peritaje técnico científico solicitado por autoridad competente, se da la pauta al juzgador para que actúe en forma imparcial y de valor probatorio a los indicios, para poder tener certeza jurídica al momento de emitir sentencia condenatoria o absolutoria, pronunciar un fallo o resolver sobre cuestiones litigiosas

El peritaje técnico científico está regulado en el Código Procesal Penal, el cual estipula que los peritos deberán ser titulados en la materia a la que pertenece el punto sobre el cual deba pronunciarse; debe de ser un profesional o técnico reglamentado, pero si no existiera técnico profesional, el órgano jurisdiccional podrá nombrar a la persona más idónea para que realice la pericia.

Por lo tanto, si el Instituto Nacional de Ciencias Forenses de Guatemala realizara un peritaje sin dicho requerimiento, estaría violentando el debido proceso y su actuación sería ilegal, de conformidad con lo establecido por el Artículo 225 del Código Procesal Penal: "El ministerio Público o el tribunal podrán ordenar peritación a pedido de parte o de oficio...".

Por su parte, el Artículo 234 del Código Procesal Penal indica que: "El dictamen será fundado y contendrá una relación detallada de las operaciones practicadas y sus resultados.". Como se puede establecer, el dictamen es el resultado del análisis de los indicios que son remitidos al laboratorio, los cuales deben de ser fundados en ciencia o arte, deberán presentarse por escrito, firmados y fechados por el perito que realizó la pericia.

Dentro del mismo cuerpo legal, en los Artículos del Código Procesal Penal, se regulan los tipos de peritajes, entre los especiales se pueden mencionar: autopsias, peritación por delitos sexuales y cotejo de documentos.

Lo anterior, no limita la labor de los peritos, ya que existe otra gama de peritajes que se realizan en el Instituto Nacional de Ciencias Forenses de Guatemala, de acuerdo a los avances de la ciencia y tecnología, entre estos: el peritaje balístico, identificación de vehículos, sustancias controladas, genética, serología, toxicología, acústica y lingüística forense, trayectoria de disparo, unidad de medicina forense y actualmente, se está implementando el laboratorio de informática forense.

La Ley Orgánica del Instituto Nacional de Ciencias Forenses de Guatemala en el Artículo cuatro, regula la función del perito indicando que el perito en su actuación se debe de basar en los principios de objetividad, profesionalismo, respeto a la dignidad humana, unidad y concentración, publicidad y transparencia, y gratitud del servicio.

La orden de peritaje deberá contener el objetivo técnico que se persigue con la pericia, el cual tiene que ser orientado al tipo de investigación que se está realizando y así optimizar los recursos y no realizar pericias que al final no sirven al proceso, en consecuencia, el fiscal o el órgano jurisdiccional encargado de la investigación debe de fijar con precisión los temas sobre los cuales versará la pericia y así evitar trabajo innecesario.

4.3. Peritaje informático como medio de prueba en el delito de programas destructivos, regulado en el Código Penal

Alarmantemente 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 Nacional Civil, el Ministerio Público, el Organismo Judicial y el Instituto Nacional de Ciencias Forenses de Guatemala deban especializarse y capacitarse en estas nuevas áreas en donde las Tecnologías de la Información y la Comunicación se convierten en herramientas necesarias en auxilio de la Justicia y la persecución del delito y el delincuente cibernético.

La obtención de Información (elementos de convicción) se constituye en una de las facetas útiles dentro del éxito de una investigación criminal, aspecto que demanda de los investigadores encargados de la recolección preservación, análisis y presentación de las evidencias digitales una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el órgano jurisdiccional.

Antes de entrar a conocer los aspectos de la creación del laboratorio de informática forense dentro del Instituto Nacional de Ciencias Forenses de Guatemala, es importante conocer aspectos fundamentales, principios básicos y el rol que debe jugar dicho laboratorio.

Principio de objetividad: El perito debe ser objetivo, debe observar los códigos de ética profesional.

Principio de autenticidad y conservación: Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.

Principio de 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

Principio de idoneidad: Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.

Principio de inalterabilidad: En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.

Principio de 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. 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 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, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

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 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.

Asimismo, es importante indicar cuales aparatos pueden ser analizados por un perito en informática forense. Entre los aparatos que pueden ser analizados podemos encontrar:

- Computador de escritorio

- Computador Portátil

- Estación de Trabajo

- Hardware de Red

- Servidor: Aparato que almacena o transfiere datos electrónico por el Internet.

- Teléfono celular

- Teléfono inalámbrico

- Aparato para identificar llamadas

- Localizador, beeper

- *GPS* (sistema de posicionamiento global): Es un sistema global de navegación por satélite capaz de ubicar geográficamente la posición de un objeto, una persona o un vehículo.

- Cámaras, videos

- Sistemas de seguridad

- Memoria "*flash*": Pequeño dispositivo que puede conservar hasta 4 gigabytes de datos o 4, 000, 000,000 bytes de información.

- Palm: Asistente personal electrónico que almacena datos y posiblemente tiene conectividad inalámbrica con el Internet.

- Juegos electrónicos: Unidad de datos que puede guardar, incluso, una memoria de

otro aparato.

- Sistemas en vehículos: Computadoras obvias y computadoras del sistema operativo del vehículo que registra cambios en el ambiente y el mismo vehículo.

- Impresora

- Copiadora

- Grabadora

- Videograbadora, *DVD*

- Duplicadora de discos

- Discos, disquetes, cintas magnéticas

- Aparatos ilícitos: Tales como los aparatos que capturan el número celular de teléfonos cercanos para después copiarlo en otros teléfonos, o los llamados sniffers, decodificadores, etcétera.

Individualización de archivos (hash) cuando se trata de archivos, como los musicales, los problemas probatorios pueden ser diversos.

En principio, los formatos de archivos comprimidos de audio conocidos como mp3 deben provenir de medios o copias legalmente obtenidas para no violar los derechos de autor. Aunque existan socios que tengan un mismo contenido de audio, los mismos pueden tener un origen o procedencia distintos.

Las fórmulas o algoritmos de compresión pueden ser diferentes, dependiendo del programa utilizado para abrirlo, o bien de la versión del mismo programa, produciéndose una calidad similar pero no idéntica desde el punto de vista probatorio. Por lo antes expuesto, de una misma versión de una pista musical de un cd legal pueden existir cientos de archivos con características técnicas diferentes. En los Estados Unidos de Norteamérica se han venido produciendo sentencias condenatorias por transferencias ilegales de archivos musicales y de video, al encontrarse en diversas máquinas de usuarios archivos idénticos a los hallados en servidores y servicios de transferencia de este tipo de archivo.

La computación avanzada por lo general no forma parte de los conocimientos privados del juez para poder valorarlos adecuadamente, por lo que es necesaria la promoción y evacuación de la llamada prueba pericial informática o experticia informática, siendo este auxilio de prueba el más idóneo cuando de hechos jurídicos informáticos se trata.

"Por prueba pericial se entiende que "es la que se deduce del dictamen de un perito en la ciencia o en el arte sobre el que verse la pericia. Bien se comprende que esta posibilidad probatoria es ilimitada, puesto que los juicios civiles o criminales pueden afectar a una gran cantidad de ciencias o artes. Las más frecuentes son la peritación

médica, la contable, la caligráfica, la balística, la escopométrica, la dactiloscópica".[30]

"Las pericias informáticas pueden recaer sobre diversos aspectos de los hechos informáticos y prácticamente sobre cualquier tipo de programa, aplicación o software, servicio web, correos electrónicos, análisis de programación de bases de datos. Se pide a los expertos se pronuncien sobre aspectos que pueden estar relacionados con el origen o procedencia de mensajes de datos, estructura, contenidos y otros".[31]

4.4. Legislación comparada

En los últimos años se ha afinado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del deficiente uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

Como un antecedente, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas de computación.

La OCDE en 1986, publicó un informe titulado Delitos de informática: análisis de la normativa jurídica, en donde se reseñaban las normas legislativas vigentes y las

[30] Guillermo Cabanellas de las Cuevas, **Diccionario de ciencias jurídicas políticas y sociales**. Pág. 819.
[31] http://es.scribd.com/doc/31783656/INFORMATICA-JURIDICA-EN-VENEZUELA consultado el 21/02/2016

propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales, como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

Los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los delitos informáticos, debido a los daños y perjuicios que le han causado a la humanidad. Sin embargo, si bien es cierto existe un esfuerzo por parte de los países para tratar de evitarlos, no existe un criterio unificado de cómo deben ser atacados, es por eso que se hace imprescindible que se siga trabajando para llegar a la unificación de los criterios y así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente.

4.5. Proyecto de creación del protocolo para el análisis de evidencia informática

Acuerdo del Consejo Directivo CD-INACIF-XX-XX

CONSIDERANDO:

Que el Instituto Nacional de Ciencias Forenses de Guatemala es la institución que por mandato constitucional le corresponde el aporte de la prueba científica y ha realizado

su mejor esfuerzo en materia de peritajes técnicos , para que todos y cada uno de los habitantes tengan acceso a los servicios que presenta la institución y que las conclusiones que plasman en el dictamen sea de acuerdo con los avances científicos, tecnológicos y que servirán para condenar o absolver a una persona o grupo de personas sea de acuerdos a una metodología actualizada respetando la dignidad humana.

CONSIDERANDO:

Que no obstante la importancia que ha tenido en nuestro país las ciencias forenses, no se puede obviar el hecho de que debería de existir un laboratorio de informática forense para investigar y aplacar de una manera frontal los delitos informáticos se hace necesario crear el protocolo adecuado para la recolección, preservación, análisis correspondiente de la evidencia informática.

POR TANTO:

En ejercicio de las atribuciones que le confiere el inciso f del Artículo ocho y los Artículos 47 y 19 de la Ley Orgánica del Instituto Nacional de Ciencias Forenses.

Acuerda

Crear el protocolo de recolección, preservación, manejo y análisis de evidencia informática:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Protocolo de recolección, preservación, manejo y análisis de la evidencia digital.

a) Recolección de los elementos físicos:

- Asegurar la escena del crimen y su respectiva documentación.

- Evaluar la escena del crimen.

- Aislar la escena del crimen, en ella se debe realizar un proceso de observación de la escena.

- Realizar las entrevistas preliminares de tal manera que se indague por la información y sobre todo de la escena bajo investigación, de igual manera, es necesario que estas actividades estén debidamente documentadas para no perder ningún indicio.

b) Documentación de la escena del crimen: Es necesario crear un registro completo y detallado para la investigación, buscando mantener la cadena de custodia que es de vital importancia para el proceso. Para este caso es posible el uso de:

- Toma de fotografía y/o video de la escena.

- Documentación de los componentes de la escena, describiendo cada uno de ellos.

- Etiquetar todos y cada uno de los componentes de la escena.

c) Recolección de la evidencia digital: Fase de mucho cuidado en la que los especialistas deben prestar mucha atención a la forma como la evidencia es recolectada, de tal manera que no afecten la integridad de la información que es almacenada a través de un medio digital o fuente donde se encuentra la información. Es necesario que:

- Se documente el estado en el que se encuentra el medio tecnológico, indispensable documentar si se encuentra apagado o encendido el medio tecnológico, puesto que de cada uno de estos estados se debe realizar una acción en particular.

- Tomar en caso de ser necesario la información más volátil del sistema, entre ellas están la información de la memoria y los procesos que se están ejecutando en caso de estar prendida la máquina y en operación normal.

d) Almacenamiento, transporte y embalaje de los indicios. Es necesario poseer las condiciones necesarias para el almacenamiento y transporte de los medios digitales, dado que condiciones como la humedad, la temperatura, las corrientes eléctricas y los campos magnéticos pueden alterar los medios de almacenamiento y por ende la información que allí se encuentra almacenada. En ellos es necesario garantizar:

- Etiquetado y marcado de los indicios identificados, con el objetivo de poder replicar en un ambiente controlado para su posterior análisis.

- Guardar los medios tecnológicos en embalajes que eviten los problemas con la estática.

- No transportar los indicios por largos períodos de tiempo, en este aspecto que salga de la escena del crimen directo para el laboratorio donde se realizar su posterior análisis.

- Se debe almacenar en un ambiente adecuado para ello, como son los laboratorios que se dispongan para investigar y analizar los componentes tecnológicos definidos.

e) Análisis de la información recolectada. En este momento en el proceso de la investigación, habla del análisis de la información ya recolectada. En esta fase fundamentalmente se busca extraer la información de los medios digitales identificados de tal forma que se pueda realizar la correspondiente reconstrucción de los eventos, y al final de ello, obtener unas conclusiones que deben ser remitidas en forma de informe en donde se sustenten los hallazgos identificados.

Dentro de este conjunto de actividades principalmente se tiene.

- Trabajar sobre una copia fiel y exacta del medio bajo investigación Esto requiere de las herramientas necesarias que permitan obtener el número de copias que sean necesarias, de tal manera que el medio original quede como evidencia, en caso de que se requiera restringir indagar sobre la veracidad del proceso.

- Proceder con la extracción de la información

Al proceder con la extracción de la información se puede:

- Utilizar más de una herramienta de extracción de información, con el objetivo de dar mayores garantías al proceso.

- Extraer información acerca del correo electrónico.

- Logs del sistema, ingresados al mismo.

- Identificación de volatilidad de la información más volátil a la menos volátil.

- Extracción de los datos y filtrado de los mismos.

- Identificar y recuperar datos que han sido: Eliminados, escondidos, cifrados, corruptos.

- Determinar líneas de tiempo o secuencia en que los eventos se presentaron.

- Evaluación del perfil del atacante.

- Construir un marco del caso en donde, de manera lógica y secuencial, se relaten los hechos identificados basados en los hallazgos.

f) Presentación e informes: Esta fase permite entregar un informe donde se presentan de manera ordenada los hallazgos encontrados, o las evidencias necesarias para soportar una investigación que se esté realizando. Dependiendo de la naturaleza de la investigación, si es de carácter interno, sólo intervienen las partes implicadas bien sea recursos humanos, directivas de la organización, e implicados, mientras en las investigaciones dentro de un proceso penal, donde intervienen entes judiciales intervendrán las partes como abogados defensores, jueces, fiscales, los reportes deben poseer las siguientes características:

- Una estructura que muestre de manera lógica la evolución de un caso investigado.

- No deben estar sujetos a juicios de valor por parte de quien redacta el reporte o generar parcialidad en el mismo, inclusive es necesario su revisión para evitar posibles inconsistencias.

- Debe ser claro, conciso, breve y simple, de tal forma que refleje sin rodeos lo que se desea mostrar.

- Es necesario que se utilice un lenguaje sencillo y claro para enlazar todos los eventos identificados.

- Los argumentos, en todos los casos, han de estar sustentados en los hallazgos identificados.

- Debe existir de manera clara la identificación del caso, fechas en que fue realizado el proceso y los procedimientos utilizados.

- Es necesario que de manera resumida se presenten los hallazgos encontrados, en caso de ser necesario se puede escribir un informe adicional con todos los detalles técnicos con los cuales se llevó a cabo el proceso de análisis de la evidencia.

- Es necesario que los reportes sean entregados en medios no modificables, ejemplo de ello puede ser formato PDF.

De igual manera un informe debe poseer como mínimo la siguiente estructura básica: Introducción: Quién solicitó el informe, qué se buscó, quién escribió el informe, cuándo y qué fue encontrado.

- Resumen de evidencias: Qué evidencias fueron examinadas, cuándo, de dónde y cuándo se obtuvieron las pruebas.

- Resumen de proceso: Qué herramientas fueron utilizadas, qué datos fueron recuperados.

- Examen de las evidencias: Archivos de logs, tráficos de red o archivos.

- Análisis: Descripción del o los análisis realizados.

- Conclusiones: Resumen que se enlace lógicamente y se refiera a todas las evidencias recolectadas.

- Glosario de términos: Explicación de los términos técnicos utilizados.

- Cierre: Esta última fase lo que busca es que en el lugar donde se revisó la información siga todos los protocolos definidos en cada una de las fases del análisis, de igual manera y siempre que sea posible se busca devolver las evidencias a sus respectivos dueños.

CONCLUSIÓN DISCURSIVA

La investigación surgió a partir de toda la información difundida tanto por medios de comunicación escrita como audiovisual, en donde claramente se percibe el problema, ya que el encargado de la persecución penal no cuenta con herramientas científicas como lo es el laboratorio de informática forenses y sus respectivos protocolos, siendo notorio que dicha falencia tiene trascendencia en la sociedad guatemalteca.

Con la entrada en vigencia de la Ley Orgánica del Instituto Nacional de Ciencias Forenses de Guatemala, se espera que en Guatemala se puede hacer uso de las ciencias forenses y criminalísticas en los procesos penales de acuerdo a los avances tecnológicos, ya que los mismas proporcionan al ente investigador medios de prueba, fortaleciendo la investigación del Ministerio Público, sin embargo a la fecha el INACIF no ha puesto en marcha el laboratorio de informática forense, con el objeto de aportar pruebas en el proceso penal en los delitos informáticos.

De acuerdo a lo anterior, el problema se solucionaría con la creación del laboratorio informática forense y protocolos para la recolección, preservación, manejo y análisis de la evidencia digital en la materia y así garantizar la aportación de prueba científica en el proceso penal.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C. A.

BIBLIOGRAFÍA

ARBULORA VALVERDE, Aristides. **La cadena de la custodia**. (s.e.) Ed: Marphasa Costa Rica, 2000.

BADILLA, Javier. **Curso de administración y procesamiento de la escena del crimen**. (s.e.) (s.E.) Escuela Judicial, sección de capacitación del Organismo de investigación, San José, Costa Rica; Costa Rica; 1999.

BENITEZ MENDIZABAL, Arquel. **La escena del crimen**. (s/e), Guatemala, 2004.

CAMACHO LASA, Luis. **El delito informático**. (s/e), España: S/E, 1990.

CABANELLAS DE LAS CUEVAS, Guillermo. **Diccionario de ciencias jurídicas políticas y sociales**. Buenos Aires: Ed. Heliasta, 1996.

CRISTÓBAL PAREJA, Ángel Andeyro, Manuel Ojeda, **Introducción a la Informática**, (s/e), (s.l.i.) 1994.

Diccionario ilustrado pequeño larousse, (s.l.i.) Ed. Printer Latinoamérica S.A., 1995.

GISPERT, Carlos. **Enciclopedia Autodidactica Interactiva**, 6° Edición, Ed: Océano. México, 2002.

HUERTA, Marcelo y LIBANO, Claudio. **Delitos informáticos**. Chile. Ed: Jurídica Cono Sur, 2007.

http://definicion.de/virus-informatico/**definición.de**. (Guatemala, 21 de enero de 2016).

http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf/**el delito informático**. (Guatemala, 25 de enero de 2016).

http://www.inacif.gob.gt/index.php?option=com/**inacif**. (Guatemala, 26 de enero de 2016).

http://www.inacif.gob.gt/index.php?option=com_content&view=article&id=59&Itemid=80 / **inacif**. (Guatemala, 26 de enero de 2016).

http://es.scribd.com/doc/31783656/INFORMATICA-JURIDICA-EN-VENEZUELA/**scribd**. (Guatemala, 26 de febrero de 2016).

http://www.rae.es/**real academia española** (Guatemala, 26 de enero de 2016).

http://www.dtj.com.ar/publicaciones.html/**el sitio del derecho**. (Guatemala, 26 de enero de 2016).

LÓPEZ CALVO, Pedro y Gómez Silva, Pedro. **Investigación criminal y criminalística**.

Colombia; Ed. Temis, S.A. Bogotá Colombia 2000.

MAGLIONA MARKOVICTH, Claudio Paúl, LÓPEZ MEDEL, Macarena, **Delincuencia y fraude informático**. Chile. Ed: Jurídica. 1999.

MANUAL DE PROCEDIMIENTOS DE CADENA DE CUSTODIA, Fiscalía General de la Nación Bogotá D.C. 2003.

MCCURDY, Jessica, **Computer Crime**, Bureau of Justice Statistics. (s/e). Estados Unidos de Norte America, 1981.

MEZA MÁRQUEZ, Miguel. **Manual de criminalística**. 3ª. Ed. Santa Fe de Bogotá Colombia; Ed. Librería del Profesional, 1991.

MONTIEL SOSA, **Juventino. Criminalística**. tomo I, México; Ed. Limusa, 1986.

MORENO CONZÁLEZ, L. Rafael. **Introducción a la criminalística**. México; Ed. Porrúa Av. República Argentina, 2002

MORALES TRUJILLO, Luis Javier y otros. **CCI Criminalística, criminología e investigación**, Ed: Sigma Editores, criminalística. Colombia, 2010.

MUÑOZ CONDE, Francisco y García Arán, Mercedes. **Manual de Derecho Penal Parte General.** 2ª edición. Ed: Tirant lo blanch. Valencia España, 1998.

OSSORIO, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**. Ed: Claridad, S.A. Buenos Aires, Argentina; 1984.

RESA NESTARES, Carlos. **Crimen organizado transnacional:** definición, causas y consecuencias.Ed: Astrea. Colombia, 2005.

REYES CALDERON, José Adolfo. **Selecciones criminalísticas**. Guatemala; Ed. Departamento de Producción Tipografía Nacional de Guatemala 2003.

REYES CALDERÓN, José Adolfo. **Técnicas Criminalísticas para el Fiscal.** Fiscalía General de la República. Ministerio Público, Guatemala 1993.

ROMEO CASABONA, Carlos María. **Poder informático y seguridad jurídica**. Fundesco. Madrid, España, 1987.

SANDOVAL SMART, L. **Manual de criminalística.** Santiago de Chile; Ed. Jurídica de Chile, 196

Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1986.

Convenio sobre la ciberdelincuencia de la Unión Europea. Budapest, Hungría, noviembre 2,001.

La Convención de las Naciones Unidas contra la delincuencia organizada. Nueva York, Estados Unidos, 2,004.

Ley del Organismo Judicial. Decreto número 2-89 del Congreso de la República de Guatemala, 1989.

Código Procesal Penal. Decreto número 52-92 del Congreso de la República de Guatemala, 1992.

Código Penal. Decreto número 17-73 del Congreso de la República de Guatemala, 1973.

Ley Orgánica del Ministerio Público, Decreto número, 90-94 del Congreso de la República de Guatemala, 1994.

Ley Orgánica del Instituto Nacional de Ciencias Forenses de Guatemala. Congreso de la República de Guatemala, Decreto número 32 -2006, 2006.

Ley de Acceso a la Información Pública, Decreto número 57-2008 del Congreso de la República de Guatemala, 2,008.