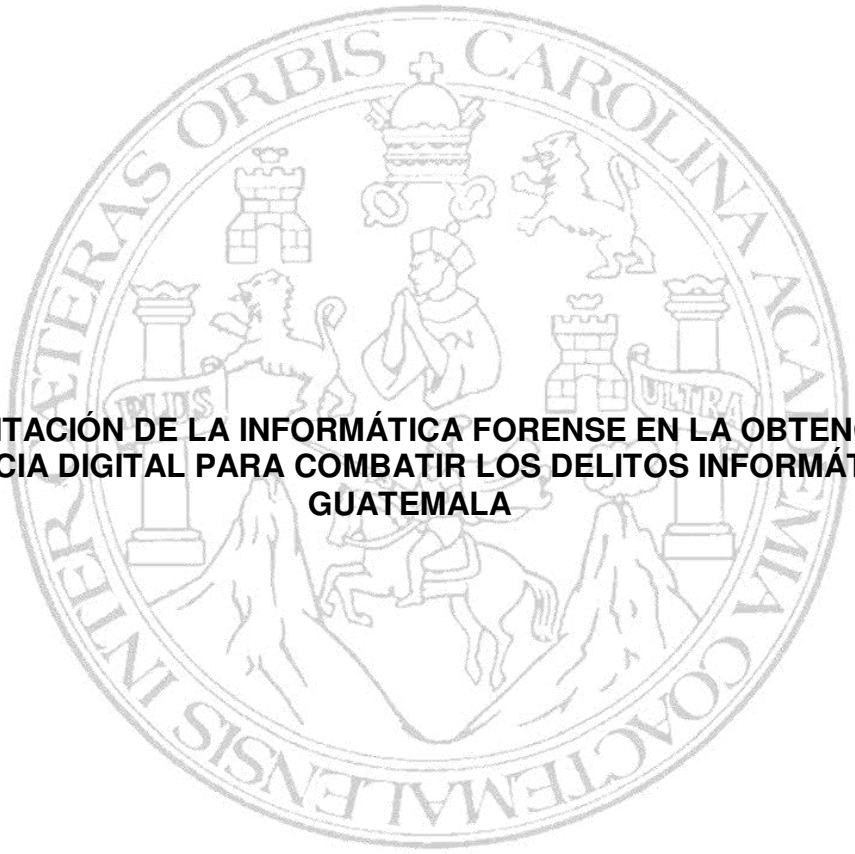
**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**
**FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**




# IMPLEMENTACIÓN DE LA INFORMÁTICA FORENSE EN LA OBTENCIÓN DE EVIDENCIA DIGITAL PARA COMBATIR LOS DELITOS INFORMÁTICOS GUATEMALA

**JOSÉ CARLOS ZAMORA ALVIZURES**

**GUATEMALA, ABRIL DE 2012**

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

# IMPLEMENTACIÓN DE LA INFORMÁTICA FORENSE EN LA OBTENCIÓN DE EVIDENCIA DIGITAL PARA COMBATIR LOS DELITOS INFORMÁTICOS 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:

**JOSÉ CARLOS ZAMORA ALVIZURES**

Previo a conferírsele el grado académico de

**LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES**

Y los títulos profesionales de

**ABOGADO Y NOTARIO**

Guatemala, abril 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: | Licda. Rosa María Ramírez Soto |
| Secretario: | Lic. Luis Efraín Guzmán Morales |
| Vocal: | Lic. Epifanio Monterroso Paniagua |

**Segunda Fase:**

| | |
|---|---|
| Presidente: | Lic. Marco Tulio Pacheco Galicia |
| Secretario: | Lic. Marvin Estuardo Aristides |
| Vocal: | Lic. Raúl Antonio Castillo Hernández |

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).

# BUFETE JURIDICO ESTRADA Y ASOCIADOS

Lic. OSCAR RENÉ ESTRADA CHEW

5ª calle 9-20 zona 1, oficina 03, ciudad de Guatemala.
Teléfono 22320727


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

Guatemala, 09 de junio de 2011

Licenciado

**Carlos Manuel Castro Monroy**

Jefe de la Unidad de Asesoría de Tesis

Facultad de Ciencias Jurídicas y Sociales

Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES
RECIBIDO
18 JUL. 2011
UNIDAD DE ASESORIA DE TÉSIS
Hora
Firma

Respetable Licenciado

De conformidad con el nombramiento de fecha 14 de junio de 2010, en el cual se me nombra como **ASESOR** y donde se me faculta para realizar las modificaciones de forma y de fondo, en el trabajo de investigación del bachiller José Carlos Zamora Alvizures, me dirijo a usted haciendo referencia a la misma con el objeto de informar mi labor y oportunamente emitir dictamen correspondiente, en relación a los extremos indicados en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Publico y habiendo revisado el trabajo recomendado se establece lo siguiente:

i. El trabajo de tesis se denomina **"IMPLEMENTACIÓN DE LA INFORMÁTICA FORENSE EN LA OBTENCIÓN DE EVIDENCIA DIGITAL PARA COMBATIR Y PREVENIR LOS DELITOS INFORMÁTICOS EN GUATEMALA"**.

ii. Al realizar la revisión sugerí correcciones que en su momento considere necesarias para mejorar la comprensión del tema desarrollado, como lo fue el de modificar el nombre del título a **"IMPLEMENTACIÓN DE LA INFORMÁTICA FORENSE EN LA OBTENCIÓN DE EVIDENCIA**

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

**DIGITAL PARA COMBATIR LOS DELITOS INFORMÁTICOS EN GUATEMALA"**, por adecuarse de mejor manera al planteamiento del problema y otras correcciones las cuales en su momento se corrigieron, constando la presente tesis en cinco capítulos realizados en orden lógico y siendo un tema jurídicamente importante siendo un aporte invaluable.

iii. En relación a los extremos indicados en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público se establece los siguiente: **a) Contenido científico y técnico de la tesis:** el sustentante abarcó tópicos de importancia en materia de delitos informáticos, delincuencia informática así como la utilización de la informática forense enfocando desde un punto de vista jurídico penal y procesal penal por ser un tema importante debido a la evolución acelerada de la nuevas tecnologías, contenido que es bastante novedoso ya que existe poca información existente y que el presente trabajo puede servir como instrumento para futuras iniciativas de ley en el Organismo Legislativo; **b) La metodología y técnicas de la investigación:** para el efecto tiene como base los métodos analítico, sistemático, inductivo y comparativo, a través de los cuales se estudió el fenómeno investigado y culminó con la comprobación de la hipótesis planteada, siendo una necesidad la aplicación de la informática forense para la persecución penal de los delitos informáticos por tener técnicas, métodos propios y especiales; **c) La redacción:** la estructura formal de la tesis compuesta por cinco capítulos se realizó en una secuencia ideal, empezando con temas que llevan al lector poco a poco al desarrollo del tema central para el buen entendimiento del mismo; **d) Contribución científica:** realiza un estudio sobre las funciones de la Informática Forense, como ciencia forense que se constituye en un instrumento que auxilia en la investigación de los delitos informáticos para el adecuado procesamiento de la escena del crimen y los conocimientos en materia informática que deben de tener los peritos que recolectan y analizan la denominada evidencia digital; el presente trabajo en su desarrollo constituye un aporte al derecho penal, al derecho procesal penal en materia de delitos informáticos, que ha cumplido con todo el procedimiento del método científico; **e)**

# BUFETE JURIDICO ESTRADA Y ASOCIADOS

Lic. OSCAR RENÉ ESTRADA CHEW

5ª calle 9-20 zona 1, oficina 03, ciudad de Guatemala.
Teléfono 22320727


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

**Conclusiones y recomendaciones:** tanto las conclusiones como las recomendaciones son congruentes con el planteamiento del problema, y que en síntesis tiene como fundamento la necesidad de la aplicación de la informática forense para la persecución de los delitos informáticos y la necesidad de la actualización de la legislación guatemalteca, conclusiones y recomendaciones que comparto con el autor puesto que las mismas se encuentran adecuadas a la realidad nacional e internacional en esta materia y están debidamente fundamentadas. Además se comprobó que la bibliografía fuera la correcta, que los métodos y técnicas fueran aplicados correctamente, en virtud de que con ellos se obtuvo la información necesaria y objetiva para la elaboración y la presentación

En conclusión y atendiendo a lo indicado el Artículo 32 del Normativo para Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General y Público, informo a usted que **APRUEBO** ampliamente la investigación realizada por lo que respecto al trabajo realizado por el sustentante bachiller José Carlos Zamora Alvizures, emito **DICTAMEN FAVORALE,** ya que considero el tema un importante aporte.

Atentamente.

Lic. Oscar René Estrada Chew
Abogado y Notario

Lic. Oscar René Estrada Chew
Col. 3,562

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

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

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

**UNIDAD ASESORÌA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**. Guatemala, diecinueve de julio de dos mil once.

Atentamente, pase al ( a la ) LICENCIADO ( A ): **RIGOBERTO RODAS VÁSQUEZ**, para que proceda a revisar el trabajo de tesis del ( de la ) estudiante: **JOSÉ CARLOS ZAMORA ALVIZURES**, Intitulado: **"IMPLEMENTACIÓN DE LA INFORMÁTICA FORENSE EN LA OBTENCIÓN DE EVIDENCIA DIGITAL PARA COMBATIR LOS DELITOS INFORMÁTICOS 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".

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

**LIC. CARLOS MANUEL CASTRO MONROY**
**JEFE DE LA UNIDAD ASESORÍA DE TESIS**

cc.Unidad de Tesis
CMCM/ brsp.

*Bufete Profesional*

*Lic. Rigoberto Rodas Vásquez*

*Abogado y Notario*

Guatemala, 22 de agosto de 2011

**LICENCIADO**
**CARLOS MANUEL CASTRO MONROY**
**JEFE DE LA UNIDAD DE ASESORÍA DE TESIS**
**FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**
**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
23 AGO. 2011
UNIDAD DE ASESORÍA DE TESIS

Licenciado Castro Monroy.

En cumplimiento con la resolución emitida por esa unidad de asesoría de tesis de fecha diecinueve de julio de dos mil once, donde se me nombró como revisor de tesis del bachiller **JOSÉ CARLOS ZAMORA ALVIZURES**, que se intitula "**IMPLEMENTACIÓN DE LA INFORMÁTICA FORENSE EN LA OBTENCIÓN DE EVIDENCIA DIGITAL PARA COMBATIR LOS DELITOS INFORMÁTICOS EN GUATEMALA**".

Dicho trabajo de tesis se encuentra a mi juicio, bien concebido y presenta un análisis científico y técnico orientado a establecer las funciones de la Informática Forense, como ciencia forense para obtener la evidencia digital y así combatir de una mejor forma los delitos informáticos en Guatemala. Procedo a emitir el dictamen correspondiente:

1. La revisión de la tesis se llevó a cabo a través de varias sesiones, habiéndose realizado las observaciones pertinentes para brindar un mejor desarrollo de la investigación, respetando el enfoque y criterio sustentado por el autor, habiéndose orientado el análisis de la investigación de mérito desde la perspectiva doctrinaria y legal vigente.

2. En relación a la distribución del contenido de la tesis, fue realizada en una secuencia adecuada, para una buena comprensión; así mismo se utilizó el

*7ma. Avenida 1-20 Zona 4 Edificio Torre Café Nivel 9, Oficina 910.*

*Teléfono: 2334-2043*

método científico y la técnica de investigación bibliográfica, con el fin de demostrar que se hizo la recolección de información de la manera ajustada a los requerimientos de este tipo de trabajo.

3. La redacción del trabajo revisado ha sido clara y práctica para la fácil comprensión del lector.

4. De la revisión realizada se establece que el trabajo es una contribución técnica y científica, por tratarse de un tema de mucho interés en la actualidad, debido a la constante evolución de la tecnología, ya que estudia y analiza las funciones con las que cumple la Informática Forense, como ciencia forense para obtener evidencia digital, cuando se ha cometido un delito informático, a través del procesamiento de la escena del crimen, que por lo particular del ilícito tiene sus propios métodos y técnicas. Además se determina que los peritos que intervienen tanto en la recolección, como en el análisis de las evidencias deben tener conocimientos amplios en la materia y de esta forma combatir de mejor forma la denominada criminalidad informática.

5. Estoy de acuerdo con las conclusiones a que se arribó en el trabajo de investigación, siendo acepciones propias del bachiller y que conllevan al verdadero objeto del tema; como también con las recomendaciones aportadas, ya que las mismas obedecen a una realidad jurídica, penal, procesal penal y en materia de delitos informáticos. Mención importante merece la conclusión a la cual arriba el sustentante, en cuanto a que en Guatemala existen una serie de obstáculos para la persecución penal de los delitos informáticos, los cuales se deben principalmente a la falta de capacitación del Ministerio Publico, de la Policía Nacional Civil y el Instituto Nacional de Ciencias Forenses, que no cuentan con el personal con la preparación necesaria. Esto deriva en la recomendación que realiza el sustentante en cuanto a la necesidad de capacitar

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

al personal de estas importantes instituciones en materia de informática forense, para la investigación efectiva y eficiente de los delitos informáticos.

6. El trabajo realizado, que se encuentra contenido en cinco capítulos, establece los aspectos elementales, objeto de la investigación, desarrollándose técnicamente con la bibliografía consultada, la cual es idónea y suficiente.

En definitiva, después de considerar los aspectos vertidos con anterioridad, el contenido del trabajo de tesis se ajusta a los requisitos que deben ser observados según la normativa respectiva, es por ello que al cumplirse con los requisitos establecidos en el Artículo 32 de la Normativa para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y Examen General Público, resulta procedente dar el presente, **DICTAMEN FAVORABLE**, aprobando el trabajo de tesis del bachiller **JOSÉ CARLOS ZAMORA ALVIZURES**. Para el efecto se ordene la impresión del mismo y se señale día y hora para la discusión en el correspondiente Examen Público.

Atentamente,

Lic. Rigoberto Rodas Vásquez
Abogado y Notario

***Lic. Rigoberto Rodas Vásquez***

***Colegiado: 4083***

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

*Edificio S-7, Ciudad Universitaria*
*Guatemala, Guatemala*

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, uno de marzo de dos mil doce.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de el estudiante JOSÉ CARLOS ZAMORA ALVIZURES titulado IMPLEMENTACIÓN DE LA INFORMÁTICA FORENSE EN LA OBTENCIÓN DE EVIDENCIA DIGITAL PARA COMBATIR LOS DELITOS INFORMÁTICOS EN GUATEMALA. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala.

LEGM/sllh.

## DEDICATORIA

A DIOS: Infinitas gracias al supremo Creador luz que ilumina mi camino y dueño de mi ser, por que en todo momento me ha guiado y protegido.

A MIS PADRES: Carlos Arnoldo Zamora Fabián (Q.E.P.D) y Blanca Marta Alvizures Mix, quienes han sido modelo de esfuerzo, trabajo, responsabilidad y honradez, quienes en todo momento me apoyaron y sin su esfuerzo no hubiera podido alcanzar esta meta.

A MI ESPOSA: Leyda Anira Palacios Bran, por su amor, comprensión, paciencia y apoyo, en todo momento, a quien dedico en especial el haber alcanzado esta meta y el día de hoy poder compartir a su lado este triunfo que no es mío es nuestro. Te amo.

A MIS HIJAS: Maryorie Sussel y Angie Mishel, por ser la bendición más grande que Dios me ha dado y la fuente de inspiración de mi vida, las amo.

A MI HERMANO: Mi amigo de toda la vida, por todo el apoyo y consejos durante toda la vida que hemos compartido y hacer más fáciles los momentos duros que hemos vivido

A MI GRAN FAMILIA: A mi abuelita, a mis tíos, de manera especial a mis tías que ya están a tu lado Dios, primos, primas, a mis suegros, cuñados, cuñadas, a mi sobrinos, a mis ahijados Gracias por el apoyo brindado, que Dios los bendiga

AL: Centro de Estudios de Derecho (CEDE), en especial a la Licenciada Ingrid Rivera y al Licenciado Omar Ricardo Barrios Osorio, por todo el apoyo, los consejos, la enseñanza y la preparación no solo para los privados sino para la vida profesional y personal.

A MIS AMIGOS: De la infancia, del Banco GyT Continental, de la Dirección de Investigaciones Criminalísticas, del Ministerio Público y de manera muy especial a mis amigos de la universidad por todo el apoyo incondicional, la confianza, la fuerza, los momentos que compartimos juntos. Gracias, que Dios los bendiga.

A: A la tricentenaria Universidad de San Carlos de Guatemala, en especial a la Facultad de Ciencias Jurídicas y Sociales, por la formación académica y profesional.

**ÍNDICE**

**Pág.**

**Pág.**

# INTRODUCCIÓN

La evolución de las denominadas tecnologías de la información y comunicaciones, T.I.C, ha llevado a la humanidad a un desarrollo acelerado en cuanto a las comunicaciones, los sistemas de información, la forma en que la información se transmite; y debido a que la información se ha convertido en un bien jurídico de gran valor, se ha hecho necesario protegerlo legalmente.

Los beneficios que ha traído la revolución digital son de gran magnitud para la humanidad, pero como proceso de evolución también trae consecuencias negativas, como lo es que el ciberespacio, la Internet, las redes sociales, todo lo que se refiere a las tecnologías de la información y comunicaciones han sido concebidos como ámbitos propicios para la realización de conductas antijurídicas, denominados delitos informáticos.

El presente trabajo se justifica en la necesidad de dar a conocer a la sociedad guatemalteca el fenómeno de los delitos informáticos, sus consecuencias y su realidad a nivel nacional, científicamente pretende plantear la necesidad de tener las herramientas científicas para poder perseguir legalmente y aportar las evidencias necesarias que sirvan como medio de prueba dentro de un proceso penal para combatir los delitos informáticos a través de la informática forense; formulando la hipótesis que la informática forense permitirá la obtención de evidencia digital para combatir los delitos informáticos en Guatemala; teniendo como objetivo general establecer el procedimiento jurídico para la implementación de la informática forense y

como objetivos inmediatos y mediatos, delimitar su implementación, los procedimientos que utiliza la informática forense. El método utilizado para el desarrollo del presente trabajo es el método científico valiéndose de los enfoques inductivo y deductivo, y de la técnica descriptiva apoyándose en la investigación documental.

El informe final de tesis contiene cinco capítulos, en el primer capítulo, se presenta la delimitación del fenómeno de la delincuencia informática así como la forma en que esta nueva forma de delinquir ha afectado a la sociedad en Guatemala; el segundo capítulo, desarrolla el tema de delitos informáticos, los sujetos que participan en los delitos informáticos, los bienes jurídicos tutelados y la clasificación de los diferentes tipos de delitos informáticos; en el tercer capítulo, se aborda el tema de la situación internacional sobre al estudio y la regulación legal en cuanto a la delincuencia organizada que se dedica a los delitos informáticos; en el cuarto capítulo, lo referente a la seguridad informática y las políticas de seguridad, abarcando la realidad procesal de los delitos informáticos; y en el quinto capítulo, que constituye la parte fundamental del presente trabajo, se desarrolla lo referente a la informática forense como ciencia forense cuyo objetivo principal es obtener todos los elementos de convicción para la persecución penal de los delitos informáticos.

En la medida que la informática forense sea aplicada, el combate a los delitos informáticos y a la criminalidad informática en general, podrá erradicarse y creará una sociedad digital más segura y confiable.

# CAPÍTULO I

## 1. Delimitación del fenómeno de la delincuencia informática

El aspecto principal de la informática, radica en que "la información se ha convertido en un valor económico de primera magnitud. Desde la antigüedad el hombre ha tratado de encontrar medios para guardar información relevante, para poderla usar posteriormente, desde la era pre-Gutenberg, que se caracterizaba por la transmisión de las informaciones de forma manual o personal, por medio de los individuos que generaban la misma, pasando por la era de la impresión, la era eléctrica-analógica, hasta la era digital que brinda la posibilidad de transmitir la información, a bajo costo, con facilidad y en forma rápida, la cual se encuentra almacenada electrónicamente, de forma bidireccional e interactiva desde cualquier parte del mundo a cualquier destino, recurriendo a una variedad de tecnologías; se puede observar la evolución de la información y el valor que ésta tiene"[1]

Como señala Camacho Losa, "En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia"[2]. Entonces me surge la interrogante ¿y por qué la informática habría de ser diferente?

[1] Magliona Markovicth Claudio Paúl, López Medel Macarena, **Delincuencia y Fraude Informático**, pág.43

[2] Camacho Losa Luis, **El Delito informático**, pág. 12

Al parecer todos los estudiosos de la materia están de acuerdo, en pensar que el surgimiento de este tipo de crímenes está íntimamente ligado al desarrollo de la tecnología informática. Las computadoras se han utilizado para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato. Para los autores chilenos Marcelo Huerta y Claudio Líbano "este fenómeno ha obligado al surgimiento de medidas legislativo penales en los estados industriales donde hay conciencia de que en los últimos años, ha estado presente el fenómeno delictivo informático"[3].

En Guatemala, el movimiento de la criminalidad informática o de los llamados delitos informáticos, no han alcanzado todavía una importancia mayor, no porque no se hayan cometido estos delitos, sino porque no se conoce en el entorno mucho sobre esta clase de delitos a pesar del efecto de globalización se está viviendo, y la razón de que esta nueva forma de lesión a bienes jurídicos tutelados no sea tomada en cuenta, es porque se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual.

La razón principal es que la informática ha invadido todas las áreas de la sociedad y por ende los avances tecnológicos son de tal magnitud que vienen a influir en todas las ramas del derecho no sólo es en el derecho penal, por ejemplo en el derecho mercantil debido a la proliferación de contratos mercantiles con la aparición del comercio electrónico, en el derecho tributario con la incorporación de paraísos fiscales que se podrían considerar virtuales, tal es el ejemplo de los casinos virtuales; también se

[3] Huerta Marcelo y Líbano Claudio**, Delitos informáticos**, pág. 4.

encuentra en el derecho civil con los continuos ataques a la propiedad intelectual. En los últimos casos sobre la piratería musical ponen de relieve la ineficacia de normas que caducan porque las mismas deben ser modificadas o sustituidas por otras más acordes al mundo en el que ahora se vive; el derecho financiero, con la aparición del ciberdinero rápidamente ahogado por los sistemas financieros tradicionales, pero que al final triunfará dado que es uno de los pocos sistemas que puede garantizar el comercio electrónico anónimo como lo es en realidad la mayor parte del que se realiza en la vida real; el derecho constitucional con los continuos ataques a uno de los derechos fundamentales, la intimidad de las personas, en las múltiples transmisiones transnacionales; el derecho internacional, atacado en su conjunto dadas las colisiones de derechos nacionales que se producen y las consecuencias que para el principio de territorialidad ello trae consigo; el derecho procesal, ya que gran parte de las pruebas que aparecen, por ejemplo, por internet son distintas a las conocidas hasta ahora por lo que se debe de acoger estas tecnologías al derecho procesal, y así podría numerar en las demás ramas del derecho, pero lo que interesa para el presente estudio es lo que ha afectado al derecho penal en cuanto a la aparición de nuevas formas de delincuencia a través de la red o bien de las tecnologías de la información y comunicaciones, -TIC-, como lo sería el terrorismo practicado en la red, crimen organizado, pornografía infantil en internet, etc., con el problema que trae consigo legislar sobre esta materias en países con culturas e ideas religiosas distintas.

A continuación he desarrollado una delimitación del fenómeno de la criminalidad informática

## 1.1. Delimitación del fenómeno

El primer problema encontrado es la delimitación de un área al que se denomine criminalidad informática.

Existe una confusión de términos y conceptos el cual está presente en todos los campos de la informática, especialmente en lo que tiene relación con sus aspectos criminales, es por eso que es necesario aclarar el confuso debate doctrinario en relación del contenido real de los delitos informáticos. Desde este punto de vista, se debe imperar la claridad absoluta con respecto a las materias, acciones y omisiones sobre las que deben recaer las sanciones que establezca el estado. Una de las características de los delitos informáticos, radica en que la acción u omisión ilícita se puede cometer en una región de un país y tenga los efectos en otra región de ese país e incluso y más importante aún en otro país, esto debido a las conexiones que se pueden realizar atreves de una red y principalmente de la internet, que tiene alcances espaciales ilimitados. Esto hace que los delitos se tengan que ver desde una perspectiva internacional.

El profesor español Romeo Casabona señala que “En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo no se puede hablar de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadoras, pero ni el bien jurídico protegido agredido es siempre de

la misma naturaleza ni la forma de comisión del hecho delictivo o merecedor de serlo, presenta siempre características semejantes, la computadora es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el hardware, el software, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información".[4]

De esta forma el profesor español Davara Rodríguez, concuerda con el autor mexicano Julio Téllez Valdés, quienes mencionan que no es adecuado hablar de delito informático ya que, como tal, no existe si necesitamos tipificar en la legislación penal para que pueda existir un delito. De ahí que "el nuevo Código Penal español de 1995 introduce el delito informático, pero no admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático"[5], de la misma manera la legislación nacional no brinda una definición de delito informático, ya que al aprobar el Decreto 33-96 del Congreso de la República de Guatemala, el legislador sólo adiciona estas figuras al Código Penal.

De lo anteriormente descrito se puede establecer que en algunas legislaciones extranjeras sea más adecuado hablar de crímenes informáticos por su trascendencia social, que de delitos informáticos, sin embargo la legislación nacional sólo tipifica delitos informáticos en general. Es por eso que demasiado complicado buscar un

[4] Romeo Casabona, Carlos María, **Poder informático y seguridad jurídica**, pag.12.
[5] Davara Rodríguez, Miguel Ángel**, Análisis de la ley de fraude informático**, pág. 23.

concepto técnico o legal que comprenda todas las gestiones inadecuadas que se vinculan a los medios o procedimientos informáticos, tanto por la diversidad de supuestos, como de los bienes jurídicos afectados.

Ahora bien, es necesario expresar que además dentro de esto existen diversidad de significados y conceptos sobre delincuencia informática, criminalidad informática, lo que viene a constituir un tema de debate doctrinario y jurídico.

### 1.1.1. Delincuencia informática y abuso informático

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

La Organización de Cooperación y Desarrollo Económico (O.C.D.E) en la Recomendación número R(81) 12 del Consejo de Europa en el Convenio sobre cibercriminalidad, define el abuso informático como " todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos".

Además Romeo Casabona aporta la misma definición incurriendo en la Recomendación R(89) 9, del Comité de Ministros del Consejo de Europa en el Convenio sobre Cibercriminalidad, considera "que la delincuencia informática es de

carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el computador"[6].

### 1.1.2. Criminalidad informática

Baón Ramírez define a la criminalidad informática como "la realización de una forma de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"[7].

El autor Tiedemann "considera que con la expresión criminalidad mediante computadoras, se hace mención que todos los actos, antijurídicos según la ley penal que se encuentre vigente sea realizados con el empleo de un equipo automático de procesamiento de datos. También señala, que este problema comprende la amenaza a la privacidad del ciudadano, y además se refiere a los daños patrimoniales producidos por el abuso de datos procesados automáticamente"[8].

Las dificultades que surgen al tratar de enfrentar este tipo de delincuencia a todo nivel es la tarea del Ministerio Público por mandato constitucional y por disposición legal. Ahora bien el fenómeno descrito en los últimos tiempos ha tenido un avance

[6] Romeo Casabona, Carlos María. **Ob. Cit**.pág.26
[7] http://www.alfa-redi.org/**rdi-articulo.shtml**?x=207 (visitada el 23 de junio de 2,011)
[8] Tiedemann, Klaus**, Poder informático y delito**, pág.16.

significativo tomando en cuenta la manifestación de la globalización, la cual no solo ha tenido beneficios, sino también ha contribuido a la masificación de esta clase de delitos y tecnificado a otra clase de cómo son los llamados delitos informáticos.

Como define Carlos Resa, "el crimen organizado no existe como tipo ideal, sino como un grado de actividad criminal o como un punto del 'espectro de legitimidad"[9]. En este contexto es el crimen organizado que a través de los años se ha ido transnacionalizando su actividad y por ello se habla de delincuencia transnacional. Dentro de esta definición de crimen organizado, la gama de actividades que puede ejecutar un determinado grupo de crimen organizado puede ser extensa, variando en cada caso según diversas variables internas y externas a la organización, y combinar uno o más mercados, expandiéndose asimismo por un número más o menos limitado de países, aunque en tiempos recientes existe una fuerte tendencia a la concentración empresarial en cada vez menos grupos de un mayor número de campos de la ilegalidad. Su repertorio de actividades incluye el delito de cuello blanco y el económico (en donde se encontrarían los delitos informáticos), pero supera a éste último en organización y control, aunque los nexos de unión entre ambos modelos de delincuencia tienden a fusionarse y el terrorismo y el ciberterrorismo pueden llegar a formar parte de sus acciones violentas en ciertas etapas o momentos.

En un inventario amplio, las actividades principales de las organizaciones criminales, en suma, abarcan la provisión de bienes y servicios ilegales, ya sea la producción y el tráfico de drogas, armas, niños, órganos, inmigrantes ilegales, materiales nucleares, el

[9] Resa Nestares Carlos, **Crimen organizado transnacional: definición, causas y consecuencias**, pág.47.

juego, la usura, la falsificación, el asesinato a sueldo o la prostitución; la comercialización de bienes lícitos obtenidos por medio del hurto, el robo o el fraude, en especial vehículos de lujo, animales u obras de arte, el robo de identidad, clonación de tarjetas de crédito; la ayuda a las empresas legítimas en materias ilegales, como la vulneración de las normativas medioambientales o laborales; o la utilización de redes legales para actividades ilícitas, como la gestión de empresas de transporte para el tráfico de drogas o las inversiones inmobiliarias para el blanqueo de dinero.

Entre aquellas organizaciones que pueden considerarse como típicamente propias del crimen organizado, practicando algunas de estas actividades, se encuentran, dentro de un listado más o menos extenso, las organizaciones dedicadas casi exclusivamente al tráfico de drogas a gran escala, ya sean propias de los países europeas o se generen en países latinoamericanos, del sudeste y el sudoeste asiático ahora existe otro grupo que ha entrado a la escena del crimen organizado transnacional son los llamados **crakers**, los verdaderos piratas informáticos, que a través del cometimiento de infracciones informáticas, han causado la perdida de varios millones de dólares, a empresas, personas y también a algunos estados.

La criminalidad o delincuencia informática es un problema global y necesita con urgencia la armonización legislativa y la cooperación internacional. El crimen organizado recurre a una vulnerabilidad de control de acceso a sistemas de cómputo y a una tecnología moderna de comunicación en la internet para cometer fraudes y extorsiones. Pero se debe de empezar a combatir este problema de forma interna, entender que este tipo de criminalidad ya es una realidad en Guatemala, existen

grupos organizados que se dedican a utilizar a las computadoras, la internet, las redes sociales y en general todo la tecnología moderna para cometer delitos o bien a causar daño al software y al hardware de los equipos de cómputo de las personas; y que la realidad es que la legislación y normatividad nacional no es adecuada para combatir a estos criminales.

## CAPÍTULO II

### 2. Delitos informáticos

En primer lugar debo partir de la idea general de establecer la definición de delito para poder desarrollar de mejor forma la definición de delito informático, en principio se puede definir al delito como toda acción u omisión típica, antijurídica y culpable, sin embargo existe extensa doctrina nacional y extranjera que establece la definición de delito como tal, la mayoría de ellas define al delito cuando cumplen los elementos que lo constituyen, de ahí que se pueda establecer que delito "es la conducta humana consciente y voluntaria que produce un efecto en el mundo exterior (acción), que se encuentra prohibida por la ley (tipicidad), la cual es contra derecho (antijuridicidad) y que la persona ha incumplido a pesar que conoce y valora la norma (culpabilidad)"[10], algunos doctrinarios establecen que la persona debe estar en capacidad de comprender lo ilícito de su acción (imputabilidad).

Partiendo de la idea anterior se podría definir el delito informático como "toda acción u omisión culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la

[10] Barrios Osorio, Omar Ricardo**, Derecho e informática, aspectos fundamentales**, pág.367.

víctima,.tipificado por la ley, que se realiza en el entorno informático y sancionado con una pena"[11].

El autor mexicano Julio Téllez Valdez señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"[12].

El autor Davara Rodríguez lo define como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"[13]

En forma básica el autor Omar Ricardo Barrios Osorio define al delito informático, como "las acciones prohibidas por la ley, que se comete en contra de uno o varios de los elementos que integran un sistema de información o los derechos que del mismo se deriven (protección de datos, intimidad o privacidad, derechos de autor)"[14].

[11]http:// www.monografias.com/trabajos12/**conygen**/conygen.shtml (visitada el 23 de junio de 2,011)
[12] Manson, Marcelo**. Legislación sobre delitos informáticos**, http://monografias.com/trabajos/legisdelinf/legisdelinf.shtml. (visitada 25 de junio de 2,010).
[13] Palazzi, Pablo A: **Delitos informáticos**, pág.49.
[14] Barrios Osorio, Omar Ricardo. **Ob. Cit.,** pág.368

## 2.1. 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 un sujeto pasivo. Por el tema que concierne a los delitos informáticos se parte de la idea que sólo las personas (físicas o individuales), pueden cometer delitos, en virtud que sólo las personas tienen razonamiento y capacidad para dirigir sus acciones. De esta suerte, el bien jurídico protegido 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 diferir del sujeto perjudicado, el cual puede, eventualmente ser un tercero.

### 2.1.1. Sujeto activo

Este está constituido por la persona física o personas físicas, que con su proceder establecen un resultado lesivo para los demás, lesionando o poniendo en peligro el bien jurídicamente tutelado En el Código Penal guatemalteco, el sujeto activo por su participación en el delito se clasifica en autores y cómplices. Ahora bien si se refiere a los delitos informáticos, las personas que los cometen, las cuales tienen ciertas características que no tienen el perfil común de los delincuentes, tienen un alto grado de conocimientos, recursos, habilidades especiales para el manejo de la informática y las tecnologías de la información y comunicaciones –T.I.C-, generalmente por la actividad laboral que realizan se encuentran en lugares especiales desde donde se maneja la información de carácter sensible, o bien son diestros en el manejo de los

sistemas informáticos, aun cuando, en muchas ocasiones, sus actividades no faciliten la realización de este tipo de delitos.

Se ha comprobado que entre los responsables de estos tipos de delitos hay una gran diversidad y la diferencia entre ellos, es la naturaleza de los delitos cometidos, de tal manera que, el individuo que ingresa en un sistema informático sin intenciones de cometer algún delito es muy diferente de la persona que labora para una institución financiera que desvía los fondos de las cuentas de los clientes o del propio banco.

En el ambiente de las tecnologías de la información y comunicaciones a los sujetos responsables de los delitos informáticos se les describe de varias formas, siendo las más comunes: hacker, cracker y pirata informático

### 2.1.2. Sujeto Pasivo

El sujeto pasivo es quien sufre las consecuencias de la comisión de un delito siendo la sociedad y la víctima o agraviado en primer término, pero además es necesario tomar en cuenta que en principio el sujeto pasivo del delito, es la persona física o jurídica que resiente la actividad delictiva, es el titular del bien jurídicamente tutelado que es dañado o puesto en peligro por la conducta del responsable y en los casos de los delitos informáticos pueden ser personas individuales o bien personas jurídicas como sociedades mercantiles, instituciones crediticias, bancos, financieras, aseguradoras, etc., que manejan un considerable volumen de información y datos, estos últimos representativos de valores o moneda administrada en forma electrónica, así mismo las

personas que se dedican a prestar específicamente servicios relacionados con las tecnologías de la información y comunicaciones como proveedores de la internet y sus aplicaciones, a los gobiernos a través de la administración tributaria también es un sujeto pasivo, en virtud que se alteran los programas de ordenador de los sistemas de control tributario de los contribuyentes, para cometer delitos relacionados con el incumplimiento del pago de impuestos (manipulación de la información); todos estos utilizan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo es sumamente importante para el estudio de los delitos informáticos, por medio de él, es posible conocer los diferentes ilícitos que se cometen a los activos informáticos, con objeto de prever las acciones ilícitas antes mencionadas debido a que muchos de los delitos son descubiertos por casualidad, desconociendo el modus operandi de los agentes delictivos, es decir la mayor parte de las veces no se tienen indicios de cómo lo realizan.

Debido a lo anterior, en Guatemala ha sido casi imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de ellos no son descubiertos o no son denunciados a las autoridades competentes y si a esto se suma la falta de una adecuada legislación que proteja a las víctimas de estos delitos, la falta de preparación técnica y jurídica por parte de fiscales, investigadores y peritos para poder brindar más y mejores elementos de convicción a los encargados de la administración de justicia, para comprender y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas 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.

Es posible afirmar que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, alertando a las posibles víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de los titulares de medios informáticos, así como una eficiente preparación al personal encargado de la investigación, y a los encargados de la administración e impartición de justicia para atender estas conductas ilícitas, se avanzaría mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más tanto a nivel nacional como internacional.

Cabe destacar que los organismos internacionales han adoptado resoluciones similares 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 para detectar, investigar, prevenir y sancionar los delitos informáticos.

### 2.2. Bien jurídico tutelado

Este es denominado de diferentes maneras, como: derecho protegido, bien garantizado, interés jurídicamente tutelado, objeto jurídico, núcleo del tipo, objeto de protección. No puede surgir el delito cuando por inexistencia del objeto de tutela o por

falta de idoneidad de la acción es imposible la lesión de un bien jurídico, "el cual se presenta en las formas más diversas debido a su pretensión de garantizar los derechos de toda persona, como pueden ser entre otros: reales, jurídicos, psicológicos, físicos, etcétera"[15].

Para Jescheck "el bien jurídico constituye el punto de partida y la idea que preside la formación del tipo. Afirma además que son bienes jurídicos aquellos intereses de la vida, de la comunidad a los que presta protección el derecho penal"[16]. En mi opinión, el bien jurídico como objeto de protección del derecho penal, es todo valor individual o de conjunto que merece la garantía de no ser vulnerado por la acción de otro.

El Estado de derecho bien entendido es la forma en que el Estado brinda protección a la sociedad, con fin del sometimiento riguroso de la ley, con lo cual, aquellos intereses sociales que ameriten ser protegidos por él se denominan **bienes jurídicos.**

El objeto del bien jurídico encuentra su origen en el interés de la vida, previo al derecho, que surge de las reacciones sociales, aunque dicho interés vital no se convierte en bien jurídico hasta que es protegido por el derecho, es este el que decide entre los intereses sociales cuáles deben convertirse en bienes jurídicos a través del proceso legislativo que lo crea.

[15] Heinrich, Jescheck Hans**. Tratado de derecho penal**, parte general. Volumen I, pág. 43
[16] **Ibíd**.

## 2.3. Bienes jurídicos tutelados en los delitos informáticos

Con relación a los delitos informáticos, se puede expresar que tiende a la protección de los bienes jurídicos, que se protegen desde el punto de vista de los delitos tradicionales, reinterpretando teológicamente los tipos penales ya existentes, para así aliviar los vacíos legales originados por los nuevos 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 por parte del ente investigador y sanción por parte del órgano jurisdiccional competente.

Y basado en lo anterior se puede decir que los bienes jurídicos tutelados en general son los siguientes:

- El patrimonio, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.
- 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.
- La seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.
- 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 de daños y el llamado terrorismo informático.

Los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "que se caracterizan porque simultáneamente afectan a varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo".[17] En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos.

Por tanto se puede decir que esta clase de delincuencia no sólo 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, en tal sentido la autora María Luz Gutiérrez Francés, respecto de la figura del fraude informático expone 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 (ya sea micro o macro social), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macro social vinculado al funcionamiento de los sistemas informáticos"[18].

Se establece entonces que "el nacimiento de esta nueva tecnología, 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

[17] Reyes Echandia, Alfonso**, La tipicidad**, pág. 28.
[18] Gutiérrez Francés, María Luz, **Fraude informático y estafa**, pág. 16.

personal registrada o sobre la información nominativa"[19]. En tal razón considero que este tipo de conductas delictivas son de carácter netamente pluriofensivo, por el hecho de que el atentar contra un solo bien jurídicamente tutelado existente de un solo sujeto pasivo, pueda llegar a tener consecuencias a nivel sociedad en bienes jurídicamente tutelados que han nacido con el surgimiento de estas nuevas tecnologías, y que en un principio no se había podido pensar que tuvieran tanto alcance.

Un ejemplo que puede aclarar esta situación, es el de un hacker que ingresa a un sistema informático con el fin de vulnerar la seguridad del sistema y averiguar la información que pueda sobre una determinada persona, esto en primer lugar se podría 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 se encuentra otro un 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 sólo importan la afección de bienes jurídicos clásicos.

## 2.4. Clasificación de los delitos informáticos regulados en el Convenio sobre la ciberdelincuencia (Convenio de Budapest)

Existen diversas clasificaciones de los delitos informáticos, desde el punto de vista doctrinario, y también legal, sin embargo, para efectos de esta tesis, haré mención a la

[19] Magliona Markovictc Claudio Paúl, López, Medel Macarena **Ob. Cit**, pág. 32

clasificación que nos presenta el Convenio sobre Ciberdelincuencia, por estar más actualizado a la realidad y contexto mundial en materia informática y expone una serie de conductas nuevas, esto debido a la continua evolución de la tecnología, este convenio es conocido como el Convenio de Budapest firmado el 21 de Noviembre de 2001 en el marco del Consejo de Europa, este instrumento jurídico internacional, es uno de los más importantes que se ha firmado hasta el día de hoy, del cual hasta ahora 22 países europeos han ratificado el Convenio y otros 22 países lo han firmado, desafortunadamente Guatemala no forma parte de este convenio.

Actualmente, el Convenio sobre la Ciberdelincuencia del Consejo de Europa es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional). Adoptado por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

Este convenio surgió a partir de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional, y en la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada rápida y operativa.

El convenio hace la siguiente clasificación:

**A. "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos.**

- **Acceso ilícito**: El acceso deliberado e ilegitimo a la totalidad o a una parte de un sistema informático, ya sea infringiendo medidas de seguridad, con la intención de obtener datos informáticos
- **Interceptación ilícita*:*** Interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos.
- **Interferencia en los Datos**: Comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
- **Interferencia en el sistema*:*** Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.
- **Abuso de los dispositivos*:*** Comisión deliberada e ilegítima de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta"[20].

Se puede notar que en cuanto a estos delitos lo que pretende proteger o el bien jurídico tutelado es a lo que se denomina sistema informático que se define como "una

[20]http:/www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/**Convenio_Ciberdelincuencia**.pdf , (visitada el 10 de abril de 2,011)

colección de personas, procedimientos, una base de datos y (a veces) hardware y software que colecciona, procesa, almacena, y proporciona datos procesos de transacciones a nivel operacional, e información para apoyar la gestión de toma de decisiones o constituirse en parte del producto o servicio"[21], las acciones ilícitas que se cometen contra el sistema informático van a afectar la disponibilidad, la integridad y sobre todo las confiabilidad de los datos contenidos en uno o varios sistemas informáticos.

**B. "Delitos informáticos**

- **Falsificación informática*:*** Cometer de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.
- **Fraude Informático*:*** Actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos, cualquier interferencia en el funcionamiento de un sistema informático"[22].

La comisión de estos delitos va a afectar a un bien que en los últimos tiempos ha adquirido una gran importancia como lo es la información la cual el autor Omar Ricardo

[21] Calderón Rodríguez, Cristian, **El impacto de la era digital en el derecho**. http://www.vlex.com/redi/ (visitada 7 de julio de 2,011)
[22]https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/**Convenio_Ciberdelincuencia**.pdf (visitada el 10 de abril de 2,011)

Barrios Osorio la define como " el conjunto de datos alfanuméricos, numéricos o lógicos que representan la expresión de un conocimiento, que pueden utilizarse para la toma de decisiones"[23], la importancia radica en la protección que se hace a la misma, ya que, su manipulación, alteración o supresión a la misma, puede causar perjuicios tanto legales como patrimoniales tanto a personas individuales como colectivas.

**C. "Delitos relacionados con el contenido**

- **Delitos relacionados con la pornografía infantil*:*** Comisión deliberada e ilegítima de producción de pornografía infantil con vistas a su difusión por medio de un sistema informático, la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático, la difusión o transmisión de pornografía infantil por medio de un sistema informático, la adquisición de pornografía infantil por medio de un sistema informática para uno mismo o para otra persona, la posesión de pornografía infantil por medio de un sistema informático o en un medio de almacenamiento de datos informáticos. Se entiende como pornografía infantil, todo material pornográfico que contenga representación visual de un menor comportándose de una forma sexualmente explicita, una persona que parezca un menor comportándose de una forma sexualmente explicita, imágenes realistas que representen a un menor comportándose de una forma sexualmente explicita"[24].

[23] Barrios Osorio, Omar Ricardo. **Obi. Cit.,** pág. 8
[24]https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/**Convenio_Ciberdelincuencia**.pdf (visitada el 10 de abril de 2,011)

Cabe mencionar que a nivel internacional, la pornografía infantil es un aspecto que ha tomado gran relevancia, el hecho que las nuevas tecnologías sean utilizadas para realizar este tipo de conductas han merecido que sean tipificadas y sean perseguibles penalmente, lastimosamente a nivel nacional no se le ha tomado la importancia debida y no se tengan los mecanismos necesarios tanto para su prevención como para su investigación y persecución, con la finalidad de proteger a los menores de edad contra estos ilícitos

### D. "Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Se refiere a acciones ilícitas en contra de la propiedad intelectual, de conformidad con las obligaciones asumidas por el Convenio de Berna para la protección de las obras literarias y artísticas, que hasta la fecha ampara a nivel internacional el derecho de los autores, con el fin de que tengan el privilegio de controlar el uso sobre sus obras literarias, artísticas o científicas, así como recibir una retribución por su utilización; así como las asumidas por el Tratado de la Organización Mundial de Propiedad Intelectual (O.M.P.I) sobre propiedad intelectual, Convenio de Roma"[25]

[25] http://www.uncjin.org/Documents/**congr10**/10s.pdf, (visitada el 15 de junio de 2,011)

## 2.5. Clasificación de los delitos Informáticos regulados en el Código Penal guatemalteco

Con la aprobación del Decreto número 33-96 del Congreso de la República de Guatemala, que entró en vigencia el tres de julio de 1,996, se adicionaron al Código Penal lo relativo a los delitos informáticos. El cuarto considerando del Decreto 33-96 del Congreso de la República de Guatemala establece: "Que los avances de la tecnología obligan al Estado a legislar en bien de la protección de derecho de autor en materia informática, tipos que nuestra legislación no ha desarrollado"

Los delitos informáticos se encuentran regulados dentro del Título IV de los delitos contra el patrimonio, con el objeto de proteger las creaciones de la propiedad intelectual, así como derechos humanos intrínsecos de las personas como lo es la intimidad personal

Para clasificar los delitos informáticos regulados en el Código Penal, se analizaran desde el punto de vista del bien jurídico tutelado en la norma tipo, para poder tener una visión más amplia de los mismos y lo que el legislador protegió en la ley:

- **Delito de alteración de programas**

El Decreto 33-96 del Congreso de la República de Guatemala, en el Artículo 14 adiciona el Artículo 274"B" que establece: "Alteración de programas. La misma pena

del artículo anterior se aplicara al que altere, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras".

El bien jurídico tutelado en el Artículo 274 "B", es uno de los elementos de los sistemas de información como lo es: las instrucciones o los programas de ordenador, pero esta protección es en cuanto a su funcionamiento, al respecto el legislador establece en cuanto a la inutilización de las instrucciones, se refiere a que con dolo no se permita utilizar una o varias de las aplicaciones o funciones del programa de ordenador y en cuanto a la inutilización de los programas que utilizan las computadoras se refiere a que los mismos no pueden ejecutarse o que se encuentran bloqueados.

Un ejemplo práctico, es la denominada bomba de tiempo, que es un programa que se adhiere de forma oculta a los programas de ordenador de los sistemas de información, para que en determinado tiempo o situación generen un bloqueo al funcionamiento del sistema o impidan el acceso a usuarios autorizados. En la mayoría de los casos son los administradores del sistema los que incurren en este ilícito, como laguna forma represiva contra la empresa; también se dan casos externos, pero llevan de por medio la comisión de otros ilícitos como estafa y extorsión.

- **Delito de reproducción de instrucciones o programas de computación**

El Decreto 33-96 del Congreso de la República de Guatemala en el Artículo 15 adiciona el Artículo 274"C", el cual estable: "Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa de quinientos a

dos mil quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación".

En este caso el bien jurídico tutelado o bienes jurídicos tutelados son los derechos de autor y derechos conexos del creador del programa de ordenador o la persona a quien cedió sus derechos.

En materia de programas de ordenador la persona individual o jurídica titular de los derechos de autor (morales, pecuniarios o patrimoniales, conexos) o sus herederos, tienen el derecho exclusivo a su reproducción, distribución, importación y exportación de copias, accesos, traducción, entre otros derechos. Lo anterior queda establecido en la ley especial, la Ley de Derechos de Autor y Derechos Conexos Decreto 33-98 del Congreso de la República de Guatemala y determinado en los contratos que celebre con quien cede algunos de los derechos de que goza en su calidad de autor.

En el lenguaje de la informática, en el lenguaje comercial, en la publicidad de las empresas afectadas y en las campañas de prevención, se les denomina a este delito **piratería**, pero se debe de aclarar que en la legislación penal guatemalteca el delito de piratería se encuentra regulado como un delito contra la seguridad colectiva, en el Libro II, Título VII, Capítulo III.

Se ha podido establecer en base a la información y estadísticas que proporcionan los medios de comunicación y los entes interesados, que el delito de reproducción de instrucciones o programas de computación, es el delito informático más cometido a

nivel mundial. El acceso a equipo de computación y uso de la tecnología, facilitan la comisión de este delito; a ello se le suma la falta de conocimiento en materia informática en aspectos técnicos y legales, el alto costo de algunos programas de ordenador y los errores en la redacción de los contratos de desarrollo y de licencia.

- **Programas destructivos.**

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

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

- Los registros
- Los programas de ordenador (software)

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

información, al sistema operativo, a los programas en general y se considera que algunos pueden llegar a dañar el hardware"[26].

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

Existen otros tipos de programas informáticos perjudiciales, algunos dañan a la propia computadora, mientras que otros utilizan la computadora para atacar otros elementos de la red; algunos programas (llamados bombas lógicas) pueden permanecer inactivos hasta que se desencadena por algún motivo, como por ejemplo, una fecha determinada, causando graves daños modificando o destruyendo datos. Otros programas parecen benignos, pero cuando se activan, desencadenan un ataque perjudicial (a los denominados caballos de Troya); otros programas (denominados gusanos) no infectan programas con virus, pero crean réplicas de ellos mismos, estas crean a su vez nuevas replicas y de ese modo se termina por invadir el sistema.

Por esta razón las personas que utilizan los sistemas de información deben de protegerse según el nivel de riesgo, con un programa antivirus; los niveles de seguridad dependen de la información y de la interconexión con otras redes.

[26] Valdés Téllez, Julio; **Derecho informático**, pág. 47.

En cuanto al hecho ilícito es importante determinar si existe responsabilidad penal o no, en virtud que la norma establece “al que distribuye o pusiere en circulación…”. Cuando una persona crea el virus informático no tiene responsabilidad penal, porque el simple hecho de crear un programa destructivo no constituye un delito. Cuando éste se distribuye o se pone en una u otras computadoras, en una red interna o externa o la internet, es cuando concurren todos los elementos de tipificación del delito, aunque este no logre el daño que se tiene propuesto en virtud de detección y eliminación por un antivirus o no ingresa a la red por medio de un firewall.

- **Destrucción de registros informáticos**

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

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

El bien jurídico tutelado se define como registro informático, que consiste en la base de datos creada por el sistema informático utilizada para la toma de decisiones. El Artículo 274 “A” establece el que “destruyere, borrare o de cualquier modo…”; destruir información se refiere a que el sujeto responsable del hecho destruya la información lo

que equivale a cambiar su naturaleza de tal forma que no pueda recuperarse por medios electrónicos (el original instalado). Al establecer **borrare**, se refiere a eliminar de forma física en los dispositivos almacenamiento la información. La frase **o de cualquier modo**… deja a una variedad de posibilidades, que puede ejemplificarse en el caso que con intención se grabe información sobre la existente, o utilice algún dispositivo para afectar el acceso a los registros informáticos.

Es importante agregar que aunque la victima cuente con una copia de seguridad de la información (backup) no es causa para eximir de responsabilidades al sujeto activo.

El Artículo 274 "A" también divide los registros en privados y públicos, considerando como un agravante cuando es contra los registros públicos. En ausencia de legislación que determine que debe de entenderse por registro públicos se interpreta que se refieren a los registros a cargo de la administración pública y que contienen datos personales. Otro criterio establece que se refiere a la naturaleza de los datos o información, es decir que los registros serán públicos aún cuando sean almacenados, procesados y/o automatizados por un ente privado.

- **Uso de Información**

El Decreto Número 33-96 del Congreso de la República de Guatemala en el Artículo 18 adiciona el Artículo 274 "F" el cual establece: "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".

En este caso la redacción del Artículo 274 "F" se muestra la confusión o el escaso conocimiento que se tenía por los legisladores en el año 1996 sobre esta materia, en virtud que en un mismo artículo se quieren regular dos situaciones diferentes. Se puede determinar que se protegen dos bienes jurídicos o derechos:

- Los registros informáticos (en cuanto a su utilización no autorizada).
- El acceso debidamente autorizado a los bancos de datos (bases de datos) o archivos electrónicos.

.

- **Los registros informáticos**

La persona que crea un registro informático (de datos lícitos), dispone de quienes van a tener autorización para hacer uso de los mismos. La utilización autorizada de los registros puede ser directa del computador que los tiene almacenados, en línea (red interna y externa) e inclusive pueden ser copiados para ser trasladados a otro equipo de cómputo; esto lo puede realizar una o varias personas autorizadas e inclusive un usuario autorizado para acceder al sistema pero no para utilizar de forma distinta los registros informáticos.

Cuando un sujeto sin la autorización del titular de ese registro informático hace uso del mismo estaría incurriendo entonces en el delito de uso de información. La redacción del

Artículo 274"F" es muy limitada y puede hacer incurrir al operador de justicia en errores. En el caso de utilizar esos registros informáticos en otro sistema de información automatizado, se estaría incurriendo en el delito establecido, le genere ese uso lucro o no. Se puede dar la situación que sea una persona quien "extrae" el registro y otra persona la que lo utilice en su sistema, esto puede estar en concurso con otros delitos.

Es importante considerar que no es el simple uso de ese registro lo que convierte al mismo en delito, en virtud que es necesario determinar algunas características de esa información (que sean datos automatizados) para establecer si es ilícita o no esa conducta. Un ejemplo claro es cuando una persona visita un sitio web por motivos de investigación, trabajos académicos, estudios y en su trabajo hace uso de un registro informático sin la autorización, pero hace la correspondiente referencia (cita bibliográfica).

- **El acceso no autorizado a los bancos de datos o archivos electrónicos**

Para ingresar a un sistema de información se debe de estar autorizado. Esta aprobación de acceso consiste, en el permiso o anuencia que se le otorga a un usuario para poder hacer uso del sistema de información en el sistema establecido. Para ejemplificar este consentimiento en el ordenamiento legal interno se puede mencionar que la resolución 11-2010 de fecha 22 de abril de 2010, emitida por la Dirección Normativa de Contrataciones y Adquisiciones del Estado del Ministerio de Finanzas Públicas que establece "las Normas para el uso del sistema de información de

contrataciones y adquisiciones del Estado –GUATECOMPRAS- , que en el Artículo cuatro establece: “Registro y control de usuarios. Salvo los usuarios con perfil público, el resto de los usuarios debe estar previamente registrado en el sistema GUATECOMPRAS para poder utilizarlo. Los usuarios de perfil Comprador Padre y Contralor deben obtener las contraseñas respectivas a través de la DNCAE quien en su calidad de Administrador y órgano rector del sistema GUATECOMPRAS, administra, capacita y entrega las contraseñas de acceso al sistema. Para el caso de la primera inscripción ésta se otorgará previo a la presentación de la documentación de respaldo que lo acredite para desarrollar el perfil de usuario de que se trate, siendo ésta la siguiente: **a**. copia de cuentadancia, **b.** copia de cédula de vecindad o pasaporte y **c**. solicitud presentada a la DNCAE, en donde se indique el perfil que solicita. Para el caso de los usuarios con perfil proveedor, previo a obtener la contraseña, el interesado deberá inscribirse en BANCASAT, a través de cualquier banco del sistema.”

Se establece entonces que para poder ingresar al sistema de información de GUATECOMPRAS, debe de cumplirse ciertos requisitos previos que la misma resolución ha regulado para poder ser un usuario del sistema, esto limita el acceso a la información contenida en el sistema de información.

Otro ejemplo de autorización y niveles de acceso se tiene en el sistema bancario: Los trabajadores tienen autorización para ingresar a determinados niveles del sistema; el cajero del banco tiene acceso para administrar información en la recepción o entrega de dinero (depósitos monetarios), pero no puede acceder a los estados de cuenta (ver saldo exacto); el jefe de la agencia bancaria si tiene esta última competencia, pero no

puede otorgar transferencias electrónicas por determinados montos y así consecutivamente (según esté diseñado el sistema).

Cuando el acceso al sistema lo realiza una persona que no está autorizada se encuadra esa acción a este delito. Es importante señalar que el simple hecho de acceder sin autorización al banco de datos o archivos electrónicos constituye delito, inclusive si no realiza ninguna acción con la información. Esto se conoce en doctrina como el delito de hacking**.**

Si el acceso fue casual, es decir no existe intención, no hay dolo, no constituirá delito en virtud que no están regulados delitos informáticos culposos.

- **Manipulación de Información.**

El Decreto Número 33-96 del Congreso de la República de Guatemala en el Artículo 17 adiciona el Articulo 274 "E" el cual establece: "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".

El delito de manipulación de la información lo comete el titular, propietario o usuario de los datos, cuando utilizando programas de computación o registros informáticos

diseñados para incumplir obligaciones con el Estado o engañar a otras personas (empresas de crédito, inversionistas, clientes o usuarios) altera la información automatizada. Parte de dos supuestos: el primero ocultar que se refiere a esconder los datos para que no puedan ser encontrados (archivos ocultos); el segundo alterar o distorsionar se refiere a cambiar los datos (unos por otros) o darle a los datos un valor distinto al real.

Además debe determinarse el grado de participación de la persona que es autor (creador) del programa de computación que permite esa administración ilícita de la información, la participación de la persona que ingresa la información y la persona que la utiliza; en el caso del autor del programa la norma establece "al que utilizare…", si el programador se limita a diseñar el programa conforme la solicitud del contratante no tendría ninguna responsabilidad en virtud que él no lo utiliza. En cuanto a la persona que ingresa los datos tampoco tendría responsabilidad, porque ingresar datos para esconderlos, duplicarlos o alterados, no es un delito. La persona que los utiliza, es decir realiza la acción de ponerlos en conocimiento del Estado o de otra persona es la que comete el ilícito. Si el que ingresa los datos tiene conocimiento posterior del hecho tipificado como delito tendría la calidad de encubridor, y si tiene conocimiento que van a ser utilizados con fines ilícitos tendría participación como autor o cómplice según el caso. Es importante establecer que en la redacción del Artículo y por el bien jurídico que protege, se interpreta que la información oculta, alterada o distorsionada se visualiza o accede desde un sistema informático, porque si ésta se imprime y se entrega a un tercero, esa información alterada o distorsionada en formato papel puede constituir otro delito.

- **Registros Prohibidos.**

El Decreto Número 33-96 del Congreso de la República de Guatemala en el Artículo 16 adiciona el Artículo 274 "D" el cual establece: "Registros prohibidos**.** Se impondrá prisión de seis meses a cuatros 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".

El bien jurídico tutelado en el Artículo 274 "D" del Decreto 33-96 del Congreso de la República de Guatemala, es la intimidad de la persona, pero para poder definir de mejor forma este bien jurídico tutelado es importante determinar que son datos personales

Al respecto la Ley de Acceso a la Información Pública Decreto 57-2008 del Congreso de la República de Guatemala en el Artículo nueve numeral 1 define los datos personales como "Los relativos a cualquier información concerniente a personas naturales o identificables". Se entiende entonces que los datos personales es la Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

La doctrina clasifica los datos personales en:

Datos Personales:

- Privados o Íntimos: Sensibles y No Sensibles
- Públicos

Asimismo la Ley de Acceso a la Información Publica también regula una definición de datos sensibles o datos personales sensibles, en el Artículo nueve numeral 2, el cual establece: que son "Aquellos datos personales que se refieren las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico , las ideologías y opiniones políticos, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencias o vida sexual, situación moral y familiar u otras cuestiones intimas de similar naturaleza". Entonces se entiende como datos sensibles aquellos datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Se define como intimidad o privacía, el derecho del individuo a ejercer el control de aquella información de sí mismo, que desee compartir con otros, de la cantidad que de la misma facilite a otros del momento en que desee hacerlo. La violación a esta norma surge cuando se crean bases o bancos de datos que al ser administrados de forma inadecuado o bien adquiridos de una forma ilegal y que entren en la esfera de la intimidad de las personas se estaría cometiendo el delito de registros prohibidos.

# CAPÍTULO III

## 3. Situación internacional

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

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

La OCDE en 1986 publicó un informe titulado **Delitos de informática: análisis de la normativa jurídica**, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que, los países podrían prohibir y sancionar en leyes penales, como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudaran a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité especial de expertos sobre delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas en el ámbito continental, el Consejo de Europa aprobó la recomendación R (89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran crear un marco de seguridad para los sistemas informáticos el mismo año.

En este contexto, considero que, si bien este tipo de organismos gubernamentales han pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con Guatemala, u otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se estableció que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las

economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal en ese momento, era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados.

Por todo ello, en vista de que, los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Octavo Congreso sobre Prevención del Delito y Justicia Penal, recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras, a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a escala internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera de los delitos informáticos y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos,

falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición.

Teniendo presente esa situación, considero que, es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada.

Durante la elaboración de dicho régimen, se deberán considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

### 3.1. Tratamiento en otros países

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

de los criterios y así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente.

Es importante señalar a continuación algunos aspectos relacionados con la legislación en los diferentes países, así como que tipo de delitos informáticos se persiguen

### 3.1.2. Argentina

En Argentina se sancionó el 4 de junio del 2008 la Ley 26.388 que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

En el nuevo ordenamiento se establece que el término **documento** comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos **firma** y **suscripción** comprenden la firma digital, la creación de una firma digital o firmar digitalmente y los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (Artículo siete Código Penal).

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

- Artículo 128: “Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

  Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años”.

- Artículo 153: “Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

- Artículo 153 bis: "Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

  La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

- Artículo 155: "Será reprimido con multa de pesos un mil quinientos a pesos cien mil, el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público".

- Artículo 157: Será reprimido con prisión de un mes a dos años e inhabilitación especial de un a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.
- Artículo 157 bis: Será reprimido con la pena de prisión de un mes a dos años el que:

  1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

  2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

  3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

  Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un a cuatro años"

- Artículo 173 inciso 16: "(Incurre en el delito de defraudación)...El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".
- Artículo 183 del Código Penal: "(Incurre en el delito de daño)...En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o

sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

- Artículo 184 del Código Penal: "(Eleva la pena a tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes):

  Inciso 5: Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

  Inciso 6: Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

- Artículo 197: "Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".
- Artículo 255: "Será reprimido con prisión de un mes a cuatro años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo".

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos".

### 3.1.3. Colombia

En Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado el denominado **De la protección de la información y de los datos** y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado **De la Protección de la información y de los datos** que divide en dos capítulos, a saber: **De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y de los atentados informáticos y otras infracciones.**

En Colombia existen instituciones de educación como UNICOLOMBIA que promueven capacitaciones en temas relacionados con delitos informáticos, el mejor manejo y uso de la evidencia digital, establecer altos estándares científicos y éticos para informáticos forenses, Llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e Instruir a los estudiantes en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática forense, la investigación científica y el proceso tecnológico de las mismas.

### 3.1.4. España

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de noviembre de 1.995. Estos tienen la misma sanción que sus homólogos no-informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo de España emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

### 3.1.5. México

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería está regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

### 3.1.6. Venezuela

En Venezuela se concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.

La ley tipifica cinco clases de delitos:

- Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); favorecimiento culposos del sabotaje o daño. (Art. 8); acceso indebido o sabotaje a sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12).
- Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17); provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19);
- Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20); violación de la privacidad de las comunicaciones (Art. 21); revelación indebida de data o información de carácter personal (Art. 22);
- Contra niños y adolescentes: difusión o exhibición de material pornográfico (Art. 23); exhibición pornográfica de niños o adolescentes (Art. 24);
- Contra el orden económico: apropiación de propiedad intelectual (Art. 25); oferta engañosa (Art. 26).

### 3.1.7. Estados Unidos

En Estados Unidos se adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986. En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país establecen el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos (mensajes electrónicos y contratos establecidos mediante Internet) entre empresas y entre empresas y consumidores

## 3.2. Organización de Estados Americanos (OEA)

La internet, las redes y tecnologías relacionadas se han convertido en instrumentos indispensables para los estados miembros de la OEA. La internet ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran el internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones. Asimismo, en la Tercera Cumbre de las Américas, en la ciudad de Québec, Canadá, en 2001, los líderes se comprometieron a seguir el aumento en la conectividad en las Américas.

Lamentablemente, la internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de internet. La información que transita por internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y defraudar a los negocios. La destrucción de los datos que residen en las computadoras conectadas por internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas. Estas amenazas a los ciudadanos, economías y servicios esenciales, tales como las redes de electricidad, aeropuertos o suministro de agua, no pueden ser abordadas por un solo gobierno ni tampoco pueden combatirse utilizando una sola disciplina o práctica. Como reconoce la Asamblea General en la resolución AG/RES. 1939 (XXXIII-O/03) (Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética), es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario. La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en respaldo a esto, celebró una Conferencia sobre Seguridad Cibernética (Buenos Aires, Argentina, del 28 al 29 de julio de 2003) que demostró la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, y que una acción eficaz para abordar este problema debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales.

La Estrategia Interamericana integral de seguridad cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética.

La Estrategia también reconoce que un marco eficaz para la protección de las redes y sistemas de información que integran la internet y para responder a incidentes y recuperarse de los mismos dependerá en igual medida de que:

- "se proporcione información a los usuarios y operadores para ayudarles a asegurar sus computadoras y redes contra amenazas y vulnerabilidades, y a responder ante incidentes y a recuperarse de los mismos;
- se fomenten asociaciones públicas y privadas con el objetivo de incrementar la educación y la concientización, y se trabaje con el sector privado, el cual posee y opera la mayoría de las infraestructuras de información de las que dependen las naciones, para asegurar esas infraestructuras;
- se identifiquen y evalúen normas técnicas y prácticas óptimas para asegurar la seguridad de la información transmitida por internet y otras redes de comunicaciones, y se promueva la adopción de las mismas; y

- se promueva la adopción de políticas y legislación sobre delito cibernético que protejan a los usuarios de internet y prevengan y disuadan el uso indebido e ilícito de computadoras y redes"[27].

De conformidad con la Declaración de Puerto España, adoptada por los Estados Miembros en el quinto período ordinario de sesiones del CICTE, el terrorismo constituye una grave amenaza a la paz y la seguridad internacionales, socava los esfuerzos continuos que fomentan la estabilidad, prosperidad y equidad en los países de la región, y viola los valores y principios democráticos consagrados en la Carta de la OEA, la Carta Democrática Interamericana y otros instrumentos regionales e internacionales, que dicha declaración está en concordancia con Declaración de Quito, en la cual se expresa por medio de sus miembros su más enérgico rechazo a toda forma de terrorismo y su respaldo al trabajo del CICTE, en el marco de la VI Conferencia de Ministros de Defensa de las Américas, celebrada en el Ecuador en la ciudad de Quito del 16 al 21 de noviembre de 2004, donde se pone énfasis en la facilitación del dialogo de los países miembros de la OEA a fin de desarrollar y avanzar medidas preventivas que anticipen y enfrenten las amenazas terroristas emergentes, como son los delitos informáticos.

### 3.3. La Convención de las Naciones Unidas contra la delincuencia organizada

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que entró en vigor en septiembre de 2003, es el principal instrumento

[27] **La Estrategia Interamericana integral de seguridad cibernética**
http://www.oas.org/juridico/english/**cyb_pry_estrategia**.pdf , (visitada el 30 de junio del 2,011)

internacional en la lucha contra la delincuencia organizada. La Convención tiene 147 Estados signatarios y 100 Estados parte, en dicha convención se pone de manifiesto las reglas básicas sobre la prosecución de Delincuencia Organizada Transnacional, dichas reglas hacen especial mención de los delitos relacionados con la legitimación de activos y los de corrupción. También se mencionan a los llamados **delitos graves** que son de acuerdo con el Artículo 2 toda "conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave". En el caso de las llamadas infracciones informáticas todas ellas son delitos graves de acuerdo a la definición de la Convención, en tal razón se encuadran en su ámbito de aplicación de la convención de conformidad al Artículo tres, siempre que dichos delitos sean de carácter transnacional y entrañen la participación de un grupo delictivo organizado.

De igual forma se debe tomar en cuenta que la Convención da la posibilidad de conseguir capacitación y asistencia de parte de los Estados signatarios en la prevención e investigación de esta clase de delitos e insta a contar con programas de capacitación y entrenamiento a las personas responsables del cumplimiento de la ley como jueces, fiscales y policías. También insiste en el uso de técnicas especiales de investigación como la vigilancia electrónica.

### 3.4. Convenio de sobre la cibercriminalidad de la Unión Europea

Este convenio busca como objetivos fundamentales los siguientes:

- Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático;
- proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y
- establecer un régimen dinámico y efectivo de cooperación internacional.

El convenio se basa en el reconocimiento fundamental de que se necesita armonizar las leyes nacionales. Es decir contar a nivel de la Unión Europea con una herramienta común tanto sustantiva como adjetiva para procesar este tipo de manifestaciones delictivas, procurando con este elemento comunitario en la parte sustantiva el mejoramiento de la cooperación internacional de los países miembros, ya que solamente existiría en esta materia, la aplicación de una ley común de carácter supranacional que permita a los gobiernos intercambiar información y pruebas. Sin embargo, para que esto de resultados y exista una verdadera cooperación hemisférica y ayuda jurídica mutua debe entrar en vigor este tipo de convenios a fin de unificar los tipos penales existentes sobre la delincuencia informática y así lograr la correlación o correspondencia entre los tipos penales en las diferentes jurisdicciones nacionales de los países miembros de la Unión Europea.

De hecho, cuanto más alcance tengan las leyes, tanto menor será el número de refugios desde la delincuencia informática organizada puede operar con impunidad.

La armonización es necesaria tanto para las leyes sustantivas como las procesales como se manifestó anteriormente. Es por tanto que todos los países deben reevaluar y revisar sus reglamentos acerca de las pruebas, el registro e incautación de los efectos de esta clase de infracciones, la vigilancia electrónica oculta y otras actividades similares, que abarquen la información digital, los sistemas modernos de computación y comunicación y la naturaleza mundial de la internet y sus diferentes servicios. Ya que al igual que las leyes sustantivas, una mayor coordinación de las leyes procesales facilitaría, de hecho, la cooperación en las investigaciones que trasciendan jurisdicciones múltiples. La Convención sobre Delitos Informáticos constituye sin duda el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos.

La misma tiene lugar en momentos en que la internet ha dejado de ser tan solo el vehículo más idóneo para la propagación y perfeccionamiento de actos criminales bajo condiciones de anonimidad, sino que además representa el entorno más frecuentemente utilizado para la financiación de este tipo de actividades.

### 3.5. Situación a nivel nacional

A nivel nacional no ha existido el interés por crear una política de combate a la criminalidad informática, pese que en la mayoría de entidades estatales utilizan sistemas informáticos y por ende surgen el riesgo de sufrir cualquier tipo de atentado a los mismos, aun y cuando en el Decreto 33-96 del Congreso de la Republica Guatemala se adicionan una serie de delitos relacionados con la informática, la

legislación nacional esta desactualizada y es necesario ponerla al día en este sentido; cabe mencionar que existe la iniciativa de Ley número 4055 del año 2009, y en la misma se ajusta de mejor manera a la actualidad en materia de delitos informáticos, ya que se ajusta a las diferentes legislaciones internacionales y convenios en esta materia, que han incluido en sus normas legales figuras delictivas de diferentes índoles.

Lo importante de esta iniciativa es que plantea la necesidad de la aprobación de una ley especial que contenga disposiciones que tiendan a proteger, integralmente, los sistemas informáticos y bases de datos, a fin de garantizar certeza jurídica en las transacciones propias del comercio electrónico. Se observa que la iniciativa toma en consideración el comercio electrónico, esto de acuerdo con el contenido de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008 del Congreso de la República de Guatemala que cada vez es más utilizado a nivel nacional, así como establece la necesidad de emitir una ley especial para prevenir y sancionar los delitos cometidos con ocasión a la normativa de comercio electrónico, y todos aquellos actos ilícitos de naturaleza informática, de igual manera establece la necesidad de la efectiva creación y aplicación de normas especiales, toda vez que, por la naturaleza de los actos de cibercrimen, se complica la aplicación de las actuales normas del Código Penal, lo que se traduce en lagunas legales que permiten al delincuente realizar actos ilícitos por medio de las nuevas tecnologías de la información. Así también, plantea la necesidad de crear una unidad especializada para investigar y combatir la delincuencia informática.

La iniciativa además establece en cuanto a su ámbito de aplicación que la ley será aplicable a los responsables de los hechos punibles si estos hubieren sido cometidos en la República de Guatemala o bien cuando alguno de los delitos previstos en la ley se cometa fuera del territorio de la República, el responsable quedará sujeto a sus disposiciones si dentro del territorio nacional se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

La iniciativa hace una clasificación legal de tres grupos de delitos contenido de la siguiente forma:

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos**. En este grupo se encuentran los delitos de: acceso sin autorización, daño informático, posesión de equipos o prestación de servicios para daño informático, espionaje informático.
- **Delitos informáticos relacionados con la propiedad y autenticidad**. Dentro de este grupo se encuentran: fraude informático, uso fraudulento de tarjetas inteligentes o instrumentos análogos, provisión indebida de bienes o servicios, posesión de equipo para falsificaciones, falsificación Informática, invitación de acceso.
- **Delitos relacionados con el contenido**. En este tercer grupo se encuentran los delitos siguientes: pornografía infantil, alteración de imágenes.

Se puede observar que la iniciativa ya incluye delitos que no están contemplados dentro del Código Penal guatemalteco como delitos informáticos, ya que no se limita a proteger la propiedad, sino abarca otros bienes jurídicos que en la actualidad son

lesionados por las nuevas formas de cometer ilícitos, a través de las nuevas tecnologías de la información, y el uso indebido de la tecnología, es importante darle la importancia necesaria a estos delitos y buscar la forma de actualizar tanto a las normas, como la forma de investigar, juzgar y sancionar estos delitos.

Desafortunadamente en la actualidad no existe interés ni la voluntad política por parte de los legisladores del Congreso de la República de Guatemala, ni del gobierno central por combatir este tipo de criminalidad, ya que esta iniciativa no ha pasado de ser eso, una iniciativa, y aunque es necesario estudiarla más a fondo y perfeccionar la misma puede servir de base para una futura ley que combata esta forma de delincuencia que cada día se desarrolla y se perfecciona en Guatemala.

# CAPÍTULO IV

## 4. Prevención de la delincuencia informática.

Los ataques a la información dirigidas a la revelación no autorizada de la misma, de la modificación o destrucción accidental o intencional o la incapacidad para procesar esa información son algunos de los aspectos más importantes que se deben de proteger

Con el fin de prevenir los ataques por parte de la delincuencia informática ya sea nacional o internacional se debe contar con dos variables importantes que son:

### 4.1. La seguridad informática

Se define como "el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya sean estos individuales o conectados a una red frente a posibles ataques premeditados y sucesos accidentales"[28].

La seguridad informática a su vez está dividida en cinco componentes a saber:

[28] Del pino, Santiago Acurio, **Informática forense en el Ecuador**, pág.23.

- **Seguridad física**

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

- **Seguridad de datos**

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

- **Back up y recuperación de datos**

Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back up de los sistemas informáticos. Permite recuperar la información necesaria en caso de que esta sufra de daños o se pierda.

- **Disponibilidad de los recursos**

Este cuarto componente procura que los recursos y los datos almacenados en el sistema puedan ser rápidamente accesados por la persona o personas que lo

requieren. Permite evaluar constantemente los puntos críticos del sistema para así poderlos corregir de manera inmediata.

- **Análisis forense**

El análisis forense o informática forense, punto principal del presente trabajo, surge como consecuencia de la necesidad de investigar los incidentes de seguridad informática, que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales. Este tema se desarrollara de mejor manera en el último capítulo del presente trabajo.

### 4.2. La Seguridad normativa (políticas de seguridad)

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

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

### 4.3. El delito informático y su realidad procesal en Guatemala

El código penal, como se desarrolló en el capítulo II del presente trabajo, contiene dentro de su capítulo VII título, los artículos 274 "A"" al 274 "G" que regula los siguientes delitos informáticos:

- "Alteración de programas.
- Reproducción de instrucciones o programas de computación.
- Destrucción de registros informáticos.
- Manipulación de información.
- Uso de Información.
- Programas destructivos
- Registros prohibidos"

El problema en la persecución penal de los delitos informáticos radica en que este tipo de infracciones son difícilmente descubiertas o perseguidas ya que los sujetos activos actúan sigilosamente, y poseen herramientas capaces de borrar todo rastro de intrusión en la consumación del delito, y esto sumado a no contar en con una policía capacitada para investigar dichos hechos, el personal del Ministerio Público no tiene la capacitación necesaria que pueda dar las directrices para la correcta investigación y recolección de evidencia de dichos actos delictivos, por otro lado no se cuenta con una legislación especial que regule estas conductas de forma actualizada, la necesidad de las herramientas tecnológicas científicas que ayuden al examen de la evidencia digital y su posterior presentación como medio de prueba ante los tribunales de justicia manteniendo de siempre la cadena de custodia y la identidad de la evidencia, la

necesidad de que los juzgadores conozcan sobre la materia para poder interpretar la evidencia digital, para resolver de la manera más justa y objetiva los procesos en los delitos informáticos.

Tomando en cuenta que este tipo de delitos evolucionan a gran velocidad y son producto de la evolución de la delincuencia con le aparecimiento de las nuevas tecnologías de la información, se debe de contar con una unidad especial para la investigación y persecución de estas infracciones informáticas, pero además existen varios problemas que en la realidad procesal es importante desarrollar.

### 4.3.1. Problemática con la concepción tradicional de tiempo y espacio

El principio de territorialidad sostiene que la ley penal de un país es aplicable cuando la infracción ha sido cometida dentro del territorio, en el momento actual esto puede haber cambiado teniendo en cuenta que el nuevo escenario en donde mayormente se da este tipo de delitos es el ciberespacio, un lugar donde no existen fronteras territoriales, y que de acuerdo a Jhon Perry Barlow, quien publicó lo que se llama **La Declaración de Independencia del Ciberespacio**, en donde manifiesta: "Gobiernos del mundo industrializado, gigantes obsoletos , de la nueva morada del espíritu (…) No os queremos entre nosotros, en el terreno donde nos reunimos no sois soberanos.. Vuestros conceptos jurídicos de propiedad, de expresión, de identidad, de movimiento y de contexto no se aplican a nosotros. Están basados en la materia"[29].

[29] http://www.eff.org/pub/publications/**Jhon_perry_barlow/barlow_**0296 (visitada el 6 de junio de 2,010)

Por lo expuesto se puede constatar que es difícil la persecución de estos delitos y su enjuiciamiento, ya que existe la posibilidad de preparar y cometer acciones delictivas informáticas en perjuicio de terceros en tiempo y espacio lejanos.

La territorialidad de la ley es considerada como un principio de soberanía del Estado y se resume al decir que no se puede aplicar al guatemalteco delincuente otra ley que no sea la guatemalteca, aclarando que no importa el lugar donde se encuentre el delincuente, es decir, sin importar el país en donde se haya cometido el delito.

El Doctor Santiago Acurio del Pino establece que "la ley penal es aplicable a los hechos punibles cometidos dentro del territorio del Estado, sin consideración a la nacionalidad el actor, de conformidad con las siguientes reglas:

- No se toma en cuenta la nacionalidad del autor.
- Se toma en cuenta el lugar de comisión del delito. La legislación se inclina por la teoría del resultado, es decir que la infracción se entiende cometida en el territorio del Estado cuando los efectos de la acción u omisión deban producirse en el Guatemala o en los lugares sometidos a su jurisdicción.
- Se aplica al concepto jurídico de territorio por el Derecho Internacional: los límites del Estado, mar territorial. espacio aéreo, etc.
- Se aplica también la teoría del territorio flotante o principio de la bandera: naves o aeronaves de bandera nacional ya sea que se encuentren en alta mar, en su espacio aéreo y en lugares en que por la existencia de un convenio internacional, ejerzan jurisdicción".[30]

[30] Del Pino Santiago Acurio, **Delitos informáticos generalidades**, pág. 58.

### 4.3.2. Principio de la nacionalidad o personalidad

Según este principio, se debe aplicar al sujeto activo únicamente la ley que corresponde a su nacionalidad, es decir, la ley del país de su origen, sea el país que sea en el que haya cometido el delito. Este principio tiene dos divisiones:

- **Principio de la nacionalidad activa**

Se funda en la obediencia que se exige al súbdito guatemalteco con respecto a su legislación. Se toma en cuenta la nacionalidad del autor del delito.

- **Principio de la nacionalidad pasiva**

El alcance espacial de la ley se extiende en función del ofendido o titular del bien jurídico protegido. Se aplicaría cuando está en juego la protección de los bienes jurídicos individuales

### 4.3.3. Principio de la defensa

Este establece que es aplicable la ley del país donde los principios son atacados por el delito, sin tomar en cuenta la nacionalidad de los realizadores. Se toma en cuenta la nacionalidad del bien jurídico protegido, es decir se aplica este principio cuando se afecta la integridad territorial. Quedando en juego la protección de los bienes nacionales. Ha sido tomado por algunos países, como por ejemplo Guatemala, el cual

puede pedir la extradición de una delincuente informático que haya vulnerado bienes jurídicos protegidos en este país como resultado de su acción delictiva, claro que esta norma no puede ser aplicada en todos los países, ya que algunos de ellos prohíbe la extradición de personas que hayan cometido una infracción en otro país, en este caso se aplica un principio de equivalencia, es decir, si el delito cometido en el otro país se encuentra tipificado en Guatemala también puede seguirse el proceso penal por el cometimiento de dicho delito.

### 4.3.4. Principio de la universalidad y justicia mundial

Este principio se refiere a que es aplicable la ley del país que primero aprehenda al delincuente, sin considerar otro aspecto.

Este principio tiene una finalidad práctica para reprimir los delitos contra la humanidad, aquellos que han sido catalogados como tales en virtud de ser considerados como ofensores de toda la humanidad. Para ello es necesario firmar convenios internacionales y unilaterales con el fin de que cada país pueda sancionar al delincuente con su propia ley, sin importar el lugar donde el individuo haya cometido el acto ni tampoco la nacionalidad del mismo.

Se prescinde tanto de la nacionalidad del autor como del lugar de comisión del delito, se fundamenta en el principio de solidaridad de los estados en la lucha contra el delito.

En doctrina penal se concede en virtud de este principio eficacia extraterritorial a la ley penal; pero en el derecho internacional condiciona esta eficacia extraterritorial tomando en cuenta:

- La calidad del bien jurídico protegido, como bienes culturales supranacionales.
- Cuando los autores del delito sean peligrosos para todos los estados.

En cuanto a los delitos informáticos de carácter transnacional, en especial el ciberterrorismo es necesario aplicar este principio por cuanto la peligrosidad de este tipo de ataques puede causar más daño que el terrorismo convencional.

### 4.4. Anonimato del sujeto activo

El anonimato del sujeto activo que participa en los delitos informáticos es un aspecto importante por cuanto que el sujeto activo de esta clase de delitos, puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que este no necesariamente puede usar su propio sistema informático, sino que se puede valer de un tercero, como por ejemplo en el caso del envío de correo no deseado o **SPAM**, en el cual se puede usar a una máquina zombi, es decir una computadora que está bajo el control del **SPAMER** y que le permite usarla como una estación de trabajo de su propia red de máquinas zombis, las cuales pertenecen a usuarios desaprensivos que no tienen al día sus medidas de seguridad y que son fácil presa de los hackers y crackers para cometer este tipo de infracciones. También

existen programas de enmascaramiento o que no permiten ver la verdadera dirección ya sea de correo electrónico o del número IP (número de identificación de red).

# CAPÍTULO V

## 5. Propuesta de implementación de la informática forense

Es importante hacer un análisis introductorio a la informática forense a fin de sentar las bases de la investigación científica en esta materia, con el objeto de proporcionar a los futuros investigadores las herramientas para poder manejar de manera técnica y legal una escena de crimen en donde se vean involucrados sistemas de información o redes y la posterior recolección y/o recuperación de la llamada evidencia digital. En la actualidad no existen investigadores especializados en estos delitos ni el Ministerio Público, ni la Policía Nacional Civil cuenta con personal capacitado para tales labores, de la misma forma el Instituto Nacional de Ciencias Forenses. Para este tipo de casos se utiliza muchas veces a personal del departamento de informática del Ministerio Público, o bien como los llamados consultores técnicos de idoneidad manifiesta para dar fuerza a los dictámenes que se emiten en las investigaciones de delitos informáticos, es entonces como se utiliza más la experiencia en la informática que la preparación técnico- académica a nivel profesional de los peritos.

### 5.1. Las ciencias forenses

Es importante antes de desarrollar el tema de la informática forense que se tenga un panorama básico de lo que son las ciencias forenses en el sentido que se entienden como la utilización de procedimientos y conocimientos científicos para encontrar, adquirir, preservar y analizar las evidencias de un delito y presentarlas apropiadamente

a los tribunales de justicia. Las ciencias forenses tienen que ver principalmente con la recuperación y análisis de la llamada evidencia latente, como por ejemplo: las huellas digitales, la comparación de muestras de ADN, etc. Las ciencias forenses combinan el conocimiento científico y las diferentes técnicas que este proporciona con los presupuestos legales a fin de demostrar con la evidencia recuperada la existencia de la comisión de un acto considerado como delito y sus posibles responsables ante un tribunal de justicia.

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

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

## 5.2. La informática forense

En principio se puede definir a la informática forense como, una ciencia forense que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos informáticos y donde se utiliza el análisis forense de las evidencias digitales, en fin toda información o datos que se guardan en una computadora o sistema informático.

El doctor Santiago Acurio Del Pino define a la Informática Forense como "la ciencia forense que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, para luego ésta ser presentada en un juzgado o tribunal competente"[31].

A la informática forense se la dado diferentes denominaciones como por ejemplo, computación forense, análisis forense digital o exanimación forense digital

La informática forense se caracteriza principalmente por la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

En conclusión la informática forense por tanto será la ciencia forense formal que se encarga del estudio de los métodos y técnicas de identificar, extraer, analizar, preservar y presentar a través de técnicas y herramientas la información, que permitan al

[31] Del Pino, Santiago Acurio. **Obi. Cit.,** pág.8

investigador forense digital poder entregar un informe en donde presente los hallazgos de manera lógica y con un sustento claro de lo que desea mostrar, y a la actividad que realiza el investigador es la investigación forense o exanimación forense aplicando los métodos y técnicas desarrolladas por la informática forense

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

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

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

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

### 5.3. Evidencia digital

"La evidencia digital se constituye en todos aquellos datos e información histórica y presente almacenada en archivos lógicos para que se pueda procesar mediante algoritmos abiertos y auditables, con la finalidad de ser expuestos de manera muy sencilla ante los tribunales de justicia"[32]

Para Miguel López Delgado la evidencia digital "es el conjunto de datos en formato binario, esto se comprende en los archivos, su contenido o referencias a éstos, que se encuentren en los soportes físicos o lógicos de un sistema comprometido por un incidente informático"[33].

Otros autores como Anthony Reyes se refieren a la evidencia digital como "objetos de datos" en relación a la información que es encontrada en los dispositivos de almacenamiento o en las piezas de almacenamiento de multimedia, que no son más que cadenas de unos y ceros, es decir de información binaria o digital grabada en un

[32] Del Pino, Santiago Acurio. **Obi. Cit.,** pág.10.
[33] López Delgado, Miguel, **Análisis forense digital**, pág.19.

dispositivo magnético (como discos duros o los disquetes), en uno de estado sólido o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD)"[34].

Como se ha mencionado la evidencia digital se puede encontrar en una gran cantidad de dispositivos, tales como computadores personales, en IPODS, teléfonos celulares, los cuales tienen sistemas operativos y programas que combinan en un particular orden esas cadenas de unos y ceros para crear imágenes, documentos, música y muchas cosas más en formato digital. Pero también existen evidencia digita existente en datos que no están organizados como archivos sino que son fragmentos de archivos que quedan después de que se sobrescribe la información a causa del borrado de los archivos viejos y la creación de los archivos nuevos, esto se llama **SLACK SPACE**, o espacio inactivo. También pueden quedar almacenados temporalmente en los archivos de intercambio o en la misma memoria RAM.

### 5.3.1. Validez jurídica de la evidencia digital

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

[34] Reyes**,** Anthony**, Investigación del Cibercrimen**, pág.34.

- **Autenticidad**

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

- **Precisión**

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

- **Suficiencia**

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

### 5.3.2. Fuentes de la evidencia digital

En muchas ocasiones se tiende a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distinguir entre aparatos electrónicos como los celulares y PDAs (asistentes digitales personales, por sus siglas en ingles) y la información digital que estos contengan. Esto es indispensable ya que el foco de la investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos.

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

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

- **Sistemas de computación abiertos**

Son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles y los servidores. Actualmente estos computadores tienen la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.

- **Sistemas de comunicación**

Estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el internet. Son también una gran fuente de información y de evidencia digital.

- **Sistemas convergentes de computación**

Son los que están formados por los teléfonos celulares llamados inteligentes o **SMARTPHONES**, los asistentes personales digitales **PDAs** (asistentes digitales personales, por sus siglas en ingles), las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

Dada la ubicuidad de la evidencia digital es raro el delito informático que no esté asociado a un mensaje de datos guardado y transmitido por medios informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

### 5.3.3. Evidencia digital constante y volátil

En un principio el tipo de evidencia digital que se buscaba en los equipos informáticos era del tipo constante o persistente es decir, la que se encontraba almacenada en un disco duro o en otro medio informático y que se mantenía preservada después de que

la computadora era apagada. Posteriormente y gracias a las redes de interconexión, el investigador forense se ve obligado a buscar también evidencia del tipo volátil, es decir evidencia que se encuentra alojada temporalmente en la memoria **RAM**, o en el **CACHE**, son evidencias que por su naturaleza inestable se pierden cuando el computador es apagado. Es importante mencionar que este tipo de evidencias deben ser recuperadas casi de inmediato.

La información residente en los medios de almacenamiento electrónico puede ser borrada, cambiada o eliminada sin dejar rastro, lo cual limita la labor del investigador forense para identificar y encontrar elementos claves para esclarecer los hechos relevantes de una investigación.

De esto se desprende que cuando se comete un delito cualquiera, muchas veces la información que directa o indirectamente se relaciona con esta conducta criminal queda almacenada en forma digital dentro de un sistema informático. Este conjunto de datos ordenados sistemáticamente y convertidos en información se convierte en evidencia digital. Aquí se presenta la primera dificultad en lo que se refiere a la obtención de esta clase de evidencia como prueba de la infracción cometida, esto debido a que los sistemas informáticos en donde se almacena la misma presentan características técnicas propias, en tal razón la información ahí almacenada no puede ser recuperada, recolectada, preservada, procesada y posteriormente presentada como indicio de convicción utilizando los medios criminalísticas comunes, se debe utilizar mecanismos diferentes a los tradicionales. Es aquí donde radica la necesidad de utilizar los procedimientos técnicos legales y la rigurosidad científica que pone a disposición de los

investigadores la informática forense a fin de descubrir a los autores y cómplices del delito informático cometido.

Como consecuencia la falta de información especializada en esta área de investigación científica, la inexistente práctica y capacitación en la obtención, recolección, documentación y posterior análisis e interpretación de la evidencia digital, pueden dar como resultado una sentencia condenatoria contra un inocente y se deje libre a un culpable, situación que no puede permitirse en un proceso penal, es por tanto necesarios que los entes encargados de la investigación, es decir el Ministerio Publico, la Policía Nacional Civil así como los jueces al momento de dictar sus resoluciones, deben de estar preparados para afrontar el reto de capacitar y entrenar al personal necesario para que lidien de forma óptima no solo con los delitos informáticos sino también con otra clase de delitos, aprovechando así las ventajas de utilizar la informática forense y la evidencia digital dentro de los procesos penales.

### 5.4. Roles en la investigación

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

- **"Técnicos en escenas del crimen informáticas:** son los primeros en llegar a la escena del crimen, son los encargados de recolectar las evidencias que ahí se encuentran. Tiene una formación básica en el manejo de evidencia y documentación, al igual que en reconstrucción del delito y la localización de elementos de convicción dentro de la red.
- **Examinadores de evidencia digital o informática (peritos informáticos):** son los responsables de procesar toda la evidencia digital o informática obtenida por los técnicos en escenas del crimen informáticos. Para esto dichas personas requieren tener un alto grado de especialización en el área de sistemas e informática. En Guatemala este proceso deberían de realizarlo peritos del Instituto Nacional de Ciencias Forenses.
- **Investigadores de delitos informáticos:** son los responsables de realizar la investigación de campo y la reconstrucción de los hechos de los delitos Informáticos de manera general, son personas que tiene un entrenamiento general en cuestiones de informática forense, son profesionales en seguridad informática, policías y examinadores forenses"[35].

### 5.5. Peritos informáticos

Es indispensable para la valoración de las pruebas o elementos de convicción la intervención de personas que tengan especiales conocimientos en materias especiales, en este caso de la materia informática, personas que prestan un servicio especial al fiscal y al juez al momento de ilustrar sobre las materias, técnicas o artes que son de su

[35] Del Pino, Santiago Acurio. **Obi. Cit.,** pág.15.

conocimiento, a fin de que dichos funcionarios en función de dichas explicaciones puedan emitir su criterio en el momento adecuado.

De acuerdo a lo que dispone el Artículo 226 del Código Procesal Penal, "los peritos deberán ser titulados en la materia a que pertenezca el punto sobre el que han de pronunciarse, siempre que la profesión, arte o técnica estén reglamentados.." los profesionales deberán ser especializados en diferentes materias y que hayan sido acreditados como tales.

Peritos son las personas que por disposición legal, encargo judicial o de la fiscalía aportan con sus conocimientos los datos necesarios para que el juez, el fiscal o la policía adquieran un grado de conocimiento para determinar las circunstancias en que se cometió una infracción, por tanto el perito entrega los elementos de convicción que permita al juez o al tribunal crear un razonamiento que dictar la resolución del caso propuesto, en fin aportan elementos que tanto el fiscal en la formulación de la acusación así como el juez valorarlos al emitir su resolución.

El profesor Jeimy Cano llama a los peritos informáticos forenses: "investigadores en informática y los define como "profesionales que contando con un conocimiento de los fenómenos técnicos en informática, son personas preparadas para aplicar procedimientos legales y técnicamente válidos para establecer evidencias en situaciones donde se vulneran o comprometen sistemas, utilizando métodos y procedimientos científicamente probados y claros que permitan establecer posibles

hipótesis sobre el hecho y contar con la evidencia requerida que sustente dichas hipótesis

Las características o requisitos que deben reunir las personas para ser peritos son:

- Ser profesional especializado y calificado, poniendo a salvo un criterio, que es aquel de que no necesariamente el perito es un profesional en determinada rama, sino una persona experta o especializada en su respectivo campo de determinada materia.
- Mayores de edad, los peritos deben tener la mayoría de edad que en nuestro país se fija en 18 años, porque a esa edad la persona ha alcanzado la madurez psicológica necesaria para prestar esta clase de asesoramiento a la administración de justicia.
- Reconocida honradez y probidad, en cuanto a la calidad moral del perito, de proceder recto, integro y honrado en el obrar, el perito es un personaje esencialmente imparcial que cumple con su cometido y se desvincula del proceso.
- Conocimientos específicos en la materia sobre la que debe informar, es decir los necesarios y específicos conocimientos para cumplir su cometido"[36].

La pericia es un medio de prueba específicamente mencionado por el Código Procesal Penal guatemalteco, con el cual se intenta obtener para el proceso, un dictamen

[36] Cano Jeimy**, Estado del arte de peritaje informático en Latinoamérica**. http://www.alfa-redy.org (visitada 15 de junio de 2,011)

fundado en especiales conocimientos científicos, técnicos o artísticos, útil para el descubrimiento o valoración de un elemento de prueba.

Un informe pericial, sus conclusiones u observaciones no son definitivos ni concluyentes, la valoración jurídica del informe pericial queda a criterio del fiscal, juez penal o tribunal de sentencia penal, quienes pueden aceptarlo o no, con el debido sustento o motivación.

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

El perito debe regirse por los siguientes principios:

- **"Objetividad:** El perito debe ser objetivo, debe observar los códigos de ética profesional.
- **Autenticidad y conservación:** Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.
- **Legalidad:** El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de sus actividades periciales y cumplir con los requisitos establecidos por ella.
- **Idoneidad:** Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.

- **Inalterabilidad:** En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.
- **Documentación:** Deberá establecerse por escrito los pasos dados en el procedimiento pericial"[37].

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

El perito informático forense según la opinión del profesor Jeimy Cano "requiere la formación de un perito informático integral que siendo especialista en temas de tecnologías de información, también debe ser formado en las disciplinas jurídicas, criminalísticas y forenses. En este sentido, el perfil que debe mostrar el perito informático es el de un profesional híbrido que no le es indiferente su área de formación profesional y las ciencias jurídicas"[38].

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

[37] Cano, Jeimy **Ob. Cit.**
[38] Cano, Jeimy **Ob. Cit.**

El perito informático cumple un rol importante dentro de una investigación penal. nace como la respuesta natural de la evolución de la administración de justicia que busca avanzar y fortalecer sus estrategias para proveer los recursos técnicos, científicos y jurídicos que permitan a los jueces, así como al Ministerio Público y a la Policía Nacional Civil, alcanzar la verdad y asegurar el debido proceso en un ambiente de evidencias digitales.

### 5.6. Etapas de la investigación forense o análisis forense

El análisis forense se entiende como "el proceso formal que se encarga de recoger, analizar, preservar y presentar a través de técnicas y herramientas la información, de tal forma que el investigador forense digital pueda entregar un informe en donde presente los hallazgos de manera lógica y con un sustento claro de lo que desea mostrar."[39]

Se puede describir el proceso de análisis forense a través de las siguientes fases:

#### 5.6.1. Preparación

Fase en la que, como su nombre lo indica, se prepara todo para poder realizar la investigación correspondiente, sin ser las únicas actividades están:

[39] **Enciclopedia CCI, Criminalística, Criminología e Investigación**. Tomo III, Investigación, Investigación policial, procedimientos y técnicas científicas, pág.1195.

- Establecer lo que se necesita para realizar la investigación tanto a nivel operacional como técnico.
- Se requiere de todas las autorizaciones legales para poder adelantar la inspección y el levantamiento de la información.
- Es necesario que los protocolos de los técnicos en escena del crimen que son las primeras personas que llegan a la escena, estén claramente definidos, de tal manera que aseguren la escena del crimen que está bajo investigación.
- Definir de manera clara la estrategia con la que se debe identificar, recolectar, embalar, analizar y transportar toda la evidencia.
- Definir claramente los perfiles que van a ser involucrados en la investigación, tanto a nivel operacional, analistas forenses y líder o líderes de los casos.

### 5.6.2. Investigación

La investigación es el componente más complejo del proceso, e involucra un gran número de actividades.

Esta etapa de investigación debe tener clara la premisa de que es importante, desde el principio hasta el fin, mantener la cadena de custodia; por consiguiente, la documentación será la pieza fundamental del proceso. De igual manera esto puede ser dividido en dos momentos.

### 5.6.3. Recolección de los elementos físicos

El primero es asegurar la escena del crimen y su respectiva documentación, para lo cual se deben tener en cuenta las siguientes consideraciones:

- **Asegurar y evaluar la escena del crimen**

Dentro de la escena del crimen es necesario que se realicen las siguientes actividades:

- Aislar la escena del crimen, en ella debe realizar un proceso de observación de la escena y en caso de ser posible delimitar la escena física.
- Realizar las entrevistas preliminares de tal manera que se indague por la información y sobre todo de la escena bajo investigación, de igual manera, es necesario que estas actividades estén debidamente documentadas.

- **Documentación de la escena del crimen**

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

- Toma de fotografía y/o video de la escena.
- Documentación de los componentes de la escena, describiendo cada uno de ellos.
- Etiquetar todos y cada uno de los componentes de la escena.

- **Recolección de la evidencia digital**

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

- Se documente el estado en el que se encuentra el medio tecnológico, indispensable documentar si se encuentra apagado o encendido el medio tecnológico, puesto que de cada uno de estos estados se debe realizar una acción en particular.
- Tomar en caso de ser necesario la información más volátil del sistema, entre ellas están la información de la memoria y los procesos que se están ejecutando en caso de estar prendida la máquina y en operación normal.

- **Almacenamiento, transporte y embalaje de los indicios.**

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

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

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

- **Análisis de la información recolectada**

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

- **Trabajar sobre una copia fiel y exacta del medio bajo investigación**

Esto requiere de las herramientas necesarias que permitan obtener el número de copias que sean necesarias, de tal manera que el medio original quede como evidencia, en caso de que se requiera restringir indagar sobre la veracidad del proceso.

- **Proceder con la extracción de la información**

Al proceder con la extracción de la información se puede:

- Utilizar más de una herramienta de extracción de información, con el objetivo de dar mayores garantías al proceso.
- Extraer información acerca del correo electrónico.
- Logs del sistema, ingresados al mismo.
- Identificación de volatilidad de la información más volátil a la menos volátil.
- Extracción de los datos y filtrado de los mismos.
- Identificar y recuperar datos que han sido:

  Eliminados, escondidos, cifrados, corruptos
- Determinar líneas de tiempo o secuencia en que los eventos se presentaron.
- Evaluación del perfil del atacante.
- Construir un marco del caso en donde, de manera lógica y secuencial, se relaten los hechos identificados basados en los hallazgos.

- **Presentación e informes**

Esta fase permite entregar un informe donde se presentan de manera ordenada los hallazgos encontrados, o las evidencias necesarias para soportar una investigación que se esté realizando. Dependiendo de la naturaleza de la investigación, si es de carácter interno, sólo intervienen las partes implicadas bien sea recursos humanos, directivas de la organización, e implicados, mientras en las investigaciones dentro de un proceso

penal, donde intervienen entes judiciales intervendrán las partes como abogados defensores, jueces, fiscales, los reportes deben poseer las siguientes características:

- Una estructura que muestre de manera lógica la evolución de un caso investigado.
- No deben estar sujetos a juicios de valor por parte de quien redacta el reporte o generar parcialidad en el mismo, inclusive es necesario su revisión para evitar posibles inconsistencias.
- Debe ser claro, conciso, breve y simple, de tal forma que refleje sin rodeos lo que se desea mostrar.
- Es necesario que se utilice un lenguaje sencillo y claro para enlazar todos los eventos identificados.
- Los argumentos, en todos los casos, han de estar sustentados en los hallazgos identificados.
- Debe existir de manera clara la identificación del caso, fechas en que fue realizado el proceso y los procedimientos utilizados.
- Es necesario que de manera resumida se presenten los hallazgos encontrados, en caso de ser necesario se puede escribir un informe adicional con todos los detalles técnicos con los cuales se llevó a cabo el proceso de análisis de la evidencia.
- Es necesario que los reportes sean entregados en medios no modificables, ejemplo de ello puede ser formato PDF.

De igual manera un informe debe poseer como mínimo la siguiente estructura básica:

- **Introducción:** Quién solicitó el informe, qué se buscó, quién escribió el informe, cuándo y qué fue encontrado.
- **Resumen de evidencias:** Qué evidencias fueron examinadas, cuándo, de dónde y cuándo se obtuvieron las pruebas.
- **Resumen de proceso:** Qué herramientas fueron utilizadas, qué datos fueron recuperados.
- **Examen de las evidencias**: Archivos de logs, tráficos de red o archivos.
- **Análisis**: Descripción del o los análisis realizados.
- **Conclusiones:** Resumen que se enlace lógicamente y se refiera a todas las evidencias recolectadas.
- **Glosario de términos:** Explicación de los términos técnicos utilizados.
- **Apéndices**: Relación de la evidencia encontrada de manera numerada y ordenada.
- **Cierre:** Esta última fase lo que busca es que en el lugar donde se revisó la información siga todos los protocolos definidos en cada una de las fases del análisis, de igual manera y siempre que sea posible se busca devolver las evidencias a sus respectivos dueños.

## CONCLUSIONES

1. La criminalidad informática utiliza sus recursos económicos en la comisión de delitos informáticos porque han encontrado en las nuevas tecnologías una forma de obstaculizar su persecución, y además son realizados en diferentes lugares sin estar presentes físicamente

2. A nivel internacional existe una gran preocupación por la comisión de los delitos informáticos, y esto ha derivado en una serie de reformas a las legislaciones de todo el mundo, celebrando Convenios Internacionales de colaboración con el objeto de unificar las legislaciones y perseguir de mejor manera estos ilícitos que se desarrollan tan rápido como la tecnología.

3. La legislación guatemalteca, no está actualizada en materia de delitos informáticos, y las conductas delictivas que prohíbe ya no se apegan a la realidad actual quedando muchas más conductas ilícitas impunes por su falta de regulación legal.

4. Los delitos informáticos se manifiestan en todas las esferas sociales a nivel nacional e internacional, pueden vulnerar bienes jurídicos tutelados de toda clase principalmente la intimidad y el patrimonio de las personas tanto individuales como jurídicas.

5. En Guatemala existe una serie de obstáculos para la persecución penal de los delitos informáticos y esto principalmente a la falta de capacitación del Ministerio Publico, de la Policía Nacional Civil y el Instituto Nacional de Ciencias Forenses que no cuentan con el personal con la preparación necesaria.

## RECOMENDACIONES

1. Es indispensable que el gobierno de Guatemala, reconozca la existencia de la criminalidad informática, cree una política criminal que identifique el perfil de los sujetos activos responsables de la comisión de los delitos informáticos, así como identificar a los sujetos pasivos más vulnerables.

2. El Estado de Guatemala, debe de celebrar o bien adherirse a los Convenios Internacionales celebrados en cuanto a la criminalidad informática, para poder unificar los criterios y las normas legales que regulan los delitos informáticos, así poder identificar a estas agrupaciones criminales internacionales,.

3. El Congreso de la República de Guatemala, a través de su función legislativa se encargue de actualizar la legislación penal en cuanto a los delitos informáticos, que conozca y apruebe la iniciativa de ley número 4055 del año 2009, ya que la misma se ajusta de mejor manera a la actualidad nacional e internacional en esta materia.

4. Es importante que tanto el Ministerio Público, como ente encargado de la persecución e investigación penal, el Instituto Nacional de Ciencias Forenses y la Policía Nacional Civil, como institución auxiliar de la investigación, capaciten a su personal en materia de informática forense, para la investigación de los delitos informáticos

5. El Organismo Judicial como órgano encargado de la administración de justicia capacite a los jueces, en esta ciencia forense, para conocer y valorar de manera objetiva e imparcial la evidencia digital que se presenta en los procesos penales.

## BIBLIOGRAFÍA


BARRIOS OSORIO, Omar Ricardo. **Derecho e Informática, aspectos fundamentales.** Ediciones Mayte, 3º edición, Guatemala, 2,006.

CALDERÓN RODRÍGUEZ, Cristian, **El impacto de la era digital en el derecho**. http://www.vlex.com/redi/ (visitada 7 de julio de 2,011)

CAMACHO LASA, Luis. **El delito informático**. Madrid, España,1,990

CANO, Jeimy. **Estado del arte de peritaje informático en Latinoamérica**. http:/www.alfa-redy.org. (visitada 15 de junio de 2,011)

DAVARA RODRÍGUEZ, Miguel Ángel. **Análisis de la ley de fraude informático**. Revista de Derecho de UNAM. México,1,990.

DEL PINO, Santiago Acurio. **Delitos informáticos, generalidades.** PUCE. Ecuador, octubre 2,007.

DEL PINO, Santiago Acurio. **Informática forense en el Ecuador** Fiscalia General del Estado de Ecuador, diciembre 2,009.

**Enciclopedia CCI, criminalística, criminología e investigación**. Tomo III, investigación, investigación policial, procedimientos y técnicas científicas. Sigma Editores. Colombia, 2,009.

GUTIERRÉZ FRANCÉS, María Luz. **Fraude informático y estafa**. Ministerio de Justicia. España, 1,991.

GUIBOURG Ricardo A., ALENDE Jorge O., CAMPANELLA Elena M**.. Manual de informática jurídica**. Editorial Astrea. Buenos Aires, Argentina, 1,996.

HEINRICH, Jescheck Hans. **Tratado de derecho penal, parte general**. Traducción y adiciones de derecho penal español por Santiago Mir Puig y Francisco Muñoz Conde. Volumen primero. Editorial Bosch. Barcelona, España, 1,981.

http://www.eff.org/pub/publications/**Jhon_perry_barlow/barlow**_0296 (consulta 06 de junio 2,010)

http://www.alfa-redi.org/**rdi-articulo**.shtml?x=207 (visitada el 23 de junio de 2,011)

http://www.monografias.com/trabajos12/**conygen**/conygen.shtml (visitada el 23 de junio de 2,011)

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/**Convenio_Ciberdelincuencia**.pdf, (visitada el 10 de abril de 2,011)

http://www.uncjin.org/Documents/**congr10**/10s.pdf, (visitada el 15 de junio de 2,011)

HUERTA, Marcelo y LIBANO, Claudio. **Delitos informáticos**. Editorial Jurídica Cono Sur. Chile 2,007.

LÓPEZ DELGADO, Miguel. **Análisis forense digital**. CRIPORED, junio 2,007,

MAGLIONA MARKOVICTH, Claudio Paúl, LÓPEZ MEDEL, Macarena, **Delincuencia y fraude informático**. Editorial Jurídica de Chile, 1,999.

MANSON, Marcelo. **Legislación sobre delitos informáticos** http://monografias.com/trabajos/**legisdelinf**/legisdelinf.shtml, (consulta el 23 de mayo de 2,011)

PALAZZI, Pablo A. **Delitos informáticos**. Editorial, AD-HOC. Buenos Aires, Argentina, 2,000.

RESA NESTARES, Carlos. **Crimen organizado transnacional: definición, causas y consecuencias**. Editorial Astrea. Colombia, 2,005.

REYES ECHANDIA, Alfonso. **La tipicidad**. Universidad de Externado de Colombia, 1,981.

REYES, Anthony. **Investigación del cibercrimen**, Syngress, 2,007

ROMEO CASABONA, Carlos María. **Poder informático y seguridad jurídica**. Fundesco. Madrid, España, 1,987.

TIEDEMANN, Klaus. **Poder informático y delito**. Barcelona, España,1,985.

VALDÉS TÉLLEZ, Julio. **Derecho informático**. 4ª edición Mc Graw-Hill. México D.F.; 2,004.

**Legislación:**

**Constitución Política de la República de Guatemala**. Asamblea Nacional Constituyente, 1,986.

**Código Penal**, Decreto número 17-73, del Congreso de la República de Guatemala, 1,973.

**Código Procesal Penal**, Decreto número 51-92, del Congreso de la República de Guatemala, 1,992.

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

**Resolución 11-2010, de la Dirección Normativa de Contrataciones y Adquisiciones del Estado**, 2,010.

**Acta Federal de abuso computacional**, Estados Unidos de Norteamérica, 1,994.

**Código Penal Federal**, México, 1,931..

**Ley 26.388 Ley de Delitos Informáticos**, Argentina, 2,008.

**Ley 1273,** del Congreso de la República de Colombia, 2,009.

**Ley Orgánica 10/1995,** España, 1,995.

**Ley Federal de Derechos de Autor**, México, 2,003.

**Ley Especial contra Delitos Informáticos**, Venezuela, 2,001.

**Convención de Roma**, 26 de octubre de 1961, Italia.

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

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