

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

**“EL PERITAJE DE LOS DELITOS INFORMÁTICOS, APLICACIÓN
Y AVANCES EN GUATEMALA”**

HERLINDO DE JESÚS OSORIO VILLAGRES

GUATEMALA, FEBRERO DE 2012

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

**EL PERITAJE DE LOS DELITOS INFORMÁTICOS, APLICACIÓN
Y AVANCES EN GUATEMALA**

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

Herlindo de Jesús Osorio Villagres

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, febrero de 2012

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

DECANO: Lic. Bonerge Amilcar Mejía Orellana
VOCAL I: Lic. Avidán Ortiz Orellana
VOCAL II: Lic. Mario Ismael Aguilar Elizardi
VOCAL III: Lic. Luis Fernando López Díaz
VOCAL IV: Br. Modesto José Eduardo Salazar Dieguez
VOCAL V: Br. Pablo José Calderón Gálvez
SECRETARIO: Lic. Marco Vinicio Villatoro López

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente: Lic. Luis Alfredo González Ramila
Vocal: Lic. Edgar Manfredo Roca Canet
Secretario: Lic. Luis Emilio Gutiérrez Cambranes

Segunda Fase:

Presidente: Lic. Obdulio Rosales Dávila
Vocal: Lic. Marco Tulio Pacheco Galicia
Secretario: Lic. Rodolfo Giovanni Celis López

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).



**CASTILLO & CASTILLO
ABOGADOS Y NOTARIOS**

**Lic. Edgar Armindo Castillo Ayala
Colegiado No. 6,220**

**3ª. Avenida 13-62 zona 1, Ciudad de Guatemala
Teléfono: 2232-7936**

Guatemala, 22 de julio 2010.

Licenciado

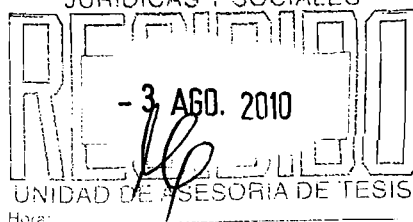
Marco Tulio Castillo Lutín

Jefe de la Unidad de Asesoría de Tesis

Facultad de Ciencias Jurídicas y Sociales

Universidad de San Carlos de Guatemala

Su Despacho.



Licenciado Castillo:

Como Asesor de Tesis del Bachiller **HERLINDO DE JESÚS OSORIO VILLAGRES**, para la realización de su trabajo titulado **“EL PERITAJE DE LOS DELITOS INFORMÁTICOS, APLICACIÓN Y AVANCES EN GUATEMALA”**, me complace hacer constar sobre dicho trabajo lo siguiente:

1. El contenido del trabajo comprende consideraciones generales sobre el avance informático, los delitos informáticos, su definición, clasificación, características, elementos personales y la posición de nuestra legislación en la materia, la informática forense como ciencia auxiliar de la criminalística, el perito informático y su actuación en este tipo de delitos, y un panorama general de la legislación guatemalteca sobre los delitos informáticos y la situación actual del peritaje informático, finalizando con una propuesta de modificación de la normativa penal en relación al tema y de la creación de un protocolo para recabar y analizar la evidencia informática para su uso como medio probatorio en el juicio penal, considerando que él mismo fue abordado técnica y científicamente.
2. Durante el trabajo de investigación, se utilizaron los métodos inductivo, analítico y sintético, que permitieron formular la propuesta citada, utilizando como técnicas el análisis, selección y recopilación de datos bibliográficos y documentales, la legislación nacional sobre el tema y el estudio comparado de legislación internacional.
3. El trabajo de tesis se encuentra redactado en forma clara, amplia y comprensible, utilizando un adecuado lenguaje técnico y científico, lo cual hace fácil su comprensión.
4. Como producto del análisis realizado de la normativa vigente sobre el tema, el Bachiller Osorio Villagres, realiza una propuesta concreta de modificación de la normativa penal en relación al tema, a fin de adecuar dicha normativa al desarrollo



**CASTILLO & CASTILLO
ABOGADOS Y NOTARIOS**

**Lic. Edgar Armindo Castillo Ayala
Colegiado No. 6,220**

**3ª. Avenida 13-62 zona 1, Ciudad de Guatemala
Teléfono: 2232-7936**

conceptual de los delitos informáticos y de la necesidad de creación de un protocolo para recabar y analizar la evidencia informática para su uso viable y confiable como medio de prueba en el juicio penal, siendo esta la contribución científica del presente trabajo de investigación.

5. Con el Bachiller Osorio Villagres, se convino que para la realización de su estudio, era necesario efectuar algunos cambios en el Plan de Investigación que originalmente se había aprobado, tomando en consideración la naturaleza y alcance del citado trabajo.
6. El trabajo plantea fundamentalmente la problemática que existe en la normativa penal vigente en materia de los delitos informáticos y los procedimientos para su investigación, por lo que se considera que las conclusiones y recomendaciones a las que se llegó con la investigación realizada, son acordes a la problemática planteada.
7. Se considera que la bibliografía utilizada en el presente trabajo de investigación, es la apropiada, tomando en consideración el tema propuesto y como fue abordado el mismo.

He guiado personalmente al sustentante durante las etapas del proceso de investigación científica, aplicando los métodos y técnicas apropiadas para resolver la problemática esbozada; con lo cual comprueba la hipótesis planteada conforme a la proyección científica de la investigación.

El trabajo de tesis en cuestión, reúne los requisitos que exige el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, razón por la cual, emito **DICTAMEN FAVORABLE**, a efecto de que él mismo puede continuar con el trámite correspondiente, para su posterior evaluación por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales y los títulos profesionales de Abogado y Notario.

Atentamente,

Edgar Armindo Castillo Ayala
Abogado y Notario

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Ciudad Universitaria, zona 12
Guatemala, C. A.



UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS Y SOCIALES. Guatemala, 5 de agosto de dos mil diez.

Atentamente, pase al (a) **LICENCIADO (A) AMPARO ROXANA GIRÓN LIMA**, para que proceda a revisar el trabajo de tesis del (de la) estudiante **HERLINDO DE JESÚS OSORIO VILLAGRES**, Intitulado: **"EL PERITAJE DE LOS DELITOS INFORMÁTICOS, APLICACIÓN Y AVANCES EN GUATEMALA."**

Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que tengan por objeto mejorar la investigación, asimismo, del título de trabajo de tesis. En el dictamen correspondiente debe hacer constar el contenido del Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, el cual dice: "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, su opinión respecto del contenido científico y técnico de la tesis, la metodología y las técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que estime pertinentes".


LIC. MARCO TULIO CASTILLO LUTÍN
JEFE DE LA UNIDAD ASESORÍA DE TESIS



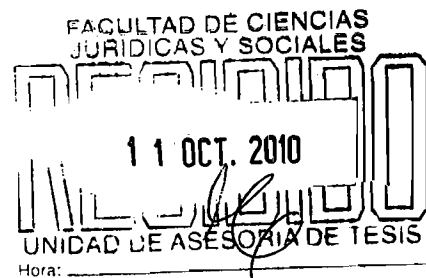
cc.Unidad de Tesis
MTCL/ ell.

Licda. Amparo Roxana Girón Lima
Abogada y Notaria
Colegiada No. 6,235
7ª. Av. 20-36 zona 1 Oficina No. 33
Teléfono: 2232-3546



Guatemala, 8 de octubre de 2010.

Licenciado
Marco Tulio Castillo Lutín
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Su Despacho.



Licenciado Castillo:

De manera respetuosa me dirijo a usted, en mi calidad de Revisor del trabajo de Tesis del Bachiller HERLINDO DE JESÚS OSORIO VILLAGRES, titulado "EL PERITAJE DE LOS DELITOS INFORMÁTICOS, APLICACIÓN Y AVANCES EN GUATEMALA", en tal sentido, me permito rendir mi dictamen sobre dicho trabajo en la forma siguiente:

1. La investigación realizada por el bachiller Osorio Villagres, fue desarrollada sobre la problemática que actualmente comprende el progreso de las técnicas informáticas y el consiguiente desarrollo de los hechos delictivos que afectan los procesos informáticos, manejando como tema central el peritaje en los delitos informáticos y planteando la necesidad de la informática forense como ciencia auxiliar de la criminalística; proponiendo la necesidad de regularizar la participación del perito informático y los procedimientos de recabar y analizar la evidencia en este tipo de delitos; en tal sentido se considera que la investigación fue realizada técnica y científicamente, en virtud del alcance y profundidad con que se abordó el tema.
2. Se pudo determinar mediante la revisión del trabajo de investigación que en el proceso de la misma fueron utilizados los métodos inductivo, analítico y sintético, lo cual permitió verificar la hipótesis planteada; habiéndose determinado también, que se utilizaron las técnicas del análisis, selección y recopilación de datos bibliográficos y documentales, y que se realizó un particular análisis de la legislación nacional y del derecho comparado.

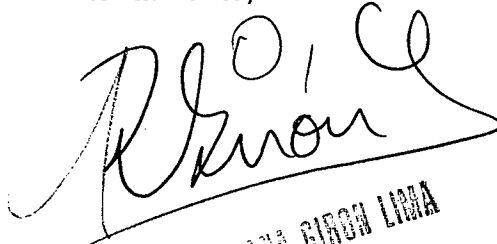
Licda. Amparo Roxana Girón Lima
Abogada y Notaria
Colegiada No. 6,235
7ª. Av. 20-36 zona 1 Oficina No. 33
Teléfono: 2232-3546



3. En el desarrollo temático del trabajo de tesis, se puede determinar que el mismo ha sido redactado con lenguaje técnico y científico, lo que permite una fácil comprensión del tema que se esta abordando y de las conclusiones a las que se arriba.
4. El Bachiller Osorio Villagres, realiza una propuesta concreta de modificación de la normativa penal en relación a los delitos informáticos; como producto del análisis realizado de la normativa vigente. Dicha propuesta persigue como fin que se adecue dicha normativa al desarrollo doctrinario que han alcanzado los delitos informáticos. Plantea además la propuesta de crear un protocolo a fin de que los procesos mediante los cuales se recaba y analiza la evidencia informática, sean seguros y garanticen el uso viable y confiable como medio de prueba en el juicio penal. En tal razón, se considera que el presente trabajo de investigación presenta una contribución científica dentro del tema de los delitos informáticos y los medios de su investigación.
5. Se considera que las conclusiones y recomendaciones a las que se arribó mediante el trabajo de investigación realizado, son acordes a la problemática planteada, y que la profundidad con que el tema fue analizado ha permitido llegar a dichas conclusiones.
6. Conforme la revisión realizada, se considera que la bibliografía que utilizó el Bachiller Osorio Villagres, en la realización de su trabajo de investigación, de conformidad con el tema propuesto fue la apropiada.

Se ha logrado determinar que la investigación realizada, reúne los requisitos que exige el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, en virtud de lo cual no existe objeción para emitir DICTAMEN FAVORABLE, a efecto de que se continúe con el trámite correspondiente, para su posterior evaluación por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales y los títulos profesionales de Abogado y Notario.

Atentamente,



LIC. AMPARO ROXANA GIRÓN LIMA
ABOGADO Y NOTARIO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Edificio S-7, Ciudad Universitaria
Guatemala, C. A.



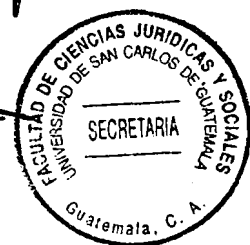
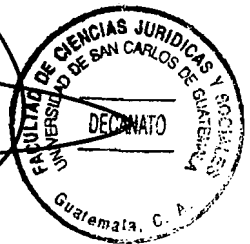
DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES.

Guatemala, diez de junio del año dos mil once.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante HERLINDO DE JESÚS OSORIO VILLAGRES, Titulado EL PERITAJE DE LOS DELITOS INFORMÁTICOS, APLICACIÓN Y AVANCES EN GUATEMALA.

Artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.-

CMCM/slh.





DEDICATORIA

- A DIOS:** Por darme la bendición de culminar esta noble profesión, y porque seguirá guiando mis pasos.
- A MIS PADRES:** Herlindo Osorio Morales y Marta Villagres de Osorio, quienes con su ayuda, amor y comprensión facilitaron la culminación de mi profesión.
- A MI HERMANA:** Ingrid, por su apoyo incondicional en todo momento.
- A MIS ABUELOS:** Por la sabiduría que me brindaron desde mi niñez, especialmente a mi abuelo Felipe (+).
- A MIS TIOS:** Juan, Filiberto, Carmelino, Felipa, María y Ana.
- A MIS PRIMOS:** Walter y Juan Carlos.
- A MI NOVIA:** Miriam, gracias por tu apoyo, ayuda y paciencia para poder lograr este éxito.
- A MIS AMIGOS:** Estuardo Morales, José López, Gustavo Caballeros, Ramiro Robles (+), Sergio Márquez, Geovanni Estrada, Rudy Ordoñez y especialmente al Lic. Roberto Figueroa.
- A MIS CATEDRÁTICOS:** Por compartir sus conocimientos con los cuales puede forjar esta profesión, en especial a los licenciados Ricardo Alvarado y Edgar Castillo por su amistad y apoyo.
- A MI TRABAJO:** Por proveerme de los recursos necesarios para sustentar mi profesión.
- A MI ASESOR Y REVISOR DE TESIS:** Por dedicarse a guiarme en la realización de este trabajo de tesis.
- A MIS PADRINOS:** Por la admiración que me inspiran y el ejemplo a seguir.
- A:** La tricentaria y gloriosa Universidad de San Carlos de Guatemala, en especial a la Facultad de Ciencias Jurídicas y Sociales.



ÍNDICE

	Pág.
Introducción.....	i

CAPÍTULO I

1. Los delitos informáticos.....	1
1.1. Consideraciones previas sobre la informática.....	2
1.2. Definición de los delitos informáticos.....	3
1.3. El bien jurídico tutelado en los delitos informáticos.....	7
1.4. Sujetos del delito informático.....	11
1.5. Características de los delitos informáticos.....	19
1.6. Clasificación de los delitos informáticos.....	20
1.7. Los piratas informáticos o <i>hackers</i>	26
1.8. Infracciones que no constituyen delitos informáticos.....	28
1.9. Los delitos informáticos en la legislación guatemalteca.....	28

CAPÍTULO II

2. La informática forense como ciencia auxiliar de la criminalística	33
2.1. La criminalística como disciplina auxiliar del Derecho Penal.....	34
2.2. Principios doctrinarios de la criminalística y sus ciencias auxiliares.....	35

2.3. La informática forense como ciencia auxiliar de la criminalística..... 36

2.4. Principios de la ciencia informática forense..... 38

2.5. La evidencia informática..... 40

CAPÍTULO III

3. El perito informático..... 49

3.1. La actividad pericial..... 50

3.2. El rol del perito informático en la recuperación de evidencia..... 53

3.3. Perfil del perito informático..... 55

3.4. Impedimentos del perito informático..... 59

3.5. El informe pericial..... 60

3.6. Deberes del perito informático..... 62

3.7. Tipos de responsabilidad del perito informático..... 62

CAPÍTULO IV

4. El análisis forense informático..... 65

4.1. Las fases del análisis forense informático..... 66

4.2. Determinar la relevancia de la evidencia..... 88

4.3. Evaluación de los procedimientos realizados en la investigación..... 89

4.4. Dificultades del investigador forense..... 90

CAPÍTULO V

5. Panorama general de la legislación guatemalteca sobre los delitos informáticos y la situación actual del peritaje informático.....	91
5.1. La persecución penal de los delitos informáticos en la legislación de Guatemala.....	91
5.2. La competencia en la función de peritaje de conformidad con la legislación guatemalteca.....	94
5.3. La metodología de la investigación del Ministerio Público en los delitos informáticos.....	98
5.4. El procesamiento de la escena del crimen en los delitos informáticos.....	100
5.5. Inconvenientes en la investigación y el proceso pericial ante los delitos informáticos.....	103
CONCLUSIONES.....	113
RECOMENDACIONES.....	115
BIBLIOGRAFÍA.....	117



INTRODUCCIÓN

El presente trabajo muestra la problemática del delito informático y la forma en que debe ser investigado. El progreso de los sistemas computacionales permite procesar y poner a disposición de la sociedad una cantidad creciente de información; junto al avance de la tecnología informática, han surgido una serie de comportamientos ilícitos denominados delitos informáticos. Es patente el daño que estos delitos pueden causar al nuevo estilo de vida y la necesidad de tipificar determinadas conductas, a fin de que sean efectiva y positivamente perseguidas y castigadas. Este tema ha sido abordado por la legislación guatemalteca inapropiadamente, lo que provoca que muchas conductas delictivas queden fuera de sanción penal además estos delitos son investigados inadecuadamente, ya que por tratarse de una materia tan especializada, debiesen de existir procedimientos preestablecidos de recuperación y análisis de la evidencia que permitan la confiabilidad y validación de esta como medio de prueba.

Como objetivos de la investigación se planteó determinar cuáles son los avances de los peritajes informáticos en la investigación realizada por el Ministerio Público, establecer si los investigadores poseen conocimientos actualizados, si los dictámenes periciales informáticos se incorporan al proceso penal y su eficacia probatoria. En la investigación se formularon como supuestos, que la ciencia forense es sistemática, se basa en hechos premeditados para recabar prueba para análisis; que la informática forense es un conjunto de técnicas especializadas con el fin de reconstruir hechos pasados basados en datos recolectados; y que el investigador forense debe tener experiencia en comunicación de datos y el apoyo de técnicos de software.



El resultado del trabajo se plasmó de la forma siguiente: capítulo I “Los delitos informáticos”, trata de la evolución de la técnica informática, definición de delitos informáticos, el bien jurídico, sujetos y características del delito, clasificación doctrinaria y jurídica; el capítulo II, “La informática forense como ciencia auxiliar de la criminalística”, plantea lo referente a la criminalística y la informática forense como ciencia auxiliar de la criminalística, la evidencia informática, características y admisibilidad; el capítulo III, “El perito informático”, se refiere a la actividad pericial, el rol del perito informático, perfil, requisitos, impedimentos, obligaciones, responsabilidades y el Informe Pericial; el capítulo IV, “El análisis forense informático”, se refiere a la actividad y procedimientos del perito forense; el capítulo V, denominado “Panorama general de la legislación guatemalteca sobre los delitos informáticos y la situación actual del peritaje informático”, que sintetiza el contenido de los capítulos anteriores y realiza un análisis de la situación guatemalteca.

Se utilizaron los métodos inductivo, analítico y sintético además de técnicas como el análisis, selección y recopilación de datos bibliográficos y documentales, la legislación guatemalteca sobre el tema y el estudio comparado de legislación internacional.

Se considera que el presente trabajo es de utilidad para la sociedad guatemalteca, el Ministerio Público, el Instituto Nacional de Ciencias Forenses de Guatemala y para los peritos informáticos, ya que explica las modificaciones legales propuestas, se adecua y actualiza la normativa penal sobre los delitos informáticos garantizando una protección a los bienes jurídicos protegidos de este tipo de delitos.



CAPÍTULO I

1. Los delitos informáticos

La informática esta hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos se realizaban manualmente.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica delitos informáticos, los cuales podrían definirse como toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas. La dependencia de la sociedad a las nuevas tecnologías de la información y de las comunicaciones, hace patente el grave daño que los llamados delitos informáticos o la delincuencia informática pueden causar a nuestro nuevo estilo de vida. De esta cuenta, cobra importancia la seguridad con la que han de contar los equipos informáticos y las redes telemáticas, con el fin y objeto de poner obstáculos y luchar con dichas conductas delictivas, y la necesidad de tipificar y reformar determinadas conductas, a fin de que estas sean efectiva y positivamente perseguidas y castigadas en el ámbito penal. En igual forma, deben de desarrollarse los procedimientos técnicos de la recolección de evidencia en este tipo de delitos, a efecto de garantizar la certeza de los medios de prueba aportados a los procesos penales que se instauren por estas infracciones.



1.1. Consideraciones previas sobre la informática

Es incuestionable la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc; son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación y condiciona el desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad, a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados.

En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos. Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la era de la información.

1.2. Definición de los delitos informáticos

“El aspecto más importante de la informática radica en que la información ha pasado a convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después”¹.

Paralelamente al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a

¹ Magliona Markovitch, Claudio Paúl y López Medel, Macarena. **Delincuencia y Fraude Informático**, pág. 37.

aplicaciones analógicas prohibidas por el principio de legalidad. La doctrina ha denominado a este grupo de comportamientos, de manera genérica, delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática.

En tal sentido y de conformidad con lo que señalan Claudio Magliona y Macarena López, “existe una confusión terminológica y conceptual presente en todos los campos de la informática, especialmente en relación con sus aspectos criminales, por eso es necesario aclarar el intrincado debate doctrinario acerca del contenido real de lo que se ha dado en llamar los delitos informáticos. En tal sentido, debe existir la claridad más absoluta respecto de las materias, acciones y omisiones sobre las que debe recaer la seguridad social que aporta el aparato punitivo del estado”.²

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios. En el caso de la legislación guatemalteca, el Código Penal en su Libro Segundo, Título VI Delitos contra el patrimonio, Capítulo VII, se refiere a los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos, en este sentido el criterio utilizado en la legislación guatemalteca, es el de diferenciar este tipo de delitos, de los delitos tradicionales.

²Ibid., pág. 45.

Nidia Callegari define al delito informático como “aquel que se da con la ayuda de la informática o de técnicas anexas”.³ Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también que lo informático puede ser el objeto de la infracción.

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiéndolo por la primera a “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin”,⁴ y por la segunda “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”.⁵

María Cinta Castillo y Miguel Ramallo entienden que “delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas”.⁶

Partiendo de esta compleja situación y tomando como referencia el Convenio de Ciberdelincuencia del Consejo de Europa, se definen los delitos informáticos como los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.

³ Callegari, Nidia. **Poder informático y delito**, pág. 59.

⁴ Téllez Valdés, Julio. **Los Delitos informáticos. Situación en México**, pág. 121.

⁵ *Ibid.*, pág. 122.

⁶ Castillo Jiménez, María Cinta y Ramallo Romero, Miguel. **El delito informático**, pág. 23.

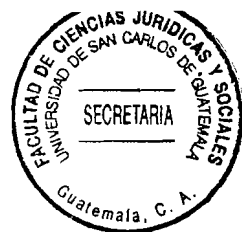


Se puede decir además, que a estas definiciones, que de una manera u otra son vagas, en cuanto no presentan una concreta delimitación de las fronteras en la que pueden producirse los delitos informáticos, desde un punto de vista estrictamente jurídico; tampoco establecen con claridad los efectos susceptibles de punibilidad de los delitos informáticos, toda vez que se establecen conductas del agente sin referencia precisa a la necesidad o no de resultados y cuales serian éstos.

Por su parte Benjamín Salt, sostiene que “el concepto de delitos informáticos abarca un conjunto de conductas de distintas características, que afectan bienes jurídicos diversos y que sólo son agrupadas bajo este concepto por su relación con el ordenador”.⁷ Esta amplitud del concepto, determina que a los fines del análisis jurídico, sea un concepto sin contenido propio, que sólo puede ser adquirido con la descripción concreta de las distintas conductas que abarca.

En tal sentido, analizando el ordenamiento jurídico guatemalteco vigente, referente a esta materia, se puede decir que el término de delito informático, no constituye por sí mismo una categoría delictiva sino que se trata de usos indebidos de cualquier medio informático. En general, para gran parte de la doctrina no existe un delito informático, sino una realidad criminal compleja, vinculada a las nuevas técnicas de información, imposible de ser incluidas en un único tipo legal.

⁷ Salt, G. Marcos. **Informática y delitos**, <http://www.derecho.org.ar> (16 de diciembre de 2009)



1.3. El bien jurídico tutelado en los delitos informáticos

En términos generales, el bien jurídico tutelado es el bien o valor lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir, ya que constituye la razón de ser del delito, y no suele estar expresamente señalado en los tipos penales. El bien jurídico tutelado nace de una necesidad de protección y se torna penal sólo si reviste una importancia fundamental, o sea cuando las condiciones sociales a proteger sirvan de base a la posibilidad de participación de los individuos en la sociedad. Se debe tomar en cuenta que para recabar en forma adecuada la evidencia que compruebe la comisión de los delitos informáticos, es necesario que se tenga bien claro cuál es el bien jurídico que se tutela en este tipo de delitos.

Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

Actualmente se presume que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por



ejemplo entre la propiedad tangible y la intangible. Esto por cuanto la información no puede ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que la información y otros intangibles son objetos de propiedad, la cual de conformidad con la Constitución guatemalteca vigente, esta protegida, y debe definirse como un bien vital, perteneciente a la comunidad o al individuo, que por su significación, es garantizada, a través del poder punitivo del Estado.

En tal sentido, la protección de la información como bien jurídico protegido, debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señalan que la penalización de conductas se desenvuelva en el marco del principio de lesividad. Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada.

Para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir “que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo”.⁸ En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos.

⁸ Magliona Markovitch, Claudio Paúl y López Medel, Macarena, op. cit., pág. 68.

Al tenor de este criterio podemos decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos; María Luz Gutiérrez Francés, respecto de la figura del fraude informático nos dice que: “las conductas de fraude informático presentan indudablemente un carácter pluriofensivo. En cada una de sus modalidades se produce una doble afección: la de un interés económico, como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macrosocial vinculado al funcionamiento de los sistemas informáticos”.⁹

Por lo cual, se puede indicar que el bien jurídico protegido en general es la información, pero está debe ser considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente, por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

- a. El patrimonio, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.
- b. La reserva, la intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.
- c. La seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

⁹ Gutiérrez Francés, María Luz. **Fraude informático y estafa**, pág. 86.

- d. El derecho de propiedad, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el llamado terrorismo informático.

En tal sentido, el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Por tanto, el nacimiento de la tecnología informática, está proporcionando nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.); sin embargo, han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa. Por tal razón se puede considerar que este tipo de conductas criminales son de carácter netamente pluriofensivo.

Un ejemplo que puede aclarar esta afirmación, es el de un hacker que ingresa a un sistema informático con el fin de vulnerar la seguridad de este y averiguar la información que más pueda sobre una determinada persona, esto en primer lugar podríamos decir que el bien jurídico lesionado o atacado es el derecho a la intimidad que posee esa persona, al ver que su información personal es vista por un tercero extraño, que sin autorización ha vulnerado el sistema informático donde dicha información está contenida. Pero detrás de ese bien jurídico encontramos otro bien colectivo que



conlleva a un ataque a la confianza en el funcionamiento de los sistemas informáticos. Es decir, de intereses socialmente valiosos que se ven afectados por estas nuevas figuras, y que no solo importan la afección de bienes jurídicos clásicos.

1.4. Sujetos del delito informático

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido, como quedó establecido anteriormente, será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, “el titular del bien jurídico lesionado será el sujeto pasivo, quien puede ser distinto del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. Por otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo”.¹⁰

a) Sujeto activo

De acuerdo al profesor chileno Mario Garrido Montt, “se entiende por sujeto activo a quien realiza toda o una parte de la acción descrita por el tipo penal. 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 generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información

¹⁰ Huerta Miranda, Marcelo y Libano Manzur, Claudio. *Los delitos informáticos*, pág. 47.

de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos".¹¹

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, "la persona que entra 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".¹² Al respecto, según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos, "el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada (insiders). Asimismo, recientes estudios realizados en América del Norte y Europa indicaron que el 73% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa (outsiders)".¹³

Actualmente el nivel típico de aptitudes del delincuente informático, es tema de controversia, ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática, en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico,

¹¹ Garrido Montt, Mario. **Nociones fundamentales de la teoría del delito**, pág. 59.

¹² Ramírez Bejerano y Aguilera Rodríguez. **Los delitos informáticos. Tratamiento internacional, en contribuciones a las Ciencias Sociales, mayo 2009.** www.eumed.net/rev/cccss/04/rbar2.htm. (15 de enero 2010).

¹³ **Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, abril 2000,** <http://www.uncjin.org/Documents/congr10/10s.pdf>, (23 de noviembre 2010).

características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos; estudiosos en la materia los han catalogado como delitos de cuello blanco, término introducido por el criminólogo Edwin Sutherland en el año de 1943, quien señala una serie de conductas que considera como delitos de cuello blanco, aún cuando muchas de estas conductas no están tipificadas como delitos. Asimismo, este criminólogo dice que tanto la definición de los delitos informáticos, como la de los delitos de cuello blanco, no está de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: “el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.”¹⁴

Tiedemann, frente a esta definición nos dice “de manera creciente, en la nueva literatura angloamericana sobre estos temas se emplea el término “hecho penal profesional” (occupational crime). Con esta referencia al papel profesional y a la actividad económica, la caracterización del delito económico se fundamenta ahora

¹⁴ Sutherland, Edwin, Citado por Tiedemann Klaus. **Poder económico y delito**, pág. 143.

menos en la respetabilidad del autor y su pertenencia a la capa social alta y más en la peculiaridad del acto (modus operandi) y en el objetivo del comportamiento”¹⁵.

A este respecto Marcelo Huerta y Claudio Libano dicen que “en lo relativo a tratarse de “ocupacional crimes”, es cierto que muchos de los delitos se cometen desde dentro del sistema por personas que habitualmente lo operan y que tienen autorizado los accesos (insiders). Sin embargo, las tendencias modernas apuntan hacia el campo de la teleinformática a través del mal uso del ciberespacio y las supercarreteras de la información o redes de telecomunicaciones. Es decir, cada día gana más terreno el delito informático a distancia. (outsiders)”¹⁶.

No es fácil descubrir y sancionar este tipo de delitos, en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos respetables.

En el caso de los delitos informáticos tiene relación con lo que se ha dado en llamar el síndrome de Robín Hood, es decir a “la creencia en cierto modo patológica, de que mientras que robar a una persona física que tiene sus problemas y necesidades materiales como todo hijo de vecino es un hecho inmoral e imperdonable, robar a una

¹⁵ Huerta Miranda, Marcelo y Libano Manzur, Claudio, op. cit., pág. 88.

¹⁶ Huerta Miranda, Marcelo y Libano Manzur, Claudio, op. cit., pág. 59.

institución como la banca que gana decenas de miles de millones al año es casi un acto social que contribuye a una más justa distribución de la riqueza”¹⁷.

Como sostiene Gutiérrez Francés, “con carácter general, la delincuencia mediante computadoras se inscribe dentro de las formas de criminalidad de *cuello blanco*, propias de la delincuencia económica, por lo cual desde el punto de vista criminológico, presentan las mismas peculiaridades que ésta, con las notas específicas que aporta lo informático”.¹⁸

Por otro lado, se puede considerar que a pesar que los delitos informáticos, no poseen todas las características de los delitos de cuello blanco, si coinciden en un número importante de ellas, por tanto diremos que la calidad del sujeto activo no es un elemento determinante en la delincuencia informática. Sólo algunos delitos, como los cometidos por los hackers propiamente dichos, podrán considerarse como realizados por un sujeto altamente calificado. Los más, no requieren, en cuanto al sujeto, calificación, ya que pueden cometerse por personas que recién se inician en la informática o por niños que están aprendiendo individualmente en sus hogares.

A este respecto el jurista mexicano Jorge Lara Rivera, nos dice que “tradicionalmente se ha considerado que este tipo de delitos se encuadra dentro de los llamados *delitos de cuello blanco* debido a que se requiere que el sujeto activo tenga un conocimiento especializado en informática. Ahora bien, no podemos negar que la

¹⁷ Camacho Losa, Luís. **El delito informático**, pág. 98.

¹⁸ Gutiérrez Francés, María Luz, *op cit.*, pág. 97.

especialización informática facilita a los sujetos a incidir criminalmente por medio de las computadoras. Sin embargo, el mundo de la computación se va convirtiendo paulatinamente en un área común y corriente, gracias a la facilidad con la que los modernos sistemas y programas pueden ser controlados”¹⁹.

En este sentido, también se puede ubicar como sujeto activo de un delito cibernético a un lego en la materia o a un empleado de un área no informática que tenga un mínimo conocimiento de computación.

Concluyendo, se puede decir que las personas que pueden cometer 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 generalmente por su situación laboral, se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Dentro de las personas que poseen estas características se puede encontrar:

- Operadores, que se pueden poner en relación con el Sistema para modificar, agregar, eliminar, sustituir información y/o programas, copiar archivos para venderlos a competidores.
- Programadores, que pueden violar o inutilizar controles protectores del programa y/o sistema; dar información a terceros ajenos a la empresa, atacar el sistema operativo, sabotear programas, modificar archivos, acceder a información confidencial.

¹⁹ Lara Rivera, Jorge. **Los delitos informáticos**, [http:// www.jusrismática.com](http://www.jusrismática.com). (18 de diciembre 2009)

- **Analistas de sistemas, que pueden entrar en colusión con usuarios, programadores y/u operadores para revelarles la operación de un sistema completo.**
- **Analistas de comunicaciones, que enseñan a otras personas la forma de violar la seguridad del sistema de comunicaciones de una empresa, con fines de fraude.**
- **Supervisores, que pueden en razón de su oficio manipular los archivos de datos y los ingresos y salidas del sistema.**
- **Personal técnico y de servicio, que por su libertad de acceso al centro de cómputo puede dañar el sistema operativo.**
- **Ejecutivos de la computadora, que pueden actuar en situación de colusión con otras personas.**
- **Audidores, que pueden actuar como los anteriores.**
- **Bibliotecarios de preparación, que pueden vender la documentación.**
- **Bibliotecarios de operaciones, que pueden destruir información mediante errores o pueden venderla a competidores.**
- **Personal de limpieza, mantenimiento y custodia, que pueden vender el contenido de los costos de papeles, fotocopiar documentos, sabotear el sistema.**
- **Usuarios, que pueden modificar, omitir o agregar información con fines fraudulentos.**

Hay que tomar en cuenta también, que algunos de los hechos punibles previstos jurídicamente pueden ser perpetrados por intermedio de una persona jurídica o con el fin que ésta reciba sus efectos o beneficios, se establecerían entonces los supuestos que harían procedente su responsabilidad, es así que los gerentes, administradores,



directores o dependientes, actuando en su nombre o representación, responderán de acuerdo con su participación en el hecho punible.

b) Sujeto pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. En primer término hay que distinguir que sujeto pasivo ó víctima del delito 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 víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

Se hace 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 autoridades para comprender, investigar y aplicar el 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.

Esta problemática ha llevado a que los organismos internacionales hayan adoptado resoluciones en el sentido de que educando a la comunidad de víctimas y estimulando

la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

En igual forma, este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas, además de que en algunos países no existe legislación alguna sobre esta clase de conductas ilícitas, lo que empeora más la situación de las víctimas de estas conductas ilícitas.

1.5. Características de los delitos informáticos

Según el mexicano Julio Téllez Valdés²⁰, los delitos informáticos presentan las siguientes características principales:

- a) Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

²⁰ Tellez Valdés, Julio. **Derecho informático**, pág. 129.

- c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- d) Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que las realizan.
- e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- i) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

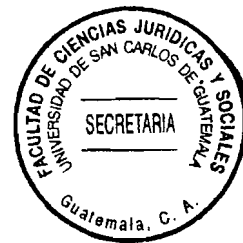
1.6. Clasificación de los delitos informáticos

De las clasificaciones doctrinales de los delitos informáticos, según nuestro criterio la más completa es la presentada por el autor mexicano Julio Téllez Valdés²¹ quien clasifica a estos delitos, de acuerdo a los criterios siguientes:

1. Como Instrumento o medio: En esta categoría el autor citado ubica las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, y señala como ejemplos los siguientes:

²¹Ibíd., pág. 96.

- a. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).
 - b. Variación de los activos y pasivos en la situación contable de las empresas.
 - c. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).
 - d. Lectura, sustracción o copiado de información confidencial.
 - e. Modificación de datos tanto en la entrada como en la salida.
 - f. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
 - g. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
 - h. Uso no autorizado de programas de cómputo.
 - i. Introducción de Instrucciones que provocan interrupciones en la lógica interna de los programas.
 - j. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
 - k. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
 - l. Acceso a áreas informatizadas en forma no autorizada.
 - m. Intervención en las líneas de comunicación de datos o teleproceso.
2. Como fin u objetivo: En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, encontrando como ejemplo entre otros los siguientes:
- a. Programación de instrucciones que producen un bloqueo total al sistema.



- b. **Dstrucción de programas por cualquier método.**
- c. **Daño a la memoria.**
- d. **Atentado físico contra la máquina o sus accesorios.**
- e. **Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.**
- f. **Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)**

Por otra parte, se puede señalar que existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- a. **Acceso no autorizado: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario. (Violación de la privacidad).**
- b. **Dstrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.**
- c. **Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.**
- d. **Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.**
- e. **Estafas Electrónicas: A través de compras realizadas haciendo uso de la Internet.**
- f. **Transferencias de fondos: Engaños en la realización de este tipo de transacciones.**

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- a. **Espionaje:** Acceso no autorizado a sistemas de informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- b. **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- c. **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- d. **Otros delitos:** Las mismas ventajas que encuentran en la Internet los narcotraficantes puede ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Por su parte los tipos de delitos reconocidos por la Organización de las Naciones Unidas –ONU- y que le han dado su carácter internacional, a fin de que los países los tomen en consideración para ser incorporados a sus distintas legislaciones penales correspondientes son los siguientes:

1. **Fraudes cometidos mediante manipulación de computadoras:**
 - a. Manipulación de los datos de entrada.
 - b. La manipulación de programas.
 - c. Manipulación de los datos de salida.
2. **Fraude efectuado por manipulación informática.**
3. **Falsificaciones informáticas:**
 - a. **Como objeto:** Cuando se alteran datos de los documentos almacenados en forma computarizada.

- b. Como Instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.
4. Daños o modificaciones de programas o datos computarizados:
- a. Sabotaje informático: Borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
- a.1. Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y proporciona a otros programas informáticos.
- a.2. Gusanos: Sé fábrica igual al virus con miras en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero puede regenerarse.
- a.3. Bomba lógica cronológica: Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro, poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente.
- a.4. Acceso no autorizado a servicios y sistemas informáticos: Por motivos diversos: desde la simple curiosidad, como el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
- a.5. Piratas informáticos o hackers: El acceso se efectúa desde un lugar exterior, situado en la red de telecomunicaciones recurriendo a uno de los diversos medios que se mencionan a continuación.

- a.6. Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Se puede considerar que no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Existe también un grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos; esta tipificación se refiere a quién, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

Existen circunstancias agravantes de la divulgación de ficheros, los cuales se dan en función de:

- a. El carácter de los datos: ideología, religión, creencias, salud, origen racial y vida sexual.
- b. Las circunstancias de la víctima: menor de edad o incapaz.

En este tipo de delitos, también se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se puede asegurar que entre esta clasificación podemos ubicar el pinchado de redes informáticas.

Ubicamos aquí también la interceptación de *e-mail*, en este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Otra forma de cometer ilícitos mediante el uso de los sistemas informáticos lo constituye la pornografía infantil. La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. Durante los últimos años, el número de condenas por transmisión o posesión de pornografía infantil ha aumentado considerablemente en varios países. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material ofensivo que se transmita o archive.

1.7. Los piratas informáticos o *hackers*

Comúnmente se define al hacker como aquel que se divierte empleando al máximo su inteligencia, sin la necesidad de ocasionar daños a un tercero. Aunque, actualmente, el alcance de la actividad de los piratas informáticos, excede los límites del simple ocio y la recreación, llegando sus actos a constituir meros hechos delictivos.

El origen de esta práctica se remonta a principios de la década de 1960, cuando en el Massachusetts Institute of Technology (MIT), los estudiantes del prestigioso centro educativo se desafiaban unos a otros a crear programas de mayor capacidad que los existentes. Actualmente las actividades de los hackers engloban varias categorías que

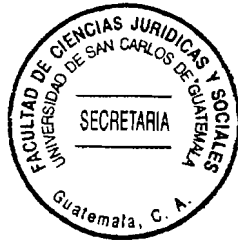


definen de forma más específica su campo de actuación, aunque no todas ellas se encuentran tipificadas como delito en la mayoría de legislaciones.

Los crackers, son los que más revuelo suelen causar. Distanciados de los hackers por criterios éticos y morales, se especializan, básicamente, en causar daño. Son famosos por robar información, desactivar las protecciones de software, ingresar en centros de seguridad restringidos o programar virus.

Los phreakers, se encargan de explorar los límites y alcances de las redes telefónicas manipulando frecuencias mediante la tecnología, consiguen realizar llamadas gratuitas a cualquier parte del mundo y en términos más drásticos vulnerar centrales importantes. En su afán por descubrir las limitaciones de las redes telefónicas, acaban incurriendo en situaciones que los pueden poner tras las rejas. Actualmente, los phreakers tienen también como blanco a la telefonía móvil, a las tecnologías inalámbricas.

Con los avances tecnológicos existentes en la actualidad, se hace difícil prever el alcance que estas actividades tendrán en un futuro. Lo que sí se puede intuir, dentro de la naturalidad inherente al hacker de superar sus propios límites, nuevos desafíos se presentarán para quienes intentan contrarrestarlos.



1.8. Infracciones que no constituyen delitos informáticos

Existen también una serie de acciones, que si bien afectan los sistemas informáticos y la información que estos conservan, los mismos no llegan a constituir delitos, dentro de estos se puede encontrar:

- a) **Usos comerciales no éticos:** Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo mailings electrónicos, al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.
- b) **Actos parasitarios:** Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate online, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc.

Así también se deben tomar en cuenta las obscenidades que se realizan a través del internet.

1.9. Los delitos informáticos en la legislación guatemalteca

De conformidad con la legislación vigente y las modificaciones incluidas al Código Penal, según el Decreto No. 33-96 del Congreso de la República, a fin de regular sobre

estas prácticas delictivas, establece en sus artículos del 274 "A" al 274 "G" los siguientes delitos informáticos:

1. Artículo 274 "A". Destrucción de registros informáticos. Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare 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.

Este delito sanciona la destrucción de la información que pudiere existir en los registros informáticos, la agresión se da en contra del soporte de esta información, como a la información en sí, en tal sentido se puede establecer que existen varios bienes jurídicos lesionados, constituyendo en si un delito pluriofensivo.

2. Artículo 274 "B". Alteración de programas. La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras.

Igual que en el caso del delito de destrucción de registros informáticos, en este tipo de delitos la agresión se da en contra del sistema informático, dicha acción pueden tener como fin otra acción delictiva o preparar u ocultar otra acción delictiva.

3. Artículo 274 "C". Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

La acción en esta figura delictiva va encaminada a lesionar el derecho de autor o propiedad intelectual, la cual se refiere con exclusividad a la propiedad intelectual sobre programas informáticos.

4. Artículo 274 "D". Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Esta figura delictiva, se puede ubicar como un delito pluriofensivo, ya que para poder crear un registro informático que perjudique a otra persona, muchas veces puede darse el caso en que para hacerlo debe ingresarse ilegalmente al registro informático de otra persona; en igual forma la finalidad de la creación de un archivo o registro prohibido, puede tener como finalidad la comisión o el ocultamiento de otro hecho delictivo.

5. Artículo 274 "E". Manipulación de información. Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.

Como se puede determinar de esta figura delictiva, el uso de los registros informáticos puede ser utilizado para la comisión de otro tipo de delitos, mediante la alteración de los registros informáticos se puede estar preparando, ocultando o realizando otro u otros delitos; sin embargo lo que esta norma sanciona es el hecho de alterar estos registros informáticos. De donde se puede establecer y confirmar que este tipo de delitos es pluriofensivo.

6. Artículo 274 "E". Uso de información. Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los

registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos.

Mediante esta figura delictiva, el bien jurídico que se protege es la información, en tal sentido los archivos electrónicos o banco de datos, son los bienes que se pretenden proteger, elevándolos a la categoría de bien jurídico tutelado o protegido. Cabe aclarar que no únicamente se está sancionando el uso de información ajena, sino también el simple ingreso a dicha información.

7. Artículo 274 "G". 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 esta figura delictiva, resalta el hecho que para que se tipifique la misma, basta con hacer circular los programas o instrucciones destructivas, la simple amenaza que representa la circulación de las instrucciones destructivas es sancionada, indistintamente de los daños que pueda o haya causado.

Podemos concluir entonces, del análisis de la doctrina y de nuestra legislación sobre el tema de los delitos informáticos que:

1. Por constituir una reforma y adición a nuestro Código Penal, su regulación no es la más acertada al incluirlos dentro Libro Segundo, Título VI del Capítulo VII referente a los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos, ya que no permite determinar con claridad cuál es el bien jurídico tutelado.



2. De conformidad con nuestra legislación, por el tipo de delitos incluidos dentro de los delitos informáticos, estos pueden considerarse como fin, pues el computador, accesorios o programas como entidad física puede ser objeto de la ofensa, al manipular o dañar la información que pudiera contener, y como medio, como herramienta del delito (medio) al existir conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.
3. De conformidad con nuestra legislación el bien jurídico protegido en este tipo de delitos, comprende la confidencialidad, integridad, disponibilidad de la información y además los sistemas informáticos donde esta se almacena o transfiere.
4. Por la variedad de bienes jurídicos protegidos, podemos considerar que en nuestra legislación este tipo de conductas criminales son de carácter netamente pluriofensivos, en virtud de existir intereses socialmente valiosos que se ven afectados por estas nuevas figuras, además de existir afección de bienes jurídicos clásicos.
5. Como actualmente se encuentran regulados los delitos informáticos en nuestra legislación, existen una cantidad considerable de conductas que, si bien lesionan bienes jurídicos tutelados, no se encuentran tipificadas como delitos, razón por la cual se promueve su investigación y sanción bajo las figuras tradicionales.



CAPÍTULO II

2. La informática forense como ciencia auxiliar de la criminalística

Durante muchos años, la ciencia criminalística estuvo representada en los tribunales solo por la medicina forense. Actualmente en cambio se suman a ella muchas actividades técnicas y científicas entre ellas la nueva ciencia de la informática forense, que constituye la rama tecnológica y legal encargada de la investigación sistemática de medios informáticos en busca de las evidencias electrónicas, que quedan presentes tras un acto delictivo.

Las ciencias forenses tienen que ver principalmente con la recuperación y análisis de la llamada evidencia latente. Las ciencias forenses combinan el conocimiento científico y las diferentes técnicas que este proporciona con los presupuestos legales a fin de demostrar con la evidencia recuperada la existencia de la comisión de un acto considerado como delictivo y sus posibles responsables ante los tribunales de justicia.

Cuando se habla de la informática forense, se debe tomar en cuenta que la informática por su parte es el conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras; así mismo que, la informática combina los aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano y que los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica.

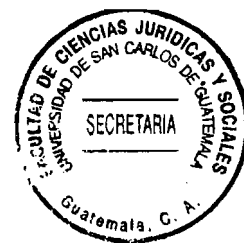
2.1. La criminalística como disciplina auxiliar del Derecho Penal

Con el objeto de poder abordar en forma apropiada la peritación de los delitos informáticos, se hace necesario determinar dentro de la criminalista, la función de la informática forense; razón por lo cual debemos partir de las definiciones de la criminalística.

La criminalística puede ser definida como la ciencia que tiene la finalidad el descubrir los componentes externos del delito, revelar los testigos mudos (indicios) de la escena del hecho delictivo, lo que llevará a descubrir al criminal; también podemos indicar que la criminalística es la disciplina auxiliar del derecho penal que se ocupa del descubrimiento y verificación científica del delito y del delincuente; en tal sentido se puede indicar en forma general que la criminalística fundamentalmente se ocupa de determinar en qué forma se cometió el hecho delictivo y quién lo cometió.

El doctor Rafael Moreno González, tratando de ser muy explícito, presenta una definición de la criminalística como una "Rama de las ciencias forenses que utiliza todos sus conocimientos y métodos para coadyuvar de manera científica en la administración de justicia".²²

²² Moreno González, Rafael. **Manual de introducción a la criminalística**, pág. 132.



2.2. Principios doctrinarios de la criminalística y sus ciencias auxiliares

La criminalística y sus ciencias auxiliares, basan sus conocimientos y sus métodos de investigación, según lo establece el autor Adolfo Santodomingo Garachana, “en los siguientes principios:

- a. Principio de intercambio: En 1910 el criminólogo francés Edmund Locard observó que todo criminal deja una parte de sí en la escena del delito y se lleva algo consigo, deliberada o inadvertidamente. También descubrió que estos indicios pueden conducirnos a su identidad. El razonamiento lógico de Locard constituye hoy en día la piedra angular de la investigación científica de los crímenes.
- b. Principio de correspondencia: Establece la relación de los indicios con el autor del hecho. Por ejemplo: si dos huellas dactilares corresponden a la misma persona, si dos proyectiles fueron disparados por la misma arma, etc.
- c. Principio de reconstrucción de hechos: Permite deducir a partir de los indicios localizados en el lugar de los hechos, en qué forma ocurrieron éstos.
- d. Principio de probabilidad. Deduce la posibilidad o imposibilidad de un fenómeno con base en el número de características verificadas durante un cotejo.”²³

Cuando se habla de la persecución penal de los delitos informáticos, en los proceso de recabación de evidencias y de su análisis a través de los peritajes, estos principios deben ser tomados en cuenta, en tal sentido, debe de analizarse la forma en cómo los mismos se aplican en la informática forense.

²³ Santodomingo Garachana, Adolfo. **Introducción a la informática en la empresa**, pág. 35.



2.3. La informática forense como ciencia auxiliar de la criminalística

Se puede definir la informática forense como la rama tecnológica y legal encargada de la investigación sistemática de medios informáticos y telemáticos en busca de evidencias electrónicas, presentes tras un acto delictivo o ilegítimo, así como la posterior gestión de las mismas

Se puede señalar que la informática forense, aplica los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes y como disciplina especializada procura el esclarecimiento de los hechos, ante lo cual se formula las preguntas siguientes: ¿quién?, ¿cómo?, ¿dónde?, ¿cuándo? y ¿porqué?, dichos cuestionamientos se formulan sobre eventos que podrían catalogarse como incidentes, fraudes o usos indebidos en el contexto de la justicia.

Frente a las diversas formas de ataques de los llamados delitos informáticos nace la informática forense como aquella disciplina “que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, para luego ésta ser presentada en una Corte de Justicia”.²⁴

“La ciencia informática o cómputo forense es un conjunto de técnicas especializadas auxiliares de la criminalística que tiene como finalidad la reconstrucción de hechos

²⁴ Acurio del Pino, Santiago. **Introducción a la informática forense**. *Revista de Derecho Informático*, septiembre 2007, <http://www.alfa-redi.org/rdi-articulo.shtml?x=9608>, (11 de octubre 2009).

pasados basados en los datos recolectados, para lo cual se procesa la información que pueda ser usada como evidencia en un equipo de cómputo”.²⁵

Para Miguel López Delgado, “esta disciplina es relativamente nueva y se aplica tanto para la investigación de delitos “tradicionales”, (homicidios, fraude financiero, narcotráfico, terrorismo, etc.), como para los propiamente relacionados con las tecnologías de la información y las comunicaciones, entre los que destacan piratería de software y comunicaciones, distribución de pornografía infantil, intrusiones y “hacking” en organizaciones, spam, phishing, etc”.²⁶

Tomando en cuenta que las evidencias electrónicas pueden ser rápidamente eliminadas o perdidas, haciendo así más difícil su persecución legal, se necesita un modo de rescatar y preservar esos datos rápidamente. La informática forense recopila y utiliza las evidencias informáticas para esclarecer los delitos informáticos usando técnicas y tecnologías avanzadas. En tal sentido, se deben de utilizar técnicas para descubrir evidencias en cualquier dispositivo de almacenamiento informático como discos duros, cintas de backup, ordenadores, portátiles, memorias usb, archivos, correos electrónicos, etc. Las investigaciones forenses informáticas sirven para, sin manipularlas, obtener evidencias electrónicas o rastros dejados en equipos informáticos. Dichas evidencias informáticas son los registros dejados en equipos informáticos, routers, firewalls o servidores de correo tras su uso.

²⁵ Thorin, Marc. **La ciencia informática: métodos, reglas, normas**, pág. 22.

²⁶ López Delgado, Miguel. **Análisis forense digital**, pág.39.

La ciencia forense es sistemática y se base en hechos premeditados para recabar pruebas para luego analizarlas. La tecnología, en caso de la identificación, recolección y análisis forense en sistemas informáticos, son aplicaciones que juegan un papel de suma importancia en recabar la información y los elementos de convicción necesarios. La escena del crimen es el computador y la red a la cual éste está conectado. En resumen a través de la informática forense, como ciencia auxiliar de la criminalística, se pretende determinar cuál es el papel que juegan los sistemas informáticos en la comisión del delito, a fin de que se puedan establecer los elementos de convicción necesarios para el proceso penal.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso penal.

2.4. Principios de la ciencia informática forense

Se puede señalar que además de los principios generales de la criminalística, los principios que rigen la ciencia forense como auxiliar de la criminalística, son los siguientes principios:

- a. **Racional:** La Investigación informática forense debe ser racional, es decir que debe explicitar sus finalidades, y deducir de éstas los medios y las acciones de investigación que se consideren necesarios y suficientes.

- b. **Eficacia, Fiabilidad y Seguridad:** La investigación informática sólo tiene sentido si se define su finalidad al examen de la eficacia o seguridad de un sistema, de la fiabilidad de una aplicación, verificación de la aplicación, etc.

La informática forense debe sentar las bases de la investigación científica en esta materia, dando las pautas a los investigadores de cómo manejar una escena del delito en donde se vean involucrados sistemas de información o redes y la posterior recuperación de la llamada evidencia digital.

El perito o informático forense, debe ajustarse a ciertas metodologías, para que las evidencias electrónicas sirvan como pruebas fehacientes de un posible delito ante eventuales procesos judiciales. Estas metodologías pueden encuadrarse dentro de lo que se considera el procedimiento genérico de investigación forense, que consta de dos fases principales:

1. Incautación confiable de la prueba y preservación de la cadena de custodia.
2. Análisis de la información disponible con arreglo al incidente investigado y Redacción del informe pericial.

Uno de los elementos esenciales es la correcta incautación de la prueba, que respete los derechos de las partes y no de pie a que se descarte en un tribunal. Otro aspecto que hay que cuidar es la correcta preservación de la cadena de custodia de todo el ciclo de vida de la evidencia, de forma que existan garantías de que la prueba no puede ser manipulada.



2.5. La evidencia informática

Cuando se comete un delito, tanto de orden común, en el que se vean involucrados medios informáticos, como delitos informáticos propiamente, muchas veces la información que directa o indirectamente se relaciona con el hecho delictivo queda almacenada en forma digital dentro de un sistema informático. Este conjunto de datos ordenados sistemáticamente y convertidos en información se convierten en evidencia digital como prueba de la infracción cometida. Para recabar dicha evidencia se hace necesario utilizar los procedimientos técnicos y legales y la rigurosidad científica que provee la informática forense, a fin de descubrir a los autores del delito cometido.

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

Se puede indicar que la evidencia digital es cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático.

En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal.

La informática trabaja en dos escenarios sobre los cuales realizará el perito sus respectivos análisis, uno de ellos es el hardware (evidencia material) que se refiere a los componentes físicos de un sistema informático en particular tales como el monitor o pantalla, impresora, módem, router, entre otros, y el otro se refiere al componente lógico es decir, a los programas computacionales, esto es, un conjunto de instrucciones para ser usadas por el ordenador con el objeto de obtener un determinado proceso o resultado.

El Doctor Santiago Acurio del Pino, en cuanto a donde debe ser ubicada la evidencia en este tipo de delitos, establece que “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 esta (evidencia digital)”.²⁷ Señalando además, dicho autor que esta distinción es de gran utilidad 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 la evidencia electrónica o hardware se referirá a todos los componentes físicos de un sistema informático, mientras que la evidencia digital o información se referirá a todos los datos, mensajes de datos y programas almacenados y transmitidos usando el sistema informático.

²⁷ Acurio del Pino, Santiago, op. cit., (11 de octubre 2009).

Esa labor debe ser llevada a cabo con máxima cautela y de forma detallada, asegurándose que se conserva intacta, en la medida posible, la información contenida en el disco de un sistema comprometido, de forma similar que los investigadores policiales intentan mantener la escena del crimen intacta, hasta que se recogen todas las pruebas posibles.

Según la autora Augustina Fournier “la prueba pericial informática es el medio de prueba, de suma importancia para cualquier actuación judicial que precisen conocimientos científicos o técnicos especializados”.²⁸ Sobre este tema, hay que tener en cuenta, que no siempre se relaciona con delitos informáticos exclusivamente, sino también con delitos contra cualquier otro tipo de delitos, es por eso que la informática puede verse implicada, por ejemplo:

- Cuando es utilizada como medio para cometer un delito.
- Cuando la informática es el objeto propio del delito (Ej.: compra de software ilegal, o discos de música piratas).
- Cuando tiene lugar en el conflicto de forma colateral, pero en ocasiones, determinante, por ejemplo la destrucción de registros informáticos.

Las evidencias electrónicas son rastros existentes en los equipos informáticos que, debidamente preservados, y puestos en relación con información existente en otros ordenadores o en el contexto de otras evidencias o de hechos probados permiten

²⁸Fournier, Augustina. **La prueba pericial informática**, <http://www.compendium.com.ar/juridico/peri2.html> (16 de septiembre de 2009).

demostrar que se ha llevado a cabo una acción, por medios informáticos o no, e, incluso, quien o quienes la han llevado a cabo.

Hay que recordar que la evidencia en el derecho procesal penal es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella, y en este tema en particular, la evidencia digital es cualquier mensaje de datos almacenado y transmitidos por medio de un sistema de información que tenga relación con la comisión de un acto que comprometa gravemente dicho sistema y que posteriormente guía a los investigadores al descubrimiento de los posibles infractores.

Es importante también establecer claramente cuál es el papel que juega la informática forense en relación con la persecución penal de investigación de delitos informáticos. Para lograr establecer dicho rol, se debe examinar la actuación del perito frente a la ocurrencia de delitos, estrategias para evitarlos, recomendaciones adecuadas, conocimientos requeridos, en fin una serie de elementos que definen de manera inequívoca el aporte que éste brinda en el manejo de los casos de delitos informáticos.

a) Fuentes de la evidencia informática

Se debe distinguir los términos de evidencia digital de la evidencia electrónica, para tal efecto debemos saber distinguir los aparatos electrónicos de la información digital que estos contengan, sin olvidarnos que nuestra investigación siempre deberá dirigirse a la evidencia digital, aunque en algunos casos también serán los aparatos electrónicos. Esta diferenciación cabe hacerla a fin de que en la investigación se sepa que evidencia

buscar y se puedan identificar las fuentes más comunes de evidencia, a efecto de utilizar los métodos más adecuados para recolectar y preservar la misma

Según lo que se ha venido relacionando hasta el momento las fuentes de evidencia digital se pueden clasificar en los tres grupos siguientes:

1. **Sistemas de computación abiertos:** conformados por las computadoras personales y los servidores, así como todos sus accesorios como teclados, ratones y monitores.
2. **Sistemas de comunicación:** compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y la internet.
3. **Sistemas convergentes de computación:** los cuales están formados por teléfonos celulares, asistentes personales, tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que pueda contener evidencia digital.

b) Clases de evidencia informática

De conformidad con el modo de conservación y permanencia, la evidencia digital se puede clasificar en:

1. **Evidencia constante o persistente:** que la constituye aquella evidencia que se encuentra almacenada en un disco duro o en otro medio informático y que se mantiene preservada después de que la computadora es apagada.
2. **Evidencia volátil:** consistente en la evidencia que se encuentra alojada temporalmente en la memoria RAM o en el CACHÉ, la cual es una evidencia

inestable y que se pierde cuando el computador es apagado, esta evidencia debe ser recuperada de inmediato.

c) Características de la evidencia informática

La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando, el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad:

1. Es volátil.
2. Es anónima.
3. Es duplicable.
4. Es alterable y modificable.
5. Es eliminable.

De conformidad con estas características, se puede determinar la labor ardua que se requiere por parte de peritos en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. Por tanto, es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y procesos que

permitan mantener la confiabilidad de los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados.

d) Admisibilidad de la evidencia informática

Como se señaló anteriormente la evidencia digital es frágil y volátil, en tal sentido, la información que se encuentra en los medios de almacenamiento electrónico puede ser borrada, cambiada o eliminada sin dejar rastro; en este sentido, es pieza probatoria básica que requiere una revisión detallada sobre cómo se crea, cómo se recolecta, cómo se asegura y finalmente cómo se presenta ante el Juez, con el fin de aportar con claridad y precisión elementos que orienten las decisiones sobre casos donde ésta evidencia sea parte fundamental del mismo.

Al responder a estos interrogantes se puede disminuir la posibilidad de incertidumbre sobre los registros electrónicos, para contar con evidencia digital de carácter probatorio admisible en juicio, en tal sentido consideramos que para que una evidencia informática pueda ser admisible en juicio necesita cubrir los requerimientos siguientes:

- **Autenticidad:** en virtud que se debe demostrar que dicha evidencia ha sido generada y registrada en los lugares o sitios relacionados con el caso, particularmente en la escena del posible ilícito o lugares establecidos en la diligencia de levantamiento de evidencia; entendiéndose como la no alterabilidad de los medios originales, buscando confirmar que los registros aportados corresponden a la realidad evidenciada en la fase de identificación y recolección

de evidencia. Para tal efecto se requiere que existan mecanismos que aseguren la integridad de los archivos y el control de cambios de los mismos.

- **Confiabilidad:** ya que se debe acreditar que efectivamente los elementos probatorios aportados vienen de fuentes que son creíbles y verificables, y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue, para tal efecto se debe demostrar que los registros electrónicos poseen una manera confiable para ser identificados, recolectados y verificados.
- **Suficiencia:** lo cual se refiere a que la evidencia es completa, se tiene presente toda la evidencia necesaria para el caso. Frecuentemente la falta de pruebas o insuficiencia de elementos probatorios ocasiona la dilación o terminación de procesos que podrían haberse resuelto. En este sentido, mientras mayores fuentes de análisis y pruebas se tengan, habrá posibilidades de avanzar en la defensa o acusación en un proceso judicial.
- **Obtenida de conformidad con las leyes:** este requisito hace referencia a los procedimientos legalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital, lo cual permitirá su incorporación al proceso penal.

Dichos requerimientos están acordes a lo que establece el Código Procesal Penal en su Artículo 183, cuando se refiere a la prueba inadmisibles, señalando los requisitos para que un medio de prueba pueda ser admitido en juicio y los medios de prueba que no pueden ser admitidos.





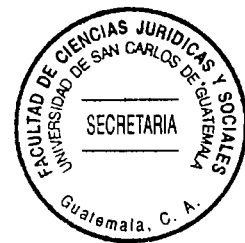
CAPÍTULO III

3. El perito informático

El perito informático es un experto en informática, capaz de emitir un dictamen (opinión) imparcial sobre unos hechos, unos bienes u otros, directamente relacionados con la materia en litigio. Es un auxiliar del juez o tribunal y siempre ha de ser un ajeno al caso, es decir, neutral. Según el concepto jurídico, perito es aquella persona que posee los conocimientos científicos, artísticos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, y que integrarán la falta que de los mismos pueda tener el juzgador.

Un perito informático dictamina sobre los hechos ocurridos o las circunstancias relevantes en el asunto, con la finalidad de ayudar a valorarlas o para adquirir certeza sobre los mismos. Analiza el pasado, los hechos ocurridos y las evidencias que dejaron, al contrario que el consultor informático, que mira al futuro para diseñar o implantar nuevos sistemas, o al auditor, que aún mirando a hechos pasados, observa también el presente para certificar o no el cumplimiento de una norma.

Un perito informático es un tercero procesal, ajeno al proceso, que posee conocimientos especializados, científicos, artísticos o prácticos, por formación reglada o sólo experiencia y acepta voluntariamente incorporar dichos conocimientos al proceso, aplicándolos al objeto de la prueba.



3.1. La actividad pericial

La prueba pericial 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 designados 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 tribunal, siempre que para ello se requieran esos conocimientos.

La palabra pericia puede hacer referencia a los conocimientos del perito, pero no como medio de prueba. En cuanto al dictamen pericial, está constituido por la opinión y el juicio que emite el perito, mientras que el peritaje comprende, además de esa opinión, el trabajo o estudio que hace el perito para dar su dictamen.

En definitiva, la actividad pericial es una actividad probatoria, ya que el dictamen pericial puede ser un medio de prueba. Pero debemos diferenciar entre perito titulado colegiado, de los técnicos o prácticos que no disponen de titulación oficial o al menos no informática.

El perito informático forense, rastrea las pruebas en los ordenadores con el fin de reconstruir el escenario de cualquier incidente o ataque informático para que los jueces puedan condenar a los autores; para investigar los delitos informáticos es necesaria la intervención de un especialista en informática forense que intentará reconstruir el



camino que ha seguido el delincuente con el objetivo de encontrar las pruebas que permitan su detención y condena.

El análisis o peritaje forense es un proceso que, mediante una metodología adecuada y formal, permite reconstruir el escenario del incidente o suceso de tal forma que podemos conocer las causas, mecanismos y herramientas, así como sus autores; para los médicos forenses, los muertos hablan, para los peritos informáticos, los que hablan son discos duros.

El investigador forense realiza la reconstrucción funcional del hecho, estableciendo el funcionamiento de un sistema o aplicación específica y como estos fueron configurados en el momento del delito. La línea de tiempo del incidente le ayuda al investigador a identificar patrones e inconsistencias en la escena, guiando a este a más fuentes de evidencia.

La pericia informática se base y fundamenta en principios técnicos y en la objetividad por lo que constituye una prueba, en la mayoría de los casos, irrefutable, eficaz e incuestionable, siempre y cuando el juzgador sepa interpretar la pericia.

De conformidad con la naturaleza y la forma en que se desarrollan los delitos informáticos, el perito informático tiene como función principal la de recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal.



Se puede señalar también, que el objetivo de un peritaje forense informático es realizar un proceso de búsqueda detallada y minuciosa para reconstruir a través de todos los medios los acontecimientos que tuvieron lugar desde el mismo instante cuando el sistema informático estuvo en su estado integro hasta el momento de detección de un estado comprometedor.

De conformidad con lo que establece el Código Procesal Penal en su Artículo 225, procede la peritación cuando para obtener, valorar o explicar un elemento de prueba fuere necesario o conveniente poseer conocimientos especiales en alguna ciencia, arte, técnica u oficio. En tal sentido, y adecuando dicha normativa al tema de investigación, se puede indicar que para investigar la comisión de un hecho delictivo que revista las características de delito informático, y sea necesario obtener evidencia informática, valorar dicha evidencia o explicar la misma, se hace necesaria la intervención de un perito informático, en virtud de las peculiaridades y características específicas de dicha evidencia, quien de conformidad con sus conocimientos y experiencia en la materia, posee la capacidad técnica para obtener, valorar o explicar dicha evidencia informática.

El peritaje forense informático, se fundamenta en la necesidad de suplir la falta de conocimiento del juez o del fiscal, en tal sentido, los peritos informáticos son las personas que por disposición legal y encargo del Ministerio Público o el tribunal, aportan con sus conocimientos los datos necesarios para que el juez o el fiscal adquieran un grado de conocimiento para determinar las circunstancias en que se cometió una infracción.

El dictamen pericial constituye un juicio de valor sobre cuestiones de hecho, respecto de las cuales se requieren conocimientos especiales. La opinión del experto no puede sustituir la función del juez, que es el único juzgador de los hechos litigiosos, de la conducta de las partes y de la norma jurídica aplicable al caso concreto. No le corresponde al perito emitir juicios de valor sobre las conductas de las partes, pues ello queda a reserva de la apreciación del juez.

En este sentido, es interesante la postura de Jeimy Cano, quien afirma que “el peritaje informático surge como respuesta natural de la evolución de la administración de justicia que busca avanzar y fortalecer sus estrategias para proveer los recursos técnicos, científicos y jurídicos que permitan al juzgador, alcanzar la verdad y asegurar el debido proceso en un ambiente de pruebas electrónicas”.²⁹

3.2. El rol del perito informático en la recuperación de la evidencia.

Se hace imprescindible establecer cuál es el rol del perito informático dentro del proceso de recuperación de la evidencia y su posterior análisis, esto en relación a las particularidades que presentan las escenas del crimen en los delitos informáticos.

En primer lugar, recordemos que debido a una instrucción generada por el Fiscal General del Ministerio Público, de una fecha para acá, se han implementado los Equipos de Escena del Crimen. Tomando en cuenta que estas personas son las

²⁹ Cano, Jeimy J. **Estado del arte del peritaje informático en Latinoamérica.** http://www.alfaredi.com//apcaaalfaredi/img_upload/374d0ee90831e4ebaa1def162fa50747/Estado_del_Arte_del_Peritaje_Informatico_en_Latinoamerica.pdf, (21 de octubre de 2009).

primeras en llegar a la escena del crimen, debe evaluarse si el personal de escena del crimen se encuentran en la capacidad técnica de realizar la recolección de la evidencia informática en la escena; de lo contrario se hace necesario requerir en forma inmediata la presencia de un perito o técnico informático para que la evidencia sea recabada en forma pertinente. Debe también evaluarse las circunstancias particulares de la escena del crimen, de la evidencia recabada en dicha escena y si la misma puede ser procesada por un Técnico Informático; de no ser así, y si la evidencia requiere mucha especialidad, se hará necesario requerir los servicios de un perito en informática, quien deberá ser una persona con un entrenamiento general en cuestiones de informática forense, ser un profesional en seguridad informática, con conocimientos de disposiciones legales y de investigación criminalística.

Como ejemplo de las evidencias informáticas ante las cuales tendrá que actuar el perito informático, con el fin de acreditar la perpetración de hechos ilícitos y sus posibles responsables, se puede mencionar las acciones ilegales siguientes:

- a. Descubrimiento y revelación de secretos o espionaje industrial, por ejemplo mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos.
- b. Delitos económicos o contra el mercado o los consumidores, realizados empleando ordenadores.
- c. Delitos contra la propiedad intelectual e industrial, como la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas.

- d. Vulneración de la intimidad, lectura de correo, interceptación de comunicaciones, protección de datos personales.
- e. Estafa, fraudes o conspiración para alterar el precio de las cosas a través de la manipulación de datos o programas; extensión de la falsificación de moneda a las tarjetas de débito y crédito; fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.
- f. Sabotaje o destrucción de cosa de valor, como daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.
- g. Amenazas, calumnias e injurias realizadas o propagadas por cualquier medio de comunicación, como Internet o correos electrónicos.
- h. Producir, vender, distribuir o exhibir, por cualquier medio, material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces.

3.3. Perfil del perito informático

Se considera que el perito informático debe reunir las condiciones técnicas y legales siguientes:

- 1. Ser profesional especializado en materia informática y encontrarse habilitado para el ejercicio de su profesión; aunque debemos tomar en cuenta lo que establece el Artículo 226 del Código Procesal Penal, al indicar que no necesariamente el perito debe ser un profesional, ya que puede designarse a una persona de idoneidad manifiesta, en aquellos lugares en que no exista un profesional titulado.

2. Ser mayores de 18 años de edad, porque a esa edad la persona ha alcanzado la madurez psicológica y legal necesaria para prestar esta clase de asesoramiento a la Administración de Justicia.

Según la opinión de Jeimy Cano, "el perito informático, de conformidad con su función forense, debe poseer una formación integral que además de sus conocimientos en temas de tecnologías de la información, también es necesario que posea formación en disciplinas jurídicas, criminalísticas y forense".³⁰

Se podría sugerir que en la formación del perito informático, deben incluirse los temas mínimos siguientes:

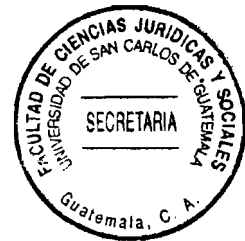
a. En el área tecnológica de información y electrónica

1. Lenguaje de programación.
2. Teoría de sistemas operacionales y sistemas de archivo.
3. Protocolos e infraestructura de comunicación.
4. Fundamentos de circuitos eléctricos y electrónicos.
5. Arquitectura de Computadoras.

b. Fundamentos de bases de datos área de seguridad de la información

1. Principios de seguridad de la información.
2. Políticas estándares y procedimientos en seguridad de la información.
3. Análisis de vulnerabilidades de seguridad informática.
4. Análisis y administración de riesgos informáticos.
5. Recuperación y continuidad de negocio.

³⁰ Ibid., pág. 22.



6. Clasificación de la información.
7. Técnicas de Hackiang y vulneración de sistemas de información.
8. Mecanismos y tecnologías de seguridad informática.
9. Concientización en seguridad informática.

c. Área jurídica

1. Teoría general del derecho.
2. Formación básica en delito informático.
3. Formación básica en protección de datos y derechos de autor.
4. Formación básica en convergencia tecnológica.
5. Formación básica en evidencias digital y pruebas electrónicas.
6. Análisis comparado de legislaciones e iniciativas internacionales.

d. Área de criminalística y ciencias forenses

1. Fundamentos de conductas criminales.
2. Perfiles psicológicos y técnicos.
3. Procedimientos de análisis y valoración de pruebas.
4. Cadena de custodia y control de evidencias.
5. Fundamento de Derecho Penal y Procesal.
6. Ética y responsabilidades del perito.
7. Metodologías de análisis de datos y presentación de informes.

e. Área de informática forense

1. Esterilización de medios de almacenamiento magnético y óptico.
2. Selección y entrenamiento en software de recuperación y análisis de datos.
3. Análisis de registros de auditoría y control.
4. Correlación y análisis de evidencias digitales.



5. Procedimientos de control y aseguramiento de evidencias digitales.
6. Verificación y validación de procedimientos aplicados en la pericia forense.

El factor humano, como en todos los campos de la ciencia y la tecnología es un factor determinante para la generación de conocimiento y avance. Sin embargo, se requiere una formación básica que oriente las actividades y acciones de los profesionales que se dedican a una parte específica de la ciencia, con el fin de disminuir la incertidumbre de sus resultados y mejorar la efectividad de sus procesos.

En este sentido, se puede señalar que las investigaciones forenses en informática no son la excepción. Es un campo de la ciencia que requiere una formación técnica avanzada y detallada en las tecnologías y aplicaciones de software que le permita explorar con profundidad los elementos aportados y poder relacionarlos para fundar hipótesis coherentes y sustentadas en la evidencia digital presentada, además, como se indico, una formación adicional en la ciencia criminalística y el derecho.

Podemos señalar que la administración de justicia, debe desarrollar elementos técnicos, jurídicos y administrativos que le permitan confrontar, validar y asegurar un adecuado proceso ante situaciones litigiosas donde la evidencia en formato digital, electrónico o informático sea la protagonista. Para tal efecto, la formación del personal especializado en estas temáticas, tiende a ser un factor decisivo para la actualización de los métodos tradicionales en ciencias penales, forenses y criminalísticas, que en este nuevo mundo de la sociedad digital, deben alcanzar niveles de pericia.



De conformidad con lo que hasta este momento se ha manifestado, se puede indicar que los requisitos que debe cubrir el perito informático para poder ejercer su cargo son los siguientes:

- a. Conocimiento y experiencia sobre la materia de la que se trate.
- b. Título oficial, le acredita para ejercer sus funciones.
- c. Colegiación profesional actualizada.
- d. Conocimientos básicos en criminalista y derecho.
- e. Acreditación de la colegiación profesional.
- f. Cumplir con el Código deontológico, cuando exista.
- g. Poseer y acreditar formación continua.
- h. Disponibilidad de tiempo y medios para la realización de la peritación.
- i. No ser parte del proceso, ni ser objeto de tacha.
- j. No estar sancionado o inhabilitado o bajo expediente disciplinario colegial.
- k. Persona física, ya que jura del cargo y adquiere responsabilidad.
- l. Actuar según el leal saber y entender profesional.

3.4. Impedimentos del perito informático

De conformidad con lo que establece el Artículo 228 del Código Procesal Penal, no pueden ser designados como peritos informáticos quienes se ubiquen dentro de cualquiera de las situaciones siguientes:

- a. No gozar de sus facultades mentales o volitivas.
- b. Los que deban abstenerse de declarar como testigos.
- c. Los inhabilitados en la ciencia, en el arte o en la técnica de que se trate.

d. Quienes hayan sido designados como consultores técnicos en el mismo procedimiento o en otro conexo.

3.5. El informe pericial

El dictamen del perito informático debe contener una opinión fundada, exponiendo de forma concisa y ordenada, al juez los antecedentes de orden técnico que tuvo en cuenta al realizar la pericia. Un informe pericial, no puede ser un mero informe, sino que ha de tener una sólida base científica, de acuerdo al conocimiento adquirido en la formación informática y otros conocimientos forenses y criminalísticos y expresados según pautas que sirvan para clarificar y asesorar de forma adecuada al juez.

En este tipo de dictámenes el perito informático deberá expresarse con un alto grado de certeza sobre las características del material analizado, comparándolo con originales o con especificaciones de un manual. Cuando la prueba pierde su materialidad, por constituir exclusivamente un dato, la peritación se vuelve compleja, debe suplir las limitaciones técnicas que dificultan la obtención del resultado pretendido y luego realizar la traducción de dichos resultados, a efecto de que sean interpretados por quienes no poseen su visión tecnológica y procedan a tener por acreditada o no la comisión de un delito.

El informe o dictamen pericial debe aclarar las preguntas o asuntos planteados por el solicitante, que puede ser el juez, fiscal, abogado de parte o bien quien haya realizado la petición y en los términos y entorno de dichas cuestiones.

De conformidad con el ordenamiento procesal penal vigente en su Artículo 234 y la doctrina sobre el tema, el informe debe realizarlo el perito en informática cubriendo como mínimo los requisitos siguientes:

- a. Claridad: El dictamen lo leerán personas desconocedoras de la materia.
- b. Concisión: Ni una página más de lo necesario, un informe muy voluminoso desalienta a su lectura.
- c. Fundamentación: La opinión se debe fundamentar en la experiencia apoyándose en la teoría y en la bibliografía.
- d. Justificación: El perito ha de justificar en qué hechos se basa para su dictamen.

A pesar de que el Dictamen Pericial pueda llegar a ser considerado por el juez o tribunal un medio de prueba, se debe insistir en que el perito no prueba el mismo nada, sólo suministra al juez una base científica o técnica. El dictamen pericial de conformidad con lo que establece el Artículo 186 del Código Procesal Penal, es apreciado por el tribunal conforme el sistema de la sana critica razonada.

La eficacia probatoria de la evidencia informática o digital y su interpretación a través de los dictámenes periciales puede generar inconvenientes, cuando la prueba derivada de los procesadores de datos se haya obtenido de sistema no implementados con software legal o reglamentaciones específicas resulta inevitable su cuestionamiento.

En el caso de los delitos informáticos, el perito informático, como profesional estará a cargo de la investigación en esta materia y es el responsable de la precisión y de que el informe sea completo, sus hallazgos y resultados luego del análisis de la evidencia

digital o registros electrónicos. En este sentido toda la documentación debe ser completa, precisa, comprensiva y auditable.

De conformidad con lo que establece el Artículo 234 del Código Procesal Penal, el dictamen se presentará por escrito y el mismo deberá ser ratificado en la audiencia de juicio oral.

3.6. Deberes del perito informático

De conformidad con lo que establece el Artículo 227 del Código Procesal Penal, el perito tiene del deber de aceptar y desempeñar fielmente el cargo, en tal sentido, del ejercicio de su cargo surgen entre otros, los siguientes deberes:

- a. Decir la verdad.
- b. Actuar con la mayor objetividad, tomando en consideración lo que pueda favorecer como lo que pueda perjudicar a cualquiera de las partes.
- c. Aceptar el cargo, salvo justa causa.
- d. Presentar ante el tribunal el dictamen por escrito.
- e. Comparecer a la ratificación, juicio o vista.

3.7. Tipos de responsabilidad del perito informático

De conformidad con el ejercicio de su cargo, el perito estará sujeto a varios tipos de responsabilidades, dependiendo de la norma o legislación:

- a. Responsabilidad Civil (por acción u omisión): reparar daño a un particular.



- Faltar al Secreto Profesional.
 - Daño patrimonial por bien mal valorado.
 - Falsedad en documento privado.
 - Responsabilidad contractual.
- b. Responsabilidad Penal (hecho delictivo voluntario): reparar daño a la sociedad.
- Falso testimonio o perjurio: falsa declaración a sabiendas.
 - Cohecho o soborno: opinión injustificada por una dádiva (como dinero).
 - Denegación de auxilio a la justicia.
 - Desobediencia al Juez o Tribunal.
 - Perturbación del orden en el Juzgado o Tribunal.
- c. Responsabilidad Disciplinaria: Por no comparecer en juicio o vista cuando sea requerido judicialmente para ello.
- d. Responsabilidad Profesional.
- Código deontológico.
 - Procedimiento disciplinario Colegial.

La mejor garantía para eliminar riesgos en la actividad profesional del perito, es actuar siguiendo la máxima que establece que obrar honradamente según ciencia y conciencia.





CAPÍTULO IV

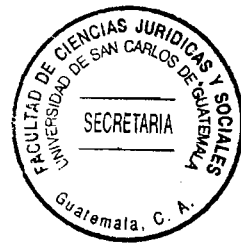
4. El análisis forense informático

El análisis forense informático es una actividad que requiere personal capacitado para realizarlo, en este sentido es primordial la intervención del perito, quien a partir de la comisión de un hecho delictivo, tendrá que seguir una serie de pasos encaminados a recopilar evidencias que le permitan determinar el método de entrada al sistema, la actividad de los intrusos, su identidad y origen, duración del compromiso y todo ello extremando las precauciones para evitar alterar las evidencias durante el proceso de recolección.

Considerando la fragilidad del insumo con el cual trabajan los peritos en informática forense, es preciso extremar las medidas de seguridad y control que éstos deben tener a la hora de ejecutar sus labores, pues cualquier imprecisión en las mismas puede llevar a comprometer el proceso en forma legal.

La recolección y análisis de la evidencia informática es un aspecto frágil del peritaje forense, especialmente porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Para tal efecto, el trabajo de análisis debe realizarse en forma técnica y ordenada, por lo cual se puede señalar como fases del análisis informático forense las siguientes:

1. Identificación del incidente.
2. Recopilación de la evidencia.



3. Preservación de la evidencia.
4. Análisis de la evidencia.
5. Documentación del incidente.

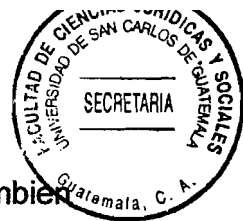
4.1. Las fases del análisis forense informático

El análisis forense constituye todo un procedimiento que conlleva una serie de fases, las mismas, las cuales deben desarrollarse en forma ordenada y completa, procurando abarcar todas las acciones que comprenden cada fase, ya que cada una de ellas se encuentra interrelacionada y la deficiencia en el desarrollo una o varias de ellas podrían generar una conclusión mal fundamentada por parte del perito informático.

a) Identificación del incidente

Una de las primeras fases del análisis forense comprende el proceso de identificación del incidente, que conlleva la búsqueda y recopilación de evidencias. Si se presume la comisión de un hecho delictivo y se sospecha que el sistema informático ha sido comprometido, no hay que perder la calma y actuar precipitadamente. Antes de comenzar una búsqueda desesperada de señales del incidente, que lo único que puede ocasionar es una eliminación de huellas, hay que actuar de forma metódica y profesional. En primer lugar hay que asegurarse que no se trata de un problema de hardware o software de la red o servidor. Se puede indicar que esta fase tiene como objeto principal descubrir las señales del ataque.

Para iniciar una primera inspección del equipo comprometido, se deberá tener en mente la premisa que debe conservarse la evidencia, en tal sentido, no debe hacerse nada



que pueda modificar dicha evidencia. Deberá utilizarse herramientas que no cambien los sellos de tiempo de acceso, o provoquen modificaciones en los archivos, y por supuesto que no borren nada.

Un paso importante es que si no existe certeza de que las aplicaciones y utilidades de seguridad que incorpora el sistema operativo, o las que se hayan instalado se mantienen intactas, se deberá utilizar otras alternativas. En este punto hay que tomar en cuenta que los atacantes dispondrán de herramientas capaces de modificar la información que el administrador verá tras la ejecución de ciertos comandos. En todo momento, hay que cuestionar la información que proporcionen las aplicaciones instaladas en un sistema que se crea comprometido.

Se considera prudente crear un CD o DVD como herramienta para la respuesta a incidentes, y si trabaja en entornos mixtos UNIX/Linux y Windows, se tendrá que preparar uno para cada plataforma. En esta fase se debe al menos, realizar las siguientes tareas:

1. Interpretar comandos en modo consola.
2. Enumerar puertos TCP y UDP abiertos y sus aplicaciones asociadas.
3. Listar usuarios conectados local y remotamente al sistema.
4. Obtener fecha y hora del sistema (date, time).
5. Enumerar procesos activos, recursos que utilizan, usuarios o aplicaciones que los lanzaron.
6. Enumerar las direcciones IP del sistema y mapear la asignación de direcciones físicas MAC con dichas IP.

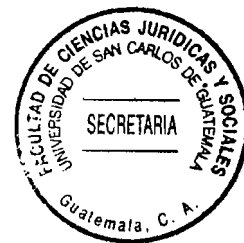


7. Buscar ficheros ocultos o borrados.
8. Visualizar registros y logs del sistema.
9. Visualizar la configuración de seguridad del sistema.
10. Generar funciones hash de ficheros.
11. Leer, copiar y escribir a través de la red.
12. Realizar copias bit-a-bit de discos duros y particiones.
13. Analizar el tráfico de red.

Realizadas las tareas anteriores se debe comenzar la búsqueda de indicios en los equipos que se consideren comprometidos, pero no se debe limitar la búsqueda sólo a éstos, ya que puede haber indicios en otras máquinas próximas tales como escaneado de puertos o tráfico inusual en cortafuegos y routers de la red.

Al iniciar la investigación nunca sabremos con qué nos podremos topar, de hecho al principio puede que no se aprecie a simple vista, ninguna huella o indicio del ataque, especialmente si para realizarlo se han empleado e instalado en los equipos comprometidos un rootkit. Como primera opción de búsqueda podemos realizar una verificación de integridad de los ficheros del sistema, otra opción es realizar una serie de verificaciones sobre del equipo.

Primero sería interesante conocer los procesos que se están ejecutando actualmente en el equipo, en busca de alguno que le resulte extraño, deberán llamarnos la atención aquellos que consuman recursos en exceso, con ubicaciones poco frecuentes en el sistema de archivos, que mantengan conexiones de red en puertos no habituales.



Es conveniente realizar otra comprobación de interés, listar todos los puertos abiertos además de los procesos, usuarios y aplicaciones que los utilizan, siempre con la idea de identificar actividad no usual. La aparición en el listado de procesos sin nombre o que emplean puertos altos (por encima del 1024) pueden ser indicios de la ejecución de un troyano o puerta trasera en el equipo.

Posteriormente se debe editar los archivos de registro del sistema y logs en busca de entradas y avisos sobre fallos de instalación, accesos no autorizados, conexiones erróneas o fallidas, etc. Dependiendo de la plataforma que se emplee se encontrarán estos archivos en distintas ubicaciones.

b) Recuperación de la evidencia y las herramientas a utilizar

El objetivo de la recuperación de la evidencia digital es localizar toda la evidencia y asegurar que todos los registros electrónicos originales disponibles y asegurados en las máquinas o dispositivos, no han sido alterados. Como señalábamos anteriormente, la recolección de evidencia informática es un aspecto frágil de la informática forense, especialmente porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional, en tal sentido, al realizar la actividad de recolección de evidencia se debe tomar en cuenta lo siguiente:

1. Se debe proteger los equipos del daño.

2. Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).
3. Algunas veces, será imposible reconstruir la evidencia (o el equipo que la contiene) si no se tiene cuidado de recolectar todas las piezas que se necesiten.

Para los efectos de la recuperación de la evidencia en los delitos informáticos, así como para realizar el análisis y la investigación correspondiente, en virtud de la especialidad de la materia, se requiere de un tipo especial de herramientas, dichas herramientas se pueden clasificar en cuatro grupos principales:

- Herramientas para la recolección de evidencia.
- Herramientas para el monitoreo y/o control de computadores.
- Herramientas de marcado de documentos.
- Herramientas de hardware.

b.1.) Herramientas para la recolección de evidencia

Existen una gran cantidad de herramientas para recuperar evidencia. El uso de herramientas sofisticadas se hace necesario debido a:

- La gran cantidad de datos que pueden estar almacenados en un computador.
- La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.



- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadores.
- Mecanismos de contraseñas.

La herramienta más común en el uso de la recuperación y análisis de la evidencia informática lo constituye la Encase, dicha herramienta posee características especiales que permite realizar las actividades siguientes:

- Copiado comprimido de discos fuente: Los archivos comprimidos resultantes, pueden ser analizados, buscados y verificados, de manera semejante a los normales (originales) ahorrando cantidades importantes de espacio en el disco del computador del laboratorio forense, permitiendo trabajar en una gran diversidad de casos al mismo tiempo, examinando la evidencia y buscando en paralelo.
- Búsqueda y análisis de múltiples partes de archivos adquiridos: Permitiendo buscar y analizar múltiples partes de la evidencia, lográndose buscar todos los datos involucrados en un caso en un solo paso. La evidencia se clasifica, si esta comprimida o no, y puede ser colocada en un disco duro y ser examinada en paralelo por el especialista.
- Posee diferente capacidad de almacenamiento: Lo que permite que los datos pueden ser colocados en diferentes unidades, como discos duros IDE o SCSI, drives ZIP, y Jazz, manteniendo su integridad forense intacta.
- Posee varios campos de ordenamiento, incluyendo estampillas de tiempo: Lo cual permite ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último

acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.

- Permite un análisis compuesto del documento: Permite la recuperación de archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el *slack* interno y los datos del espacio *unallocated*.
- Búsqueda automática y análisis de archivos de tipo zip y attachments de e-Mail, firmas de archivos, identificación y análisis: Esta herramienta verifica esta firma para cada archivo contra una lista de firmas conocida de extensiones de archivos. Si existe alguna discrepancia, como en el caso de que un sospechoso haya escondido un archivo o simplemente lo haya renombrado, detecta automáticamente la identidad del archivo, e incluye en sus resultados un nuevo ítem con la bandera de firma descubierta, permitiendo evidenciar de este detalle.
- Análisis electrónico del rastro de intervención: Sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento reciclado son a menudo puntos críticos de una investigación informática. Esta herramienta proporciona los medios prácticos de recuperar y de documentar esta información de una manera no invasora y eficiente.
- Vista de archivos y otros datos en el espacio *unallocated*: Esta herramienta posee una interfaz tipo Explorador de Windows y una vista del disco duro de origen, que permite ver los archivos borrados y todos los datos en el espacio *unallocated*, permitiendo examinar y determinar cuándo el archivo reescrito fue creado.

- Integración de reportes: Esta herramienta permite generar el reporte del proceso de la investigación forense como un estimado. En este documento realiza un análisis y una búsqueda de resultados, en donde se muestra el caso incluido, la evidencia relevante, los comentarios del perito, imágenes recuperadas, criterios de búsqueda y tiempo en el que se realizaron las búsquedas.

b.2.) Herramientas para el monitoreo y/o control de computadores

Algunas veces se necesita información sobre el uso de los computadores, por lo tanto existen herramientas que monitorean el uso de los computadores para poder recolectar información. Existen algunos programas simples como o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

b.3.) Herramientas de marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente.



El foco de la seguridad está centrado en la prevención de ataques. Algunos sitios que manejan información confidencial o sensible, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes.

b.4.) Herramientas de hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se debe de utilizar herramientas especiales para realizar este trabajo. Actualmente se han diseñado programas especiales para el trabajo del peritaje forense informático.

Además de esto, los medios informáticos utilizados por los peritos informáticos, deben estar certificados de tal manera, que éstos no hayan sido expuestos a variaciones magnéticas, ópticas (láser) o similares, por el riesgo de que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas.

De conformidad con lo que establece la guía para la mejor practica del examen forense de la tecnología digital, "la esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática, pues al igual que en la

medicina forense, un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de las causas de la muerte del paciente”.³¹

Dentro de la fase de recolección o recuperación de la evidencia, se considera que deben cubrirse las actividades mínimas siguientes:

- Establecer un criterio de recolección de evidencia digital según su volatibilidad, de la más volátil a la menos volátil.
- Documentar todas las actividades que el profesional a cargo de la recolección ha efectuado durante el proceso de tal manera que se pueda auditar el proceso en sí mismo y se cuente con la evidencia de este proceso.
- Asegurar el área donde ocurrió el siniestro, con el fin de custodiar el área o escena del delito y así fortalecer la cadena de custodia y recolección de la evidencia.
- Registrar en medio fotográfico o video la escena del posible ilícito, detallando los elementos informáticos allí involucrados.
- Levantar un mapa o diagrama de conexiones de los elementos informáticos involucrados, los cuales deberán ser parte del reporte del levantamiento de información en la escena del posible ilícito.

³¹ International Organization of computer evidence-IOCE-. **Líneas Guía para la mejor practica del examen forense de la tecnología digital.** http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html.(22 de diciembre de 2009).



c) Preservación de la evidencia

Una vez que se ha recolectado la evidencia del ataque, se ha de continuar siendo metódico y sobre todo conservando intactas las huellas del crimen; en tal sentido se debe asegurar esa evidencia a toda costa, por lo tanto no se recomienda iniciar el análisis forense sobre las copias recolectadas. Como primer paso se deberá realizar dos copias de las evidencias obtenidas, verificando o comprobando la integridad de cada copia realizada.

Se deben incluir firmas en la etiqueta de cada copia de la evidencia sobre el propio CD o DVD, incluyendo también en el etiquetado la fecha y hora de creación de la copia, nombre cada copia, para distinguirlas claramente del original. Estos datos deben trasladarse a otra etiqueta y pegarla en la caja contenedora del soporte, incluso se considera conveniente precintar el original para evitar su manipulación inadecuada.

Si se considera necesario y se decide extraer los discos duros del sistema para utilizarlos como evidencia, se deberá seguir el mismo procedimiento, colocando sobre ellos la etiqueta que la identifique como evidencia original, incluyéndose además la fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó. Se debe tomar en cuenta que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Toda precaución es poca para la conservación de la evidencia recabada.



Todo este procedimiento deberá ajustarse a lo que la normativa que sobre el manejo de evidencia y cadena de custodia ha implementado el Ministerio Público a través de las instrucciones correspondientes. Dicho control tiene como finalidad establecer las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Para tal efecto se considera conveniente preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento.

Dicho formulario o instrumento deberá documentar como mínimo lo siguiente:

- a. Dónde, cuándo y quién manejo o examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- b. Quién estuvo custodiando la evidencia, durante cuánto tiempo y dónde se almacenó.
- c. Cuando se cambie la custodia de la evidencia también deberá documentarse cuándo y cómo se produjo la transferencia y quién la transportó.

La finalidad de estas medidas es que el acceso a la evidencia sea restringido y quede claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas a intentos de acceso no autorizados.

La custodia de todos los elementos allegados al caso y en poder del perito informático y de los investigadores, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas

que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

d) Análisis de la evidencia

Una vez se ha recolectado la evidencia, tomado las imágenes de los datos requeridos y su debida cadena de custodia, es tiempo para iniciar el ensamble, análisis y articulación de los registros electrónicos para establecer los hechos de los eventos ocurridos en el contexto de la situación bajo análisis o establecer si hacen falta evidencias para completar o aclarar los hechos.

El objetivo de esta fase es “reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior al inicio del ataque, hasta el momento de su descubrimiento”.³² Este análisis se dará por concluido cuando conozcamos cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

El proceso de análisis de la evidencia digital o informática conlleva varias etapas; siendo las principales las siguientes:

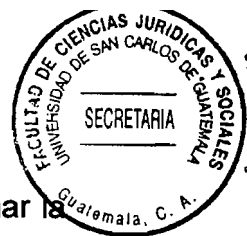
- Preparación para el análisis, adecuar el entorno de trabajo.
- Reconstrucción de la secuencia temporal del ataque.
- Determinación de cómo se realizo el ataque.

³² López Delgado, Miguel, op. cit., pág. 49.

Antes de comenzar el análisis de las evidencias deberá acondicionar un entorno de trabajo adecuado al estudio que desee realizar. Lo más recomendable es no trabajar sobre los discos duros originales recuperados; en tal sentido, la opción es trabajar con las imágenes que se recabaron como evidencias, o mejor aún con una copia de éstas, en todo caso se debe tener en cuenta de trabajar estas imágenes como se encontraban en el sistema comprometido.

Se puede trabajar de dos formas:

1. Preparando dos estaciones de trabajo en una de ellas, que contendrá al menos dos discos duros, se debe instalar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En ese mismo ordenador y sobre un segundo disco duro, se debe colocar las imágenes manteniendo la estructura y sistema de los archivos tal y como se encontraban en el equipo atacado. En el otro equipo instale un sistema operativo configurado exactamente igual que el del equipo atacado, además mantenga nuevamente la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como “conejiillo de indias” y realizar sobre él pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.
2. Otra de las formas es, utilizar software que le permita crear una plataforma de trabajo con varias máquinas virtuales (varios equipos lógicos independientes funcionando sobre un único equipo físico). Se puede también conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para



intentar hacer un análisis “en caliente” del sistema, para lo cual se deberá tomar la precaución de montar los dispositivos en modo sólo lectura.

Una vez montadas las imágenes del sistema comprometido en nuestra estación de trabajo independiente y con un sistema operativo anfitrión de confianza. El primer paso que deberá dar es crear una línea temporal de sucesos o reconstrucción de la secuencia temporal del ataque al sistema. Sin duda esta será la información que más tiempo llevará recopilar, pero será el punto de partida para el análisis.

Para comenzar se debe ordenar los archivos por sus fechas, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará fechas muy distintas a las de los ficheros más antiguos.

La idea es buscar ficheros y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. La mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus *aplicaciones* en lugares donde no se suele mirar, como por ejemplo en los directorios temporales.

Se debe buscar los archivos de sistema modificados tras la instalación del sistema operativo, así como los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros borrados por sus atacantes. Se debe procurar acceder al

espacio residual que hay detrás de cada archivo y leer en zonas que el sistema operativo no ve.

Se debe pensar que se está buscando *una aguja en un pajar*, por lo que se debe ser metódico, ir de lo general a lo particular, por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar la fecha de borrado y cotejarla con la actividad del resto de los archivos. Se tienen que buscar entradas anómalas y compararlas con la actividad de los ficheros. Además hay que buscar la creación de usuarios y cuentas extrañas sobre la hora que considere se inició el compromiso del sistema.

Una vez que disponga de la cadena de acontecimientos que se han producido, se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha. Estos datos, al igual que en el caso anterior, deberán obtenerse de forma metódica, empleando una combinación de consultas a archivos de logs, registro, claves, cuentas de usuarios, etc.

Un buen punto de partida es repasar los servicios y procesos abiertos que se recopilaron como evidencia volátil, así como los puertos TCP/UDP y conexiones que estaban abiertas cuando el sistema estaba aún vivo. En tal sentido, se deberá examinar con más detalle aquellas circunstancias que resultaron sospechosas cuando se buscó indicios sobre el ataque, y realizar con ellos una búsqueda de vulnerabilidades a través de Internet. Si ya se ha determinado cuál fue la vulnerabilidad que dejó al sistema

expuesto, se debe realizar una búsqueda en Internet algún *exploit* anterior a la fecha del compromiso, que utilice esa vulnerabilidad.

En este punto es muy importante ser metódico, reforzando cada una de las hipótesis planteadas, empleando una formulación causa-efecto, también es el momento de arrancar y comenzar a utilizar nuestra máquina *conejillo de Indias*. Pruebe sobre ella los exploits que ha encontrado, si he leído bien. Hay que recordar que en el análisis forense una premisa es que los hechos han de ser reproducibles y sus resultados verificables, por lo tanto se debe comprobar si la ejecución de ese exploit sobre una máquina igual que la comprometida y en perfecto estado (causa posible), genera los mismos eventos que ha encontrado entre sus evidencias (efecto verificable).

e) Identificación del autor o autores del incidente

Si ya se ha logrado averiguar cómo entraron en sus sistemas, ahora corresponde saber quién o quiénes lo hicieron. Para este propósito es de gran utilidad consultar nuevamente algunas evidencias volátiles que se recopiló en las primeras fases, por lo que hay que revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además se debe buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperaron por si el atacante eliminó alguna huella que quedaba en ellos. La identificación de los atacantes es de especial importancia para llevar a cabo acciones legales posteriores o investigaciones internas a su organización.

Para perseguir a los atacantes, se deberán realizar algunas pesquisas como parte del proceso de identificación. Primero se debe averiguar la dirección IP del atacante, para ello hay que revisar con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la escucha. También se podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de e-mail, conexiones fallidas, etc.

No hay que sacar conclusiones prematuras, muchos atacantes falsifican la dirección IP con técnicas especiales. Otra técnica de ataque habitual consiste en utilizar *ordenadores zombis*, éstos son comprometidos en primera instancia por el atacante y posteriormente son utilizados como lanzaderas del ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar a su atacante tendrá que verificar y validar la dirección IP.

También puede emplear de forma ética técnicas hacker, para identificar al atacante, hay que pensar que si este dejó ejecutándose en el equipo comprometido “un regalito” como una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas. Aquí entra en juego nuevamente el ordenador habilitado “conejillo de indias”.

Otro aspecto que es conveniente averiguar, es el perfil de sus atacantes, aunque sin entrar en detalles podrá encontrarse con los siguientes tipos:

1. **Hackers:** Son los más populares, se trata de personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos. Sus ataques suelen tener motivaciones de tipo ideológico (pacifistas, ecologistas, anti globalización, anti Microsoft, etc.) o simplemente lo consideran como un desafío intelectual).
2. **Script-kiddies:** Son una nueva especie que ha saltado a la escena de la delincuencia informática recientemente. Se trata de jóvenes que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y *ver qué pasa*. Su nombre viene de su corta edad y del uso intensivo que hacen de los scripts (guiones) de ataque que encuentran por Internet.
3. **Profesionales:** Son personas con muchísimos conocimientos en lenguajes de programación, en redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo UNIX. Suelen realizar los ataques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo, realizando un estudio meticuloso de todo el proceso que llevará a cabo, recopilando toda la información posible sobre sus objetivos, se posicionará estratégicamente cerca de ellos, realizará un tanteo con ataques en los que no modificará nada ni dejará huellas, cuando lo tenga todo bien atado entonces atacará.

f) Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense le ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron a sus sistemas. Esto le permitirá evaluar el compromiso de sus equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

- **Ataques pasivos:** En los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.
- **Ataques activos:** En los que se altera, y en ocasiones seriamente, tanto la información como la capacidad de operación del sistema.

Deberá tenerse en cuenta además, otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados. Por ejemplo ataques al cortafuegos, el router de conexión a Internet o Intranet, el servidor Web corporativo, los servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio o negocio que preste la organización y las relaciones de dependencia entre sus usuarios. Hay que pensar que una manipulación de una Web corporativa que realiza funciones meramente publicitarias tendrá un impacto mucho menor, pues que si eso mismo ocurre por ejemplo en eBay, que su negocio está basado totalmente en las subastas por Internet y un parón en su servidor Web puede traducirse en miles de euros de pérdidas por cada hora.



g) Documentación del incidente

El perito informático a cargo de la investigación es responsable de la precisión y completitud del reporte, sus hallazgos y resultados luego del análisis de la evidencia digital o registros electrónicos. En este sentido toda la documentación debe ser completa, precisa, comprensiva y auditable.

Para la ejecución de la fase de la documentación del incidente conocida como dictamen técnico, se recomienda lo siguiente:

- Documentar los procedimientos efectuados por el profesional a cargo.
- Mantener una bitácora de uso y aplicación de los procedimientos técnicos utilizados.
- Cumplir con exhaustivo cuidado con los procedimientos previstos para el mantenimiento de la cadena de custodia.
- Mantener una copia de la cadena de custodia y de la notificación oficial para adelantar el análisis de los registros electrónicos.
- Incluir las irregularidades encontradas o cualquier acción que pudiese ser irregular durante el análisis de la evidencia.
- Preparar una presentación del caso de manera pedagógica, que permita a las partes observar claramente el contexto del caso y las evidencias identificadas.
- Detallar las conclusiones de los análisis realizados sustentados en los hechos identificados.
- Evitar los juicios de valor o afirmaciones no verificables.

El dictamen o formato de presentación del informe de análisis de evidencia digital, debe detallar entre otros aspectos los siguientes:

1. Identificación de la agencia o empresa que adelantó el análisis.
2. Identificador del caso.
3. Investigador o profesional que ha adelantado el caso.
4. Identificación de las entidades que han provisto las evidencias.
5. Fechas de recepción y reporte.
6. Lista detallada de elementos recibidos para análisis donde se detallen aspectos como serial, marca y modelo.
7. Breve descripción de los pasos metodológicos seguidos.
8. Resultados de los análisis donde se detallen con claridad los hallazgos.
9. Conclusiones.

Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del perito o investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones.

Los peritos informáticos o forenses deben prepararse para declarar ante un jurado o juicio, por tanto, es probable que en el curso de la investigación o del caso, lo puedan llamar a declarar en ese instante o mucho tiempo después. Por tanto, el mantener un sistema automatizado de documentación de expedientes de los casos, con una

adecuada cuota de seguridad y control, es labor necesaria y suficiente para salvaguardar los resultados de las investigaciones y el debido cuidado, diligencia y previsibilidad del profesional que ha participado en el caso.

4.2. Determinar la relevancia de la evidencia

Dentro del proceso de análisis e investigación de las evidencias digitales es necesario valorar las mismas de tal manera que se identifiquen las mejores evidencias que permitan presentar de manera clara y eficaz los elementos que se desean aportar en el proceso y en el juicio que se lleve. El objetivo es que el ente que valore las pruebas aportadas observe en sus análisis y aportes los objetos de prueba más relevantes para el esclarecimiento de los hechos en discusión.

Para determinar la relevancia de la evidencia, se sugiere dos criterios para tener en cuenta a saber:

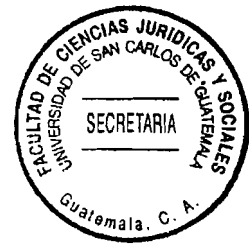
- a. Valor probatorio: Que establece aquel registro electrónico que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación y confiabilidad del sistema.
- b. Reglas de la evidencia: Que establece que se han seguido los procedimientos y reglas establecidas para la adecuada recolección y manejo de la evidencia.

Para demostrar la relevancia de la evidencia se considera que deben realizarse las acciones mínimas siguientes:

1. Demostrar con hechos y documentación que los procedimientos aplicados para recolectar y analizar los registros electrónicos son razonables y robustos.
2. Verificar y validar con pruebas que los resultados obtenidos luego de efectuar el análisis de los datos, son repetibles y verificables por un tercero especializado.
3. Auditar periódicamente los procedimientos de recolección y análisis de registros electrónicos, de tal manera que se procure cada vez mayor formalidad y detalles en los análisis efectuados.
4. Fortalecer las políticas, procesos y procedimientos de seguridad de la información asociados con el manejo de evidencia digital.
5. Procurar certificaciones profesionales y corporativas en temas relacionados con computación forense, como una manera de validar la constante revisión y actualización del tema y sus mejores prácticas.

4.3. Evaluación de los procedimientos realizados en la investigación

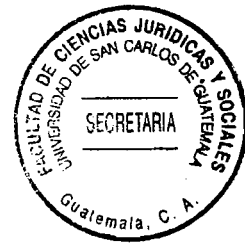
Finalmente y no menos importante, es el hecho de que el perito informático o investigador mantenga un ejercicio de autoevaluación de sus procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses, de tal manera que el ciclo de calidad debe incluir estas actividades - Planear, Hacer, Verificar y Actuar, y la misma sea una constante que permita incrementar la actual confiabilidad de sus procedimientos y cuestionar sus prácticas y técnicas actuales para el mejoramiento de su ejercicio profesional y la práctica de la disciplina.



4.4. Dificultades del investigador forense

El perito o investigador forense requiere de varias habilidades que no son fáciles de adquirir, es por esto que el usuario normal se encontrará con dificultades como las siguientes:

1. Carencia de software especializado para buscar la información en varios computadores.
2. Posible daño de los datos visibles o escondidos, aún sin darse cuenta.
3. Será difícil encontrar toda la información valiosa.
4. Es difícil adquirir la categoría de *experto* para que el testimonio personal sea válido ante una corte.
5. Los errores cometidos pueden costar caro para la persona o la organización que representa.
6. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.
7. Falta de experiencia para mostrar, reportar y documentar un incidente computacional.
8. Dificultad para conducir la investigación de manera objetiva.
9. Dificultad para hacer correctamente una entrevista con las personas involucradas.
10. Reglamentación que puede causar problemas legales a la persona.



CAPÍTULO V

5. Panorama general de la legislación guatemalteca sobre los delitos informáticos y la situación actual del peritaje informático

Como se ha analizado, la problemática de los delitos informáticos ha sido ampliamente estudiada a nivel doctrinario, así también ha sido estudiado el que hacer de los peritos informáticos, cada vez que se ven en la necesidad de recabar evidencia en este tipo de delitos. Se hace ineludible entonces, relacionar todo ese cúmulo de conocimientos doctrinarios con lo que establece nuestra legislación en relación al tema, partiendo desde la Constitución Política de la República, como norma suprema, pasando por la normativa ordinaria, normativa reglamentaria, hasta llegar a la normativa individualizada, que en nuestro caso lo constituirán las directrices o instrucciones que emite el Ministerio Público. Dentro de este análisis, se establecerá la competencia de varias instituciones de la administración de justicia con competencia en este ámbito.

5.1. La persecución penal de los delitos informáticos en la legislación de Guatemala

Conforme las disposiciones contenidas en la Constitución Política de la República vigente, en su Título V, Capítulo VI, Artículo 251 señala que el Ministerio Público es una institución auxiliar de la administración pública y de los tribunales con funciones,



autónomas, cuyos fines principales son velar por el estricto cumplimiento de las leyes del país.

Dicho precepto es desarrollado en el Decreto No. 40-94 del Congreso de la República, que contiene la Ley Orgánica del Ministerio Público, la cual en su Artículo 2, numeral 1), establece que es función del Ministerio Público, entre otras la de investigar los delitos de acción pública y promover la persecución penal ante los tribunales, según las facultades que le confieren la Constitución, las leyes de la República, y los Tratados y Convenios Internacionales.

Dicha normativa coincide con lo que preceptúa el Decreto No. 51-92 del Congreso de la República, que contiene el Código Procesal Penal, en su Artículo 107, que establece que el ejercicio de la acción penal corresponde al Ministerio Público como órgano auxiliar de la administración de justicia conforme las disposiciones de este Código.

Hasta aquí, del análisis de la normativa relacionada, se podría determinar que para efectos de la investigación de los delitos informáticos, el ejercicio de la acción penal correspondería al Ministerio Público; sin embargo y de conformidad con lo que establece el Artículo 24 Quáter del Código Procesal Penal que regula que serán perseguibles, sólo por acción privada, entre otros, los delitos relativos al derecho de autor, la propiedad industrial y delitos informáticos. En este caso se procederá únicamente por acusación de la víctima, conforme el procedimiento especial regulado en el Libro Cuarto, Título III, del Código Procesal Penal, referente al Juicio por Delitos de Acción Privada.

Como se ha venido analizando, los delitos informáticos poseen una naturaleza particular, que va desde la dificultad de identificar el bien jurídico tutelado, los medios especializados mediante los cuales se cometen, la particularidad y dificultad de identificar al sujeto activo, y la necesidad de procedimientos técnicos para su comprobación.

En este orden de ideas, para este tipo de delitos, cabe ubicar esta particularidad en lo que establece el Artículo 476 del Código Procesal Penal, al referirse al Juicio por Delitos de Acción Privada, que establece que cuando fuere imprescindible llevar a cabo una investigación preliminar por no haber sido posible identificar o individualizar al querellado o determinar su domicilio o residencia o fuere necesario establecer en forma clara y precisa el hecho punible, el querellante lo requerirá por escrito, indicando las medidas pertinentes. El tribunal así lo acordará y enviará el expediente al Ministerio Público para que actúe conforme a las reglas de la investigación preparatoria, quien lo devolverá una vez concluidas las diligencias.

En tal sentido, el proceso de investigación de los delitos informáticos, retorna nuevamente a la competencia del Ministerio Público, por lo cual, si bien en este tipo de delitos, la acción se promoverá en forma privada mediante la presentación de la querrela respectiva, la fase de investigación preparatoria corresponde al Ministerio Público.

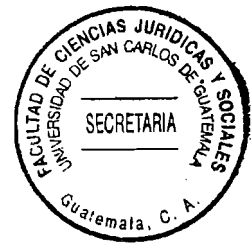
Es de tomar en cuenta también, como se ha comentado en los primeros capítulos de la presente investigación, sobre la clasificación que se hace de los delitos informáticos,

en la cual se determinaba que existen delitos en los cuales se utiliza los medios informáticos para la comisión de delitos, sin que estos estén tipificados específicamente como delitos informáticos, como el caso del terrorismo o el espionaje, en los cuales se pueden estar utilizando medios informáticos para la comisión de los mismos, la investigación preparatoria correspondería al Ministerio Público.

Razón por la cual, indistintamente si la acción delictiva se encuadra en cualesquiera de los delitos que el Código Penal tipifica como delitos informáticos, o bien si constituye cualesquiera de los otros delitos en que se utilicen medios informáticos para su comisión, debe quedar claro que el proceso de investigación corresponderá siempre al Ministerio Público.

5.2. La competencia en la función de peritaje de conformidad con la legislación guatemalteca

Habiendo hecho la aclaración anterior, se debe analizar a quien, dentro del Ministerio Público, correspondería realizar el trabajo de investigación de los delitos informáticos y para tal efecto cabe estudiar lo que establece el Artículo 40 de la Ley Orgánica del Ministerio Público, que regula lo referente a la Dirección de Investigaciones Criminalísticas, estableciendo dicho artículo que dicha Dirección estará integrada por un cuerpo de peritos en distintas ramas científicas, dependerá directamente del Fiscal General de la República, tendrá a su cargo el análisis y estudio de las pruebas y otros medios de convicción que coadyuven al esclarecimiento de los hechos delictivos que investiguen los órganos del Ministerio Público.



En base a lo cual se podría señalar que la investigación de los delitos informáticos correspondería a los peritos de la Dirección de Investigaciones Criminalísticas del Ministerio Público; sin embargo en la parte considerativa del Decreto No. 32-2006, del Congreso de la República, que contiene la Ley Orgánica de Instituto Nacional de Ciencias Forenses de Guatemala se establece que la función jurisdiccional necesita de medios de prueba válidos y fehacientes en los procesos judiciales y en consecuencia es indispensable la cooperación de los expertos y peritos en ciencias forenses, que apliquen los avances tecnológicos, metodológicos y científicos de la medicina legal y criminalística, como elementos esenciales en la investigación criminal y de cualquier otra naturaleza.

Además, se establece que el servicio médico forense que forma parte del Organismo Judicial, no responde en la actualidad a los requerimientos judiciales ni a la necesaria separación que debe existir entre la investigación criminalística y la administración de justicia, ni mucho menos al ente responsable de la persecución penal, razones que determinan la necesidad de crear un ente independiente que se responsabilice de todo lo relativo a la investigación técnica y científica, especialmente en la ocurrencia de hechos delictivos.

Sobre dichas consideraciones, se crea el Instituto Nacional de Ciencias Forenses de Guatemala –INACIF-, como una institución auxiliar de la administración de justicia, con autonomía funcional, personalidad jurídica y patrimonio propio. Dicha institución tiene competencia a nivel nacional y la responsabilidad en materia de peritajes técnicos

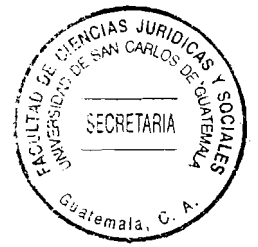


científicos de conformidad con lo que establece su Ley orgánica. Por lo cual se debe entender que la competencia en materia de peritajes técnicos corresponde, de conformidad con la ley a este Instituto.

El INACIF fundamenta sus actuaciones, entre otros, en los siguientes principios:

- a. **Objetividad:** En el ejercicio de sus funciones mantendrá objetividad e imparcialidad y observará el más escrupuloso respeto y acatamiento a la Constitución Política de la República y leyes; y en lo atinente a los tratados y convenios internacionales reconocidos y ratificados por Guatemala.
- b. **Profesionalismo:** Sujetará sus actuaciones a los más altos niveles de rigor técnico, científico y ético, teniendo como metas la eficiencia y la efectividad de aquellas;
- c. **Publicidad y transparencia.** Los procedimientos y técnicas periciales que se apliquen serán sistematizadas y ordenadas en protocolos o manuales, los cuales serán público y accesibles para los interesados, debiendo realizar actualizaciones periódicas.
- d. **Actualización técnica:** Incorporará, con base a sus posibilidades económicas, las innovaciones tecnológicas y científicas para mejorar sus actuaciones, así como el establecimiento de programas de capacitación y actualización para su personal técnico.

De conformidad con lo que se ha comentado en capítulos anteriores referente al perfil y actuar del perito informático, vemos que existe coincidencia entre estos principios de actuación establecidos en la Ley Orgánica del INACIF, y lo que doctrinariamente se establece como parte del perfil para este tipo de peritos.



Sin embargo, y pese a lo comentado, cabe analizar el Artículo 48 de la Ley Orgánica del INACIF, el cual establece la continuidad del servicio, al señalar que los servicios que están bajo responsabilidad del Organismo Judicial, Ministerio Público y Ministerio de Gobernación, en materia forense, continuarán prestándose por los mismos, hasta el momento en que el INACIF se encuentre integrado y organizado de conformidad con la presente Ley.

Actualmente se sabe que a este Instituto de Ciencias Forenses, le ha costado mucho integrarse y organizarse, particularmente debido a la falta de recursos financieros, lo que ha imposibilitado desarrollar e implementar un equipo de técnicos especialistas en informática que le permitan realizar los peritajes necesarios en los delitos informáticos; por tal razón y de conformidad con la normativa analizada el Ministerio Público debiese seguir prestando el servicio de la elaboración de peritajes en este tipo de delitos, con su equipo técnico especializado.

Al realizar un análisis de la estructura organizativa administrativa del Instituto de Ciencias Forenses, se determina que dentro del Área Pericial, específicamente dentro del Departamento Técnico Científico, no existe una Sección de Informática Forense, que cuente con los técnicos especialistas, que puedan realizar la actividad del peritaje informático, lo que confirma que, corresponde al Ministerio Público a través de la Dirección de Investigaciones Criminalísticas, realizar la función de los peritajes informáticos en el caso de los delitos informáticos.



De conformidad con lo que establece la Ley Orgánica del Ministerio Público, esta Institución tendrá a su cargo el análisis y estudio de las pruebas y otros medios de convicción que coadyuven al esclarecimiento de los hechos delictivos que investiguen y corresponde al fiscal a cargo de la investigación de un delito reunir los elementos de convicción de los hechos punibles en forma ordenada, debiendo también proponer la prueba pertinente y necesaria, y producirla en el debate, debiendo hacer una interpretación restrictiva de las normas de incorporación de la prueba por lectura al juicio oral.

5.3. La metodología de la investigación del Ministerio Público en los delitos informáticos

Se ha determinado mediante el análisis anterior que, la investigación de los delitos informáticos corresponde al Ministerio Público. Esta institución, con el objeto de realizar los fines del proceso en cuanto a la averiguación del delito, las circunstancias en que pudo haberse cometido, la determinación de la posible participación del sindicado y su condena, debe plantearse una metodología de su trabajo de investigación.

Para tal efecto, con fecha 1 de febrero del año 2006, el Fiscal General, formula la Instrucción No. 001-2006, Instrucción General para la Aplicación de la metodología de la Investigación Criminal, dicha instrucción tiene por objeto mejorar la planificación, ordenamiento, control y seguimiento de las investigaciones criminales realizadas por los

funcionarios del Ministerio Público, a efecto de que se realiza una construcción efectiva y lógica de la acusación.

Dicha instrucción señala que en la investigación debe aplicarse un método que permita construir progresivamente una teoría para cada caso, debiendo elaborarse una hipótesis criminal preliminar hasta culminar con la conclusión que permitirá ejercer con éxito la acción penal ante los órganos jurisdiccionales. En dicho método debe incluirse un plan de investigación, el cual entre sus componentes debe incluir el componente probatorio, en el cual se determinarán los medios que se utilizaran para probar los elementos facticos. En el caso particular de los delitos informáticos, y ante la necesidad de apoyo de un investigador criminal especializado, en el plan de investigación se deberá establecer la necesidad del peritaje informático o digital para la comprobación de este tipo de delitos.

De conformidad con dicha instrucción, para realizar una investigación adecuada, se deberá tomar en cuenta la guía básica para la solicitud de análisis sobre indicios levantados en la escena del crimen, allanamientos, inspecciones o registros, la cual constituye un instrumento orientador para el requerimiento de análisis técnicos o científicos a realizarse sobre los indicios encontrados.

Al realizarse un análisis sobre la Guía básica para la solicitud de análisis, se logra determinar que la misma no incluye análisis sobre evidencia informática o digital; razón por la cual se puede considerar que esta instrucción al no abarcar la evidencia

informática, no orienta a los Fiscales sobre qué debe de solicitarse a los técnicos o peritos, en el caso del peritaje de la evidencia digital o informática.

5.4. El procesamiento de la escena del crimen en los delitos informáticos

Dentro del trabajo de investigación, el Ministerio Público, considera que la escena del crimen constituye el primer escenario de investigación de los delitos flagrantes, por lo que su adecuado procesamiento permitirá dotar a los fiscales, de indicios que le posibiliten construir y posteriormente reafirmar, desestimar o modificar la hipótesis del caso investigado, con lo cual podrá tomar una serie de decisiones en torno a sus actividades de investigación.

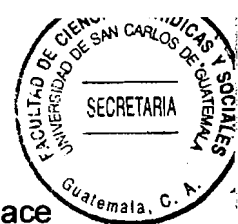
Ante dicha situación, el Fiscal General, con fecha 30 de octubre del año 2006, formula la Instrucción General No. 7-2006, denominada Instrucción General para la Aplicación del Manual de procedimientos para el procesamiento de escenas del crimen.

En dicha Instrucción se establece que el procesamiento de la escena del crimen tiene por objeto inspeccionar el área, fijar la escena, recolectar y resguardar todo objeto material, sin importar el tamaño, que esté relacionado con un presunto hecho delictivo y que permita establecer la existencia del hecho y las circunstancias en que pudo ser cometido. En el caso particular de los delitos informáticos, es de tomar en cuenta la particularidad de este tipo de delitos y la forma en que puede presentarse la escena de este tipo particular de delitos.

El Manual que habilita dicha instrucción, establece que debe elaborarse un plan de procesamiento por parte del Fiscal. En el caso de los delitos informáticos, debe tomarse en cuenta lo particular de este tipo de delitos, las posibles escenas del crimen que pueden presentarse y lo especial de la evidencia informática. En tal sentido, en la elaboración del plan de procesamiento de la escena en un delito informático o digital, el Fiscal deberá evaluar si el Técnico especialista del Departamento de Recolección de Evidencias del Ministerio Público, posee la capacidad y técnica necesaria para realizar la recolección de las evidencias digitales, en virtud de que para la recolección de las mismas, como quedo establecido en capítulos anteriores, se deben utilizar procedimientos específicos para evitar la contaminación de la evidencia o pérdida de información.

Si se considerará que dichos técnicos no tienen la capacidad necesaria, deberá acompañarse o solicitar el auxilio de un Perito en Informática Forense, para que este proceda a la recolección de la evidencia digital, pudiendo el técnico levantar o recopilar toda aquella evidencia que no sea digital.

Será responsabilidad del Perito en Informática Forense, la recolección de la evidencia, el marcaje y embalaje de la misma, lo cual lo realizará de conformidad con las técnicas especiales correspondientes, a efecto de garantizar su pureza y conservación y que más adelante no se promuevan objeciones en cuanto a la evidencia recabada y se garantice su admisibilidad como medio probatorio en la etapa del juicio penal.



En tal sentido, se debe entender que la Instrucción y Manual a los que se hace referencia, es una guía general para el procesamiento de escenas de crimen, y no puede contener o referirse a cada caso en particular, razón por la cual consideramos que por lo particular de la materia en los delitos informáticos, debiera de existir una instrucción especial en cuanto al manejo de escena del crimen en este tipo de delitos.

Cabe hacer mención que en algunos casos se puede presentar la situación de la incautación y el bloqueo de sistemas informáticos completos, al igual que en el caso de cualquier otra prueba. La incautación de todo un sistema informático puede resultar técnicamente inviable, o bien ser desproporcionada por tratarse de un entorno con muchos usuarios a los que interesa el contenido de los datos. Cuando se pretende obtener datos para determinadas investigaciones, las facultades legales tradicionales pueden resultar insuficientes a causa de: a) problemas relacionados con la obtención de acceso al sistema informático; b) la naturaleza intangible de los datos; y c) el hecho de que los datos puedan estar almacenados en un sistema conectado, situado fuera del local registrado.

Queda establecido que el problema que se presenta por parte de las instituciones llamadas a realizar la persecución penal de los delitos informáticos, es la falta de preparación, tanto del Ministerio Público, como de la Policía Nacional Civil, esto por un lado por la falta de infraestructura necesaria, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de este tipo de delitos, así como la falta de información por parte de los Fiscales y agentes de

investigación de la Policía Nacional, en virtud de no existir una Unidad Especializada para la investigación de este tipo de delitos.

Por otro lado también, la falta de preparación de jueces y magistrados, quienes se ven confundidos por la particular especialidad del tema y su común confusión con los delitos de orden común.

5.5. Inconvenientes en la investigación y el proceso pericial ante los delitos informáticos

Como se ha determinado hasta aquí, la investigación de la delincuencia informática, no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los peritos informáticos buscan vestigios digitales que de acuerdo a sus características suelen ser volátiles y de vida corta.

Es preciso considerar que la internet brinda grandes beneficios a los usuarios, pero su fácil acceso también podría perjudicarlos. Los usuarios de internet, corren un alto riesgo de ser perjudicados mediante actos delictivos como la estafa, o cualquier otro ataque, relacionados con las tecnologías. Las cifras sobre los delitos informáticos, son inciertas, las pocas denuncias que se presentan, ya sea por la falta de conocimiento o interés impide la lucha contra este tipo de delitos.

Es importante considerar los retos particulares que están latentes a todo nivel e incluso para los actores involucrados, en el manejo de los Delitos Informáticos, sean estos el

Ministerio Público, la Policía Nacional Civil, la Corte Suprema de Justicia, investigadores, y hasta la misma sociedad.

Podemos señalar como retos que se deben superar con relación al delito informático, los siguientes:

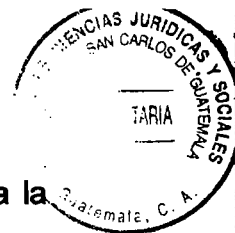
1. Marco legal inadecuado.
2. Formación profesional de los peritos e investigadores.
3. Limitaciones tecnológicas.
4. Creación de un protocolo para la ejecución del peritaje informático.

a) Marco legal inadecuado

Debemos considerar la problemática Jurídica, ya que si bien es cierto en nuestro país, se han iniciado los primeros pasos en la generación de la modificación del Código Penal vigente, al incluirse los delitos informáticos, aún dicha normativa no es suficiente para abarcar la problemática que representan este tipo de ilícitos, y el tratamiento de esta nueva modalidad de delincuencia, por ello es necesaria la precisión de un marco legal que contemple a los delitos informáticos de una manera integral.

En este contexto podemos señalar como inconvenientes para el manejo de delitos informáticos los siguientes:

- Falta de la infraestructura y tecnologías adecuada en los entes u organismos de investigación como: el Ministerio Público y la Policía Nacional Civil. Las investigaciones o experticias a nivel informático en su mayoría se dan por



denuncias realizadas bajo otro contexto de delitos tales como: robo, daño a la propiedad, estafas, entre otros, que son investigados por Fiscalías de delitos comunes del Ministerio Público, y a lo interno de estas Fiscalías por la Dirección de Investigaciones Criminalísticas o el Departamento Informático, debido a la falta de una regulación, o unidad que opere este tipo de infracciones.

- Falta de iniciativas que permitan el desarrollo de brigadas y unidades estructuradas y especializadas, para la investigación de los delitos de índole informático, nacional y transnacional, desde su inicio con el levantamiento de evidencias hasta la aplicación de procedimientos de mayor complejidad.
- Falta de especificaciones claras y concisas en la petición de pericias informáticas, elemento importante que cabe destacar, ya que durante las peticiones de pericias informáticas solicitadas por medio de la autoridad, incurre en términos amplios sobre la práctica de peritaje informático, en la cual no se especifican requerimientos sólidos sobre lo que se va a investigar, en cuyo caso es importante la comunicación entre los fiscales, jueces y tribunales con los investigadores o peritos de la rama de informática, previo a establecer la diligencia de la pericia.
- Falta de una comunicación efectiva entre los especialistas informáticos y los judiciales; mantener un lenguaje común entre los especialistas de informática y los operadores judiciales es trascendental, principalmente, al exponer por parte del perito informático, los criterios utilizados en el desarrollo de la investigación ante una investigación judicial.

- Otro aspecto, a considerar es la problemática legal, que se presenta cuando este tipo de delitos traspasa las fronteras y las jurisdicciones, lo que pone en relieve la importancia de la cooperación internacional.

b) Formación

La formación surge como factor incluyente para cada uno de los involucrados que dirigen la investigación, pues muchas veces se encuentran confundidos ante el tratamiento de este tipo de delitos. En el contexto de la formación podemos señalar como inconvenientes para el manejo de delitos informáticos los siguientes:

- Falta de preparación para los miembros de los organismos que persiguen la delincuencia en el campo informático (Ministerio Público, Policía Nacional Civil, jueces, etc.).
- Falta de preparación a nivel de formación en el ámbito de los procedimientos y técnicas utilizadas para la persecución de los delitos informáticos por parte de los especialistas.
- Falta de programas de capacitación que atañen a los delitos informáticos.
- Falta de cultura informática, aquellos individuos que no tienen conocimientos informáticos básicos (Internet, correo electrónico), son más vulnerables y tienen mayores probabilidades de ser víctimas de un delito.

La investigación forense en informática es un campo de la ciencia que requiere una formación técnica avanzada y detallada en las tecnologías y aplicaciones de software que le permita explorar con profundidad los elementos aportados y poder relacionarlos

para fundar hipótesis coherentes y sustentadas en los dictámenes periciales informáticos.

Es importante destacar bajo este contexto, que algunas Universidades del país, han incluido en su pensum de estudio para las carreras de Abogacía y Notariado, y de Ingeniería en Sistemas, los cursos sobre la Informática legal, que permiten preparar a los profesionales desde una etapa muy temprana, sobre aspectos generales como las regulaciones existentes y que atañen a las tecnologías, así como también, el desarrollo y progreso de países vecinos en cuanto a la legislación para perseguir estos actos ilícitos no solo bajo la perspectiva local sino transnacional.

c) Limitaciones tecnológicas

La distribución de las tecnologías de la información y las comunicaciones en todo el mundo no es uniforme. Existen vastas diferencias en los tipos y números de adelantos tecnológicos en diferentes partes del mundo. La denominada brecha digital fue reconocida en la Declaración del Milenio de las Naciones Unidas del 2000.³³

La Declaración de Principios adoptada por la Cumbre Mundial sobre la Sociedad de la Información, establece que los beneficios de la revolución de la tecnología y la información están actualmente distribuida de manera desigual entre los países desarrollados y en desarrollo y dentro de las sociedades. Esta declaración también

³³ Programa de las Naciones Unidas para el Desarrollo. **Un Mundo de experiencias en desarrollo**, <http://www.undp.org/spanish/about/> (31 de octubre de 2009).

incluye el compromiso de transformar esta brecha digital en una oportunidad digital para todos en particular para aquellos que corren el riesgo de quedar rezagados y marginados.

Considerando este aspecto, no es de sorprenderse entonces que en el Ministerio Público, para la investigación de este tipo de delitos, se utilice a los técnicos del Departamento de Informática (con funciones administrativas), para realizar la recabación de evidencia en las escenas del crimen y para el análisis de peritaje de la evidencia digital recabada, que en muchas ocasiones no cuentan con la experiencia, los medios u herramientas y la formación adecuada para la ejecución de la investigación del acto ilícito.

Si bien es cierto que, de conformidad con el Decreto No. 21-2006 del Congreso de la República, en el año 2006, entró en vigencia la Ley Contra la Delincuencia Organizada, la cual posibilita el monitoreo y escucha de llamadas telefónicas, correos electrónicos, y todo lo que está inmerso dentro del espectro electromagnético de comunicaciones, como un medio para la investigación de grupos delictivos organizados y delitos de grave impacto social; esta iniciativa innovadora no permite el tratamiento de los delitos informáticos desde una perspectiva integral; siendo este proyecto uno, entre los que se deberían fomentar para el desarrollo de una política en pro de la persecución de la delincuencia informática, que permita el control integral de los delitos de índole tecnológico.

En igual forma, la falta de infraestructura, herramientas modernas y demás implementos tecnológicos requeridos para la persecución de este tipo de delitos incrementa el riesgo de que la investigación sea realizada de una manera inadecuada por parte de los especialistas.

d) Protocolo para la ejecución del peritaje informático

Los procedimientos de recolección y análisis de evidencia digital generalmente se encuentran sustentados en herramientas de software, procedimientos internacionalmente aceptados y experiencia del investigador. Mientras mayor sea la capacidad de las herramientas para identificar, recolectar, asegurar y analizar la evidencia en medios electrónicos, mejores resultados y controles se pueden mantener.

Sin embargo, no se puede perder de vista que el software no es infalible y requiere un proceso de depuración y pruebas que exige una revisión por parte de la comunidad científica, identificación y valoración de sus tasas de error, resultados de uso en casos anteriores, entre otras, que permitan aumentar la confiabilidad y la repetitividad de los resultados.

Por tal razón, se hace necesario fijar un protocolo que defina los procedimientos estándares mínimos a aplicar en la recolección de la evidencia digital y los procedimientos para la ejecución del trabajo del análisis de la misma por parte del perito, así como de la forma de presentación del informe o dictamen pericial. Este protocolo garantizará que la evidencia recolectada y analizada sea admisible como



medio probatorio en la etapa del juicio penal, y permitirá utilizar un mismo lenguaje de fácil comprensión para fiscales del Ministerio Público y jueces del Organismo Judicial.

Dicho protocolo permitiría comprender y analizar en contexto las condiciones requeridas de la evidencia digital y así establecer procedimientos de valoración de pruebas digitales que permitan mantener un debido proceso con las garantías requeridas para las partes alrededor de la evidencia aportada al mismo. Así mismo, aumentar la capacidad de los jueces para comprobar y verificar la evidencia digital, que permita avanzar hacia una actualización de los procedimientos probatorios, fortaleciendo así las apreciaciones y fallos que se emitan.

e) Otras consideraciones

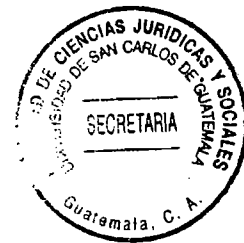
Un factor muy relevante con el que debe contar el profesional acreditado y que cumple como perito profesional es su ética profesional, la labor que cumple como investigador es altamente sensitiva, en la que se debe tener mucho cuidado de no cometer errores, tener una adecuada madurez emocional juega un papel fundamental, para soportar la presión durante su ejercicio de investigación, y utilizar la máxima objetividad al plasmar sus conclusiones.

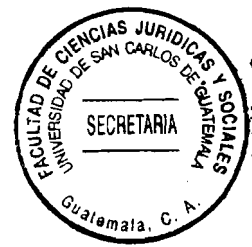
Por otro lado, la falta de información o poco interés de las personas, muchas veces las denuncias no se presentan, por lo cual, es importante promover el desarrollo de programas y campañas, orientadas hacia las leyes definidas y relacionadas con la información y la informática, en las que se difunda, comunique y establezca acciones de



información prevención, y denuncia de actos delictivos que laceren y pongan en peligro el bien jurídico protegido en el campo informático que es la información.

Finalmente se puede decir que la evidencia digital es un desafío para la justicia, que sugiere una evolución de la misma para disminuir la brecha técnico-legal existente y, un reto para los profesionales de la tecnología, para descubrir en el ordenamiento legal una manera de soportar las investigaciones con material y medios tecnológicos más idóneos y precisos.





CONCLUSIONES

1. Los delitos informáticos causan grave daño al estilo de vida moderno, debido a la dependencia de la sociedad a las nuevas tecnologías informáticas, por lo que surge la necesidad de luchar contra dichas conductas delictivas y de tipificar determinadas conductas, a fin de que estas sean efectiva y positivamente perseguidas y castigadas en el ámbito penal.
2. Jurídica y doctrinariamente no existe consenso en cuanto a cuál es el bien jurídico tutelado en este tipo de delitos, concluyéndose en que los mismos tienen un carácter pluriofensivo o complejo, ya que simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo de delitos.
3. Los delitos informáticos poseen una naturaleza especial, que requiere de procedimientos y técnicas especiales de investigación, debido a los bienes jurídicos que tutelan, las características particulares de los sujetos activos que no responder al denominador común de los delincuentes y los medios y modos de la comisión de dichos delitos.
4. El perito informático, no siempre es un profesional especialista en la ciencia informática, ni tampoco posee conocimientos adicionales de criminalísticas y derecho, que le permitan emitir un dictamen con la objetividad y requerimientos



legales necesarios para que el mismo tenga efectividad y eficiencia como medio probatorio.

5. Los delitos informáticos en Guatemala, no son investigados con propiedad, por no existir en el Instituto Nacional de Ciencias Forenses y el Ministerio Público un departamento técnico con la especialidad para este tipo de delitos y al no existir un protocolo con los procedimientos mínimos para la recolección de evidencia y su análisis, que permita su validación y aceptación como medio de prueba.



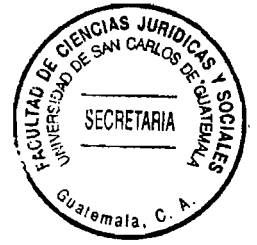
RECOMENDACIONES

1. Se debe realizar un análisis de la legislación penal vigente por parte del Organismo Legislativo en lo relativo a los delitos informáticos, a efecto de determinar si los tipos delictivos vigentes, alcanzan a cubrir todas las acciones que en la práctica atentan contra los sistemas informáticos y el uso adecuado de los mismos.
2. El Ministerio Público debe establecer un protocolo con procedimientos mínimos, para la recuperación de la evidencia informática y su evaluación pericial, el cual debe contener el perfil del perito informático, los procedimientos de recuperación de la evidencia informática, de su peritación y requisitos del informe pericial, que permitan la confiabilidad de esta evidencia como medio de prueba.
3. El Instituto Nacional de Ciencias Forenses- INACIF- debe incluir dentro del perfil del perito informático, la formación profesional en aspectos de criminología y ciencias jurídicas; además procurar su capacitación y actualización continua que le permita mantenerse al día de los avances tecnológicos en la ciencia informática.
4. A través de una instrucción del Fiscal General del Ministerio Público debe de ser autorizado, un protocolo de procedimientos en la investigación informática, el cual debe ser implementado por medio de un Manual Para la investigación de delitos informáticos.



5. Se debe crear en el Ministerio Público, en la Dirección de Investigaciones Criminológicas, una Unidad de Investigación Informática, con competencia en la recuperación de la evidencia digital en las escenas del crimen de los delitos informáticos y su análisis pericial, debiendo estar dotada de personal adecuado y equipos y programas informáticos apropiados.

BIBLIOGRAFÍA



- ACURIO DEL PINO, Santiago. **Introducción a la informática forense**. Revista de derecho informático, alfa-redi, No. 110, septiembre, 2007. <http://www.alfaredi.org/rdi-articulo.shtml?x=9608>.
- BATISTA, Eusebio. **Instituciones para la defensa de los derechos humanos en el aspecto penal**. Memoria final para optar por el título de Licenciado en Derecho. Universidad Nacional Autónoma de México UNAM.2001.
- BARRIENTOS PELLECCER, César. **Derecho Procesal Penal guatemalteco**. Tomo I, 2ª Edición. Magna Tierra Editores, 1997.
- BERTOLINO, Pedro. **El funcionamiento del Derecho Procesal Penal**. Buenos Aires, Argentina. Depalma, 1985.
- BINDER BARIZZA, Alberto. **Derecho Procesal Penal, introducción al Derecho Procesal Penal**. Buenos Aires, Argentina, (s.e.), 1993.
- BORJA OSORIO, Guillermo. **Derecho Procesal Penal**. Editorial Carioca, México, (s.f.).
- CALLEGARI, Nidia. **Poder informático y delito**. Barcelona, España, (s.e.), 1985.
- CAMACHO LOSA, Luis. **El Delito Informático**. Madrid, España, (s.e.), 1987.
- CANO, Jeimy J. **Estado del arte del peritaje informático en Latinoamérica**. http://www.alfaredi.com//apcaaalfaredi/img_upload/374d0ee90831e4ebaa1def162fa50747/Estado_del_Arte_del_Peritaje_Informatico_en_Latinoamerica.pdf.
- CASTILLO JIMENÉZ, María Cinta y Ramallo Romero, Miguel. **El delito informático**. Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático. 22-24 junio 1989.
- DE LEÓN VELASCO, Héctor Aníbal y De Mata Vela, José Francisco. **Curso de Derecho Penal guatemalteco, parte general y parte especial**. (s.e.), Guatemala. 2003.



Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, abril 2000, <http://www.uncjin.org/Documents/congr10/10s.pdf>,

DOTEL MATOS, Héctor y Almazor González C. **Manual de Derecho Penal general y procedimiento penal**. Editora Corripio. República Dominicana, (s.f.).

DUARTE, Nosei. **Comportamiento agresivo y actividad antisocial (seguridad ciudadana)**. Escuela Nacional de Policía, Argentina, 1998.

DUARTE, Nosei. **Manual básico de la investigación criminal**. Escuela Nacional de Policía, Argentina, 1999.

FOURNIER, Agustina. **La prueba pericial informática**
<http://www.compendium.com.ar/juridico/peri2.html>.

GARRIDO MONTT, Mario. **Nociones Fundamentales de la teoría del delito**. Santiago de Chile. Editorial Jurídica de Chile. 1992.

GUTIÉRREZ FRANCÉS, María Luz. **Fraude Informático y estafa**, ed. Ministerio de Justicia, Centro de Publicaciones, Madrid, 1991.

HUERTA MIRANDA, Marcelo y Líbano Manzur Claudio. **Los delitos informáticos**. Editorial Jurídica Cono Sur. Buenos Aires, Argentina, 2006.

International Organization of Computer Evidence –IOCE-. (2002), **Líneas Guía para la mejor practica del examen forense de la tecnología digital**.
http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html.

LARA RIVERA, Jorge. **Los Delitos Informáticos**, <http://www.jusrismática.com>.

LÓPEZ DELGADO, Miguel, **Análisis Forense Digital**, Junio del 2007, CRIPORED. Acurio del Pino, Santiago, **Introducción a la Informática Forense**, http://www.alfaredi.com/apcaaalfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf.

LLACER RUBIO, Enrique. **Informática y empresa**, Editorial Rural Provincial, Sevilla, España, 1983.

MALDONADO AGUIRRE, Alejandro. **El control constitucional**. Publicación de la Corte De Constitucionalidad. Guatemala, Guatemala, (s.f).



MAGLIONA MARKOVICHT, Claudio Paúl y López Medel Macarena. **Delincuencia y fraude informático**. Editorial Jurídica de Chile. 1999.

Ministerio Público de la República de Guatemala, **Manual del fiscal**. Segunda Edición, Guatemala, 2001.

MORENO GONZÁLEZ, Rafael. **Manual de introducción a la criminalística**. Editorial Porrúa, México, 1993.

OSSORIO, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**. Buenos Aires, Argentina, Editorial. Heliasta S.R.L., 1981.

Programa de las Naciones Unidas para el Desarrollo. **Un Mundo de experiencias en desarrollo**, <http://www.undp.org/spanish/about/>.

RAMÍREZ Bejerano y Aguilera Rodríguez. **Los delitos informáticos. Tratamiento internacional, en Contribuciones a las Ciencias Sociales**, www.eumed.net/rev/cccss/04/rbar2.htm.

Real Academia de la Lengua Española. **Diccionario de la lengua española**. Editorial Espasa Calpe, S.A., Madrid España, 1990.

REYES ECHANDÍA, Alfonso. **La tipicidad**. Universidad de Externado de Colombia, 1981.

SALT, G. Marcos. **Informática y Delitos**, <http://www.derecho.org.ar>.

SÁNCHEZ, Cecilia. **Proceso Penal y derecho fundamentales**. Edición 1 Escuela poder judicial de Costa Rica, 1997.

SANTODOMINGO, Adolfo. **Introducción a la informática**. Editorial Ariel S.A., España. 1997.

TELLEZ VALDÉS, Julio. **Los delitos informáticos. Situación en México**. México, 2006.

TELLEZ VALDÉS, Julio, **Derecho informático**. 3ª.ed., Ed. Mc Graw Hill, México, 2003.

TIEDEMANN, Klaus. **Poder económico y delito**. Editorial Ariel, Barcelona, España, 1985.



THORIN, Marc. **La ciencia informática: métodos, reglas, normas.** Ed. Masson, S.A., España. 1989.

Universidad de Cádiz, Servicio de Publicaciones. **Fundamentos informáticos,** España, 1996.

Legislación:

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

Código Penal. Decreto No. 17-73 del Congreso de la República de Guatemala, 1973.

Reformas al Decreto No. 17-93 del Congreso de la República de Guatemala, Decreto No. 33-96 del Congreso de la República de Guatemala, 1996.

Código Procesal Penal. Decreto No. 51-92 del Congreso de la República de Guatemala. 1994.

Ley del Organismo Judicial. Decreto No. 2-89 del Congreso de la República de Guatemala. 1990.

Ley Orgánica del Ministerio Público. Decreto No. 40-94 del Congreso de la República de Guatemala, 1994.

Ley Orgánica de Instituto Nacional de Ciencias Forenses de Guatemala. Decreto No. 32-2006 del Congreso de la República de Guatemala, 2006.