

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

**EL VALOR PROBATORIO DE LOS SOPORTES INFORMÁTICOS EN EL DELITO DE
FRAUDE ELECTRÓNICO**

MARÍA JOSÉ ROBLEDO RAMIREZ

GUATEMALA, NOVIEMBRE DE 2019

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

**EL VALOR PROBATORIO DE LOS SOPORTES INFORMÁTICOS EN EL DELITO DE
FRAUDE ELECTRÓNICO**

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

MARÍAJOSÉ ROBLEDO RAMIREZ

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

Y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, noviembre de 2019

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

DECANO:	Lic.	Gustavo Bonilla
VOCAL I:	Lic.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Henry Manuel Arriaga Contreras
VOCAL III:	Lic.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Denis Ernesto Velásquez González
VOCAL V:	Br.	Abidán Carías Palencia
SECRETARIO:	Lic.	Fernando Antonio Chacón Urizar

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente:	Lic.	Erick Rolando Huitz Enrique
Vocal:	Lic.	Edwin Orlando Xitumul Hernández
Secretario:	Lic.	William Armando Vanegas Urbina

Segunda Fase:

Presidente:	Lic.	José Alfredo Pinto Sequén
Vocal:	Lic.	Evelyn Johana Chévez Juárez
Secretario:	Lic.	Horacio Joel Avendaño Madrid

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 la Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).



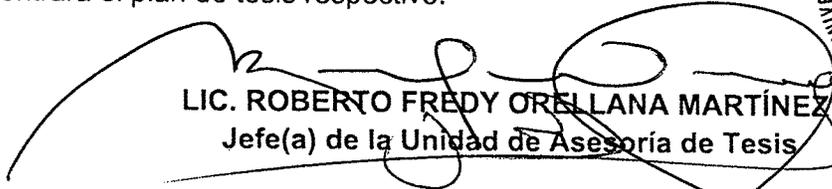
Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala,
 23 de septiembre de 2019.

Atentamente pase al (a) Profesional, WALTER ESTUARDO GARCIA TELLO
 _____, para que proceda a asesorar el trabajo de tesis del (a) estudiante
MARIAJOSÉ ROBLEDO RAMÍREZ, con carné 201211101,
 intitulado EL VALOR PROBATORIO DE LOS SOPORTES INFORMÁTICOS EN EL DELITO DE FRAUDE
ELECTRÓNICO.

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

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

Adjunto encontrará el plan de tesis respectivo.


LIC. ROBERTO FREDY ORELLANA MARTÍNEZ
 Jefe(a) de la Unidad de Asesoría de Tesis



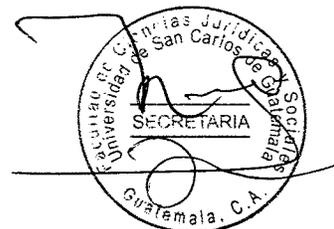
Fecha de recepción 24 / 09 / 2019. f)

Asesor(a)
 (Firma y Sello)
LICENCIADO
Walter Estuardo García Tello
 ABOGADO Y NOTARIO



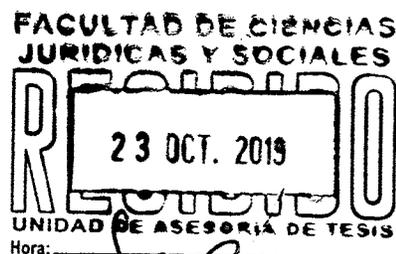


Lic. WALTER ESTUARDO GARCIA TELLO



Guatemala 15 de octubre de 2019

Lic. Roberto Fredy Orellana Martínez
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala



Distinguido Licenciado Fredy Orellana Martínez:

De conformidad con lo señalado según nombramiento de fecha 23 de septiembre de 2019, se me nombró Asesor de la bachiller Mariajosé Robledo Ramirez de su tesis que se intitula: **“EL VALOR PROBATORIO DE LOS SOPORTES INFORMÁTICOS EN EL DELITO DE FRAUDE ELECTRÓNICO”**. Para el efecto hago de su conocimiento:

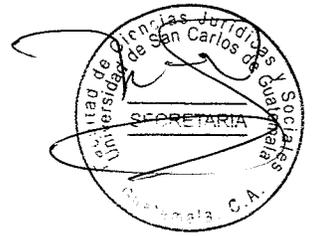
- a) **Del contenido científico y técnico de la tesis:** El trabajo de tesis desarrollado, de conformidad con el plan de investigación, muestra una amplia y exhaustiva explicación científica fundamentada en una recolección de datos referentes al tema, los cuales fueron obtenidos de forma minuciosa a través de la recopilación normativa de los instrumentos e instructivos aplicables y exigidos.
- b) **De las referencias bibliográficas:** El trabajo de tesis cuenta con suficientes referencias bibliográficas, con lo que se resguarda el derecho de autor y se enriquece la investigación realizada por parte del sustentante.
- c) **De la metodología y técnicas de investigación utilizadas:** Al llevar a cabo la elaboración de la tesis fue necesario el empleo de los métodos analítico e inductivo y la técnica de investigación bibliográfica y documental, para la obtención de conocimientos básicos relacionados con el tema investigado y para llegar a la conclusión discursiva.
- d) **De la redacción capitular:** La redacción de los capítulos tiene un contenido acorde a la realidad. La misma es de útil consulta para la sociedad guatemalteca y señala claramente los objetivos trazados.
- e) **De la conclusión discursiva y bibliografía utilizada:** la conclusión discursiva desarrolla con claridad que es esencial garantizar la veracidad de la evidencia digital durante el proceso de investigación, y para ello es indispensable contar con los conocimientos y habilidades especiales en la recaudación, embalaje y manipulación de este tipo de evidencia.

8av 3-35 Colonia Rivera del Río, zona 13 San Miguel Petapa.

Tel: 3020 0781



Lic. WALTER ESTUARDO GARCIA TELLO



- f) **Del parentesco:** Se hace la aclaración que entre la bachiller y el asesor no existe parentesco alguno dentro de los grados de ley.

Doy a conocer que el trabajo de tesis de la sustentante cumple de manera eficaz con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, por lo que extendiendo **DICTAMEN FAVORABLE** para que pueda continuar con el trámite respectivo, para evaluarse posteriormente por el Tribunal Examinador en el Examen Público de Tesis, previo a optar al grado académico de Licenciada en Ciencias Jurídicas y Sociales.

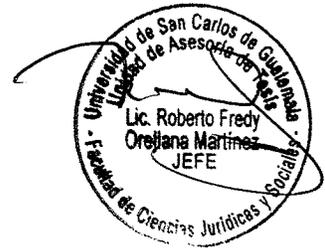
Atentamente.

LIC. WALTER ESTUARDO GARCIA TELLO
ASESOR DE TESIS
COLEGIADO 10730

LICENCIADO
Walter Estuardo García Tello
ABOGADO Y NOTARIO

8av 3-35 Colonia Rivera del Río, zona 13 San Miguel Petapa.

Tel: 3020 0781



DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 07 de noviembre de 2019.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante MARIAJOSÉ ROBLEDO RAMÍREZ, titulado EL VALOR PROBATORIO DE LOS SOPORTES INFORMÁTICOS EN EL DELITO DE FRAUDE ELECTRÓNICO. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

RFOM/JP.





DEDICATORIA

A DIOS:

Por ser lámpara a mis pies y lumbrera a mi camino. Por permitirme culminar esta etapa tan importante en mi vida. Hasta aquí puedo decir que su misericordia me alcanzó.

A MI MADRE:

Arely Ramírez por enseñarme con tu ejemplo que el pilar más importante en mi vida debe ser Dios. Porque tu valentía fue mi motivación para alcanzar tan anhelada meta, gracias por tus oraciones, a través de ellas hoy veo culminada mi carrera universitaria.

A MI PADRE:

José Robledo, por ser ejemplo de superación académica y profesional, por esforzarte cada día por darnos lo mejor.

Gracias a ambos por inculcarme principios, el valor de servicio y enseñarme que en la vida hay que soñar en grande y perseverar para alcanzar nuestras metas. Gracias porque han llenado mi vida de alegría y amor cuando más lo he necesitado. Espero enorgullecerlos el día de hoy. Los amo.

A MIS HERMANAS:

Marialejandra y Mariaceleste, Por ser mis primeras amigas en la vida. Espero este logro sea un ejemplo en sus vidas; que Dios permita que lleguen mucho más lejos que yo. Gracias por creer en mí, por su apoyo incondicional. Recuerden, siempre juntas en todo momento. Las amo.



A MIS AMIGOS:

Que durante toda mi vida han estado conmigo, los que conocí en la universidad y los que gracias a Dios ha puesto en mi camino, agradecerles por brindarme su amistad, esperando seguir contando con cada uno de ustedes.

A: Mis amigas Shandy, Isabel, Claudia, Lesly, Josselyn y Zorel, porque nuestra amistad supero los salones de clase, convirtiéndose en mis hermanas por elección.

A: Mis amigos y futuros colegas: Lily, Tephi, Gaby Rosales, Carlos Pimentel y Byron Morales por acompañarme a lo largo de la carrera compartiendo conmigo momentos únicos, felices y difíciles en la facultad, haciendo de ella una maravillosa experiencia.

A: Lic. Walter García Tello, por su valioso apoyo como asesor, brindando sugerencias oportunas para el enriquecimiento de la elaboración de mi tesis.

A: La Universidad de San Carlos de Guatemala. Por ser mi Alma Mater, por darme el honor de ser egresada de la grande entre las grandes y permitirme ser, orgullosamente San Carlista.

A: La Facultad de Ciencias Jurídicas y Sociales, por ser parte de mi formación profesional, así como brindarme los mejores momentos al lado de los mejores compañeros.

A: Usted que me acompaña en este acto.



PRESENTACIÓN

El trabajo de tesis desarrollado se enmarca dentro de las investigaciones cualitativas, se investigó las causas de los incidentes informáticos, derivado de la insuficiencia de preceptos legales, que permiten perseguir y sancionar a los sujetos.

Este informe corresponde al derecho público, específicamente a la rama del derecho penal.

Los sujetos en estudio, en los casos de los delitos informáticos pueden ser individuos particulares o sociedades que utilizan sistemas automatizados de información para infringir lo que la ley establece. El objeto de estudio de la tesis fue determinar la necesidad que las normas que establece el Código Penal, decreto número 17-73 del Congreso de la República, sean reevaluadas e incorporadas a una ley especial contra los delitos informáticos.

El aporte académico es lograr establecer la importancia del valor probatorio de los soportes informáticos en el delito de fraude electrónico que en principio son similares a los demás delitos comunes, pero que, en su forma novedosa de acción, resultan extrañas para los legisladores y los órganos de administración de Justicia y que las mismas sean tomadas en cuenta para futuras contribuciones a reformas del Código Penal Guatemalteco, en virtud de que únicamente el Artículo 274 del mismo cuerpo legal, regula lo referente a los delitos informáticos.



HIPÓTESIS

Se debe tomar con valor probatorio admisible el análisis del dictamen del forense de los sistemas tecnológicos, dentro de los procesos judiciales y para su íntegra aplicación en los procesos penales en el ámbito jurídico guatemalteco.



COMPROBACIÓN DE LA HIPÓTESIS

Para comprobar la hipótesis, se emplearon los métodos de investigación deductivo e inductivo. Los cuales fueron utilizados para para establecer los antecedentes que se tienen sobre la informática jurídica para determinar la comisión del delito de fraude electrónico incorporando el valor probatorio de los soportes informáticos.

Se logró validar la hipótesis planteada, evidenciándose que es necesario que en la legislación guatemalteca se incorpore el valor probatorio de los soportes informáticos en el delito de fraude electrónico.



ÍNDICE

	Pág.
Introducción	i

CAPÍTULO I

1. Valor probatorio.....	1
1.1. La prueba en general	3
1.2. Definición de prueba penal.....	3
1.3. Derecho probatorio.....	4
1.4. Principios de la actividad probatoria.....	5
1.5. Objeto de la prueba.....	9
1.6. Medios de prueba.....	9
1.7. Indicios de la prueba penal	10
1.8. Órganos de la prueba.....	11

CAPÍTULO II

2. Soportes informáticos.....	13
2.1. Los bienes informáticos.....	15
2.2. Base de datos	15
2.3. El ordenador y la computadora	17
2.3.1. Primeros ordenadores	18
2.3.2. Ordenadores electrónicos.....	18
2.3.3. Circuitos integrados	19
2.3.4. Microminiaturización.....	20
2.3.5. Desarrollo de computadoras.....	21
2.3.6. Computadoras	22
2.3.7. Las computadoras en la oficina	24
2.3.8. Beneficios y efectos de la computadora	25
2.4. La red de información internet.....	26
2.4.1. La historia de vida de internet.....	27



	Pág.
2.4.2. Servicios varios de internet.....	28
2.4.3. Módems y formas de conexión a internet.....	30
2.4.4. Protocolos de comunicación.....	31
2.5. El documento electrónico.....	32
2.5.1. Características.....	33
2.5.2. Clases.....	36
2.6. Firma electrónica.....	36
2.7. Elementos que componen un documento electrónico.....	37
2.8. Leyes vigentes que contemplan la utilización de medios computarizados.....	37

CAPÍTULO III

3. Bien jurídico tutelado en los delitos informáticos.....	41
3.1. Los bienes jurídicos protegidos en el delito informático.....	43
3.2. Definición y el concepto de delitos informáticos.....	45
3.3. Sujetos del delito informático.....	45
3.3.1. Sujeto activo.....	46
3.3.2. Sujeto pasivo.....	47
3.4. Tipos de delitos informáticos.....	48
3.4.1. Los fraudes.....	49
3.4.2. El sabotaje informático.....	50
3.4.3. El espionaje informático y el robo o hurto de software.....	51
3.4.4. El robo de servicios.....	52
3.4.5. El acceso no autorizado a servicios informáticos.....	53

CAPÍTULO IV

4. El valor probatorio de los soportes informáticos en el delito de fraude electrónico.....	55
4.1. Hechos jurídicos informáticos como medios probatorios convencionales.....	58



4.2. Problemática actual de la prueba electrónica.....	Página 60
4.3. Régimen jurídico de la prueba electrónica	63
4.4. Recolección y valoración de la prueba electrónica	69
CONCLUSIÓN DISCURSIVA	73
BIBLIOGRAFÍA	75



INTRODUCCIÓN

El problema a investigar es sobre el delito de fraude informático incorporando el valor probatorio de los soportes informáticos; la evidencia digital es una de las figuras de la investigación criminal que en la actualidad ha planteado nuevos retos a las instituciones encargadas de la averiguación de la verdad, conjuntamente con esta se establece la cadena de custodia digital que supone nuevos retos para la identificación, recolección, preservación y resguardo de los indicios o evidencias digitales que se generan en distintos dispositivos de tecnología.

Considerar el manejo de la cadena de custodia en la recolección de evidencia digital en Guatemala resulta importante para las nuevas formas de investigación, al contemplar la influencia de la tecnología en la mayoría de los procesos que realiza la persona en su vida cotidiana esto mismo genera causalmente una fuente de evidencia digital en la comisión de hechos delictivos.

La tecnología avanza a pasos agigantados, superando lo que los legisladores puedan prever. La tarea de los jueces se ha tornado muy valiosa, pues son ellos los que, a falta de legislación, han brindado soluciones justas a problemas sin precedentes. Mucho se ha escrito en materia de banca electrónica en los últimos años.

Entre las causas de análisis se cita que, la tecnología en el uso adquiere una especificidad en su aplicación al ámbito forense. Especificidad que la hace contribuyente de aportes únicos e irrepetibles en la investigación de hechos criminales de diversa naturaleza, y a su vez, permite la interrelación transdisciplinaria con las demás profesiones que desarrollan actividades periciales en auxilio de los magistrados, funcionarios judiciales, letrados y la sociedad en general.

La aplicación de técnicas de vanguardia, para la realización de peritajes tecnológicos especializados como consecuencia aportar logros y avances al campo investigativo a las instituciones encargadas de la persecución penal en Guatemala.



Este estudio contiene cuatro capítulos, el capítulo I, se refiere al valor probatorio, el capítulo II, se enfoca en los soportes informáticos; el capítulo III, se describe el bien jurídico tutelado en los delitos informáticos; y, por último, el capítulo IV se enfoca al valor probatorio de los soportes informáticos en el delito de fraude electrónico.

Con este documento se pretende realizar un aporte, en el cual la protección conociendo la peligrosidad de los fraudes informáticos, su forma de operar, los bienes jurídicamente protegidos que se encuentran vulnerables, la falta de normas para perseguir, procesar y sancionar a los delincuentes en materia informática, se hace sumamente necesario que el Estado, creen una ley especial contra los fraudes informáticos, a efecto de garantizar los derechos de los guatemaltecos, previniendo a los autores de los fraudes informáticos abstenerse de continuar vulnerando dichos derechos.



CAPÍTULO I

1. Valor probatorio

La prueba es una verificación de afirmaciones que se lleva a cabo utilizando los elementos de prueba que disponen las partes y que se incorporan al proceso a través de los medios de prueba permitidos legalmente y con arreglo a ciertas garantías.

La expresión de la prueba tiene varias significaciones; en un sentido muy amplio se podría decir que prueba es todo medio que sirve para investigar y demostrar cualquier hecho. Sin embargo, en sentido más restringido, desde el punto de vista jurídico pero que sigue siendo amplio, se puede indicar que prueba es el conjunto de motivos y razones que suministra certeza en el proceso.

La prueba puede ser definida en términos simples como: “Un medio de verificación de las proposiciones de hecho que los litigantes formulan en el juicio”¹, así como también se puede decir que la prueba es una confirmación de las aseveraciones llevadas a cabo por medio de elementos o fuentes probatorias de las cuales disponen los involucrados y que son incorporados al proceso por medio de dichos elementos y con arreglo a ciertas garantías.

“Conjunto de actuaciones que dentro de un juicio, cualquiera que sea su índole, se encaminan a demostrar la verdad o la falsedad de los hechos aducidos por cada una de las partes, en defensa de sus respectivas pretensiones litigiosas. Las pruebas generalmente admitidas en las legislaciones son las de indicios (v.), la presunción (v.) y especies, la confesión en juicio (v.), la de informes (v. prueba de informes); la instrumental, llamada también documental (v. instrumentos, prueba instrumental); la testimonial (v. declaración, prueba testifical o testimonial), la pericial (v. perito, prueba pericial.)

¹Hernández Villareal, Gabriel. **Actualidad y futuro del derecho procesal: Principios, reglas, y pruebas.** Pág. 170.



Algunas legislaciones determinan el valor de ciertas pruebas, al cual se tiene que atender el juzgador, pero lo más corriente y lo más aceptable es que la valoración de las pruebas sea efectuada por el juez con arreglo a su libre apreciación.

A más del significado procesal anterior, el de mayor relieve jurídico, prueba es toda razón o argumento para demostrar la verdad o la falsedad en cualquier esfera y asunto. | Ensayo o experiencia. | Parte minúscula que se gusta de un producto, o que se examina, para verificar si agrada o si presenta las cualidades apetecidas por el eventual adquirente.

En los procedimientos, son objeto de prueba los hechos controvertidos, y solamente los hechos. Por excepción, que se interpretan de maneras distintas, los tribunales exigen a veces que se pruebe la costumbre, no obstante ser fuente jurídica, y el Derecho extranjero aplicable a su caso; ambos, en cuanto a su vigencia.²

La prueba es una actividad procesal dirigida a alcanzar la certeza judicial de ciertos elementos para decidir un litigio sometido a proceso. Una cosa es la prueba y otra el hecho conocido.

A medida que el juez tenga conocimiento de los elementos probatorios irá formando su criterio hasta quedar convencido de la existencia del delito y la responsabilidad del autor. Para que el juzgador declare la existencia de responsabilidad penal e imponga la sanción correspondiente al autor de un hecho punible, es preciso que adquiera la certeza de la comisión y la vinculación al acusado.

Es decir que el juzgador debe de adoptar tal criterio con base al convencimiento generado por la certeza proporcionada tras la valoración de los medios probatorios aportados por los órganos de prueba. Por lo que la prueba es el medio a través del cual se llega al conocimiento de los hechos históricos que interesan en el proceso.

² Ossorio, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales.** Pág. 817.



1.1. La prueba en general

Esta se puede indicar que, en su más amplio sentido, se refiere a un hecho verídico que como un supuesto es utilizado para fundamentar un motivo que se deriva en otro hecho. En cualquier caso la prueba es un el cual busca alcanzar un fin. A través de las pruebas se pueden demostrar teorías científicas y así determinar los hechos.

1.2. Definición de prueba penal

Esta es la forma en la cual se puede confiar de una forma fidedigna para alcanzar el fin de descubrir la realidad, es el mayor garante contra la injusticia de los fallos judiciales. Por lo tanto, las pruebas deben de ser objetivas, para poder ser demostrados las circunstancias o hechos en litigio para que las resoluciones judiciales se basen en pruebas que demuestren la culpabilidad o inocencia del imputado.

“El conjunto de actuaciones que dentro de un juicio, cualquiera que sea su índole, se encaminan a demostrar la verdad o la falsedad de los hechos aducidos por cada una de las partes, en defensa de sus respectivas pretensiones litigiosas.”³

Las tres definiciones de los doctrinarios concluyen que la prueba busca demostrar la verdad sobre hechos ilícitos penales, por lo que conducen a entender que la prueba es un medio por el cual el señor juez, resuelve un ilícito penal, demostrando que los medios proporcionados son los elementos positivos de la prueba que le serán útiles al dictarse una sentencia apegada a la ley, ya sea condenatoria o absolutoria.

Sin la prueba no se puede impartir justicia, y ésta debe de ser lo más objetiva posible, lo cual es imprescindible para que la misma sea apegada al derecho que tiene el imputado, teniendo el juez, esa oportunidad para darle la valoración en su oportunidad y así enmarcarse dentro el debido proceso, otorgando al sindicado el principio de

³ **Ibid.** Pág. 625.



inocencia en los Artículos 14 del Código Procesal Penal y 14 de la Constitución Política de la Republica.

1.3. Derecho probatorio

“En Guatemala el Código Procesal Penal vigente, inspirado en el Código tipo para Latinoamérica, según el licenciado Hugo Roberto Jáuregui, recoge todas las características de un proceso acusatorio formal, en especial en lo que a la prueba se refiere, el imputado deja de ser un medio de prueba para ser sujeto procesal, quien tiene la facultad de no probar su inocencia (Principio *Onus Probandi*), declarar, proponer, fiscalizar y contradecir la prueba, y en los casos de duda en la aplicación de una ley debe de preferirse en todo caso una interpretación favorable al reo o al procesado (Principio *favor rei*.)

Pudiendo además otorgársele medidas que aseguren su presencia en el proceso (principio de *favor libertatis*), buscando con ello proteger su dignidad humana, valor protegido a través de la presunción de inocencia.”⁴

Tal como lo establecen tanto la Constitución Política de Guatemala en su artículo número catorce, en relación con el derecho de defensa que tiene toda persona, los cuales son inviolables, por lo que ninguna persona puede ser condenada y menoscabada sus derechos, que tiene toda persona que se encuentre dentro del territorio nacional dentro de un proceso; sin que se le haya citado, oído y vencido en proceso legal ante juez o tribunal preestablecido y ante todo competente.

Asimismo, en el Código Procesal de Guatemala, preceptúa que toda persona a quien se le inicia un proceso debe considerársele como inocente durante todo el procedimiento.

⁴ Domínguez, Mario. **Temas de derecho probatorio penal.** Pág. 32.



1.4. Principios de la actividad probatoria

En Guatemala, el derecho probatorio se desarrolla conforme a normas jurídicas que regulan, y que en su conjunto constituyen el llamado derecho probatorio en el cual se concretan basado en principios.

- a) En Guatemala le corresponde al Ministerio Público, pues en su ejercicio de la acción penal, así se lo permite, ya que es el órgano auxiliar de la administración de justicia, también tiene a su cargo el procedimiento preparatorio, como se establece en el Artículo 107 del Código Procesal Penal guatemalteco; con relación al siguiente principio se puede establecer que, en lo que respecta al proceso penal se da la necesidad de lealtad procesal, puesto que existen sanciones penales tales como el delito de calumnia, falso testimonio, encubrimiento, simulación de delito, así como otras sanciones disciplinarias de distinta naturaleza, el principio de necesidad va íntimamente ligado con el principio de legitimidad de las fuentes de la prueba, por lo que todos aquellos elementos probatorios que no llenen el requisito de certeza, deben ser excluidos y calificados como fuentes impuras de prueba.
- b) Tomando en cuenta el Artículo 108 del Código Procesal Penal guatemalteco, el Ministerio Público es quién debe formular los requerimientos y solicitudes conforme al criterio de necesidad, aún a favor del imputado, el principio de objetividad establece que mediante la aplicación de la ley debe averiguarse la verdad en la comisión de un hecho delictivo a través de los órganos de justicia, encargados de establecer la verdad mediante los medios de prueba permitidos legalmente y el principio de libertad probatoria indica que todos los hechos y circunstancias de interés para la correcta solución de un caso puede ser objeto de prueba, salvo las limitaciones a que se refiere el estado civil de las personas.
- c) El Código Procesal Penal en el Artículo 290; relaciona la actuación del Ministerio Público debe de estar apegado a la ley, pues su función principal es la aplicación de la ley penal, procurando aclarar el hecho y la situación del procesado, claro está que



la prueba va a servir para acusar y también para descargar la culpabilidad del sindicado de un hecho delictivo. En materia penal, todo hecho, circunstancia o elemento, contenido en el objeto del procedimiento y, por tanto, importante para la decisión final, puede ser probado y a través de cualquier medio de prueba permitido por la legislación.

Relacionando lo anterior en el Artículo 182 del Código Procesal Penal guatemalteco, señala que se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso por los medios de prueba permitido por la ley, en los Artículos 181,182,183 Código Procesal Penal por ejemplo la prueba científica de ADN, esto es permitido.

d) Aplicando el principio procesal de preclusión, vencida esta etapa procesal, no se pueden aportar nuevos medios de prueba. Salvo excepciones que establece la ley, como por ejemplo cuando puede ampliarse o modificarse la demanda antes que haya sido contestada por el demandado. En tal sentido el Artículo 504, 454 del Código Procesal Penal guatemalteco, que al ser modificada o dejar sin efecto la pena impuesta, o las condiciones de su cumplimiento, el Juez de ejecución promoverá la revisión de la sentencia ejecutoriada, a través de la Corte Suprema de Justicia.

Lo que demuestra que la preclusión no opera cuando favorece al condenado, no así para el ente acusador.

El Ministerio Público solo tiene una oportunidad para demostrar la culpabilidad de una persona, mientras que el sindicado tiene dos, porque, aunque haya sido sentenciado y este en una cárcel cumpliendo su pena, él puede demostrar su inocencia aportando medios de prueba para ello, esto es lo que explica este principio.



- e) Principio de idoneidad de la prueba, puede decirse que éste representa una limitación al principio de la libertad de la prueba, pero es igualmente necesario, pues significa que el tiempo y el trabajo de los funcionarios judiciales y de las partes en esta etapa del proceso no debe perderse en la recepción de medios que por sí mismos o por su contenido no sirvan en absoluto para los fines propuestos y aparezcan claramente improcedentes o inidóneos. De esa manera, se contribuye a la concentración y a la eficacia procesal de la prueba.
- f) Principio de originalidad de la prueba, este principio significa que la prueba en lo posible debe referirse directamente al hecho por probar, para que sea prueba de éste, pues si apenas se refiere a hechos que a su vez se relacionan con aquél, se tratará de pruebas de otras pruebas.

No se puede aportar pruebas que sean distintas del hecho que se desea probar, pues éstas deben referirse directamente para la averiguación y descubrimiento de la verdad, en el proceso no sirve que se aporten mil pruebas que lo único que forman es hacer abundante el expediente, es mejor aportar las que si van a servir al proceso y le ayudaran al juez para dictar la sentencia.

- g) Principio de eficacia o utilidad jurídica de la prueba, este principio complementa al principio de la necesidad de la prueba y de la prohibición de aplicar el conocimiento privado del juez sobre los hechos. Si la prueba es necesaria para el proceso, debe tener eficacia jurídica para llevarle al juez el convencimiento o la certeza sobre los hechos que sirven de presupuesto a las normas aplicables al litigio, o a la pretensión voluntaria, o a la culpabilidad penal investigada.

No se concibe la institución de la prueba judicial sin esa eficacia jurídica reconocida por la ley, cualquiera que sea el sistema de valoración y de aportación de los medios al proceso, pues este principio no significa que se regule su grado de persuasión, sino que el juez, libre o vinculado por la norma, debe considerar la



prueba como el medio aceptado por el legislador, para llegar a una conclusión sobre la existencia y las modalidades de los hechos afirmados o investigados.

- h) Principio de contradicción de la prueba, al proceso no pueden ingresarse pruebas en forma subrepticia de la contraparte. Todo se resume a que la parte contra quien se produce una prueba debe gozar de la oportunidad procesal para conocerla, discutirla, es decir, la prueba debe llevarse a la causa con conocimiento de las partes en la audiencia.
- i) Principio de igualdad de oportunidad de la prueba, se relaciona íntimamente con el principio de la contradicción de la prueba, pero no se identifica con él. Para que haya esa igualdad es indispensable la contradicción, con todo, este principio significa algo más: que las partes dispongan de idénticas oportunidades para presentar o pedir la práctica de pruebas y para contradecir las aducidas por el contrario. Es un aspecto del otro principio más general de la igualdad de las partes ante la ley procesal.
- j) Principio de comunidad o adquisición de la prueba, una vez incorporada la prueba al proceso, con el cumplimiento de requisitos legales, ya la prueba pertenece al proceso, no a quien aporto esa prueba, a quien la solicitó, por tal manera, que una vez incorporada al proceso sirve de manera indistinta a las partes, y una vez ingresada, pierde oportunidad de ser retirada del mismo, haciendo parte del universo probatorio.

Y por idéntica razón el conocimiento del juez no puede llenar vacíos probatorios, ni sustituir medios de prueba, la prueba pertenece al proceso no a la parte que la solicitó o participó en la prueba. El Artículo 350 del Código Procesal Penal, estipula el principio de comunidad de prueba. Debe de entenderse que toda prueba aportada por las partes dentro del proceso penal es patrimonio del proceso, es decir que la prueba debe de servir tanto para la parte acusadora como a la parte acusada.



1.5. Objeto de la prueba

“Es aquello susceptible de ser probado, sobre lo que debe o puede recaer la prueba. Siempre se examinará primero en un proceso penal lo que puede ser probado. También se considerará qué es lo que se debe probar en un proceso determinado.”⁵

La prueba puede recaer sobre la existencia de hechos y circunstancias humanas; la prueba puede recaer sobre hechos naturales o humanos, físicos o psíquicos y sobre la existencia y cualidades de las personas, cosas y lugares. Pero los hechos notorios y los evidentes no serán objeto de prueba, salvo que sean controvertidos razonablemente.

La prueba deberá versar sobre la existencia del hecho delictuoso y las circunstancias que lo califiquen, lo agraven, atenúen, justifiquen, o influyan en la punibilidad y la extensión del daño causado en un proceso penal determinado.

La materialidad de la prueba es fundamental en el proceso porque aviva los sentidos del juzgador, por ejemplo, un video donde el sindicado está golpeando en forma inhumana a un niño de diez años, luego introduce aparatos sexuales y lo termina violando, este video ésta probando un hecho delictuoso como lo es la violación sexual o sea que si cumple con el objeto de la prueba y sirve en el proceso en forma conjunto con las demás pruebas al momento de dictar sentencia.

1.6. Medios de prueba

“Llámense así las actuaciones que, dentro de un procedimiento judicial, cualquiera que sea su índole. Se encaminan a confirmar la verdad o a demostrar la falsedad de los hechos aducidos en el juicio. / En materia penal son también las actuaciones que en el sumario o en el plenario tratan de investigar la culpabilidad o la inocencia del inculpado.

⁵ Oviedo Silva. **La injusticia de la justicia**. página 119.



Los medios corrientes de prueba son: la documental, (también llamada instrumental), la de informes, la confesión en juicio, la testimonial, la pericial, el reconocimiento judicial (llamada inspección ocular), el careo y las presunciones o indicios.”⁶

Normalmente el valor de las pruebas va de acuerdo con arreglo a la libre apreciación del juez o tribunal.

Estos son procedimientos formales para la incorporación de elementos probatorios dentro del proceso, dicha incorporación se rige por ciertas garantías y que tiene su razón de ser en la necesidad de controlar los instrumentos de los que se vale el juzgador para adquirir el conocimiento de los hechos, tomando en cuenta que deben ser medios de prueba permitidos legalmente, no así medios que se basen en suposiciones, ya que deben de apegarse a ciertas garantías.

Siendo importantes los medios de prueba, pues a través de la misma se descubre la verdad, garantizándola y determinando el hecho criminal.

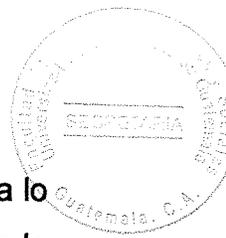
1.7. Indicios de la prueba penal

El uso de este término ha sido mal empleado en muchas ocasiones, se ha usado para catalogar ciertas pruebas o para aludir el grado de eficacia que la misma pueda tener.

Esto ha causado duda a muchos en cuanto a que es un indicio, siendo el indicio más bien un elemento de prueba como anteriormente se define, constituye un dato, circunstancia, que probado, permite mediante un razonamiento lógico, inferir la existencia o inexistencia de otros. Es decir, el vestigio o señal de algo que por el momento no se conoce, expresamente, es la conjetura de un hecho o circunstancia.

Si se tiene conocimiento, por cualquier medio, de la preparación o realización de un delito, o indicios para considerar la comisión de hechos punibles y perseguibles de

⁶ Ossorio. *Op. cit.* Pág. 460.



oficio, el Ministerio Público actuará sin necesidad de que el agraviado o una persona lo requiera, y no puede supeditar la investigación a razones de conveniencia debido a lo cual sustrae esta actividad preparatoria del proceso penal, bajo control judicial, a la disposición de las partes.

Lo anterior, siempre que no proceda el criterio de oportunidad y se trate de delitos privados, en los que debe producirse el impulso procesal por la persona afectada.

En la actualidad hablar de indicio es decir también hablar de evidencia, son casi parecidos, ya que la evidencia se puede dividir en material, intelectual y psicológico.

La evidencia es todo lo que se encuentra en un lugar en donde se ha cometido la comisión de un hecho delictivo y que es reprochable para la sociedad.

1.8. Órganos de la prueba

El órgano de prueba es la persona que colabora con el juez, independiente de qué tipo de medio de prueba pueda ser el elemento de prueba que proporciona. El dato probatorio por parte del órgano de prueba puede haber sido obtenido por orden de juez, como un perito, intérprete o un traductor, o bien de forma accidentalmente en caso del testimonio.

En nuestro medio le corresponde al Ministerio Público la averiguación de un hecho delictivo, por lo tanto, aportar las pruebas que resulten de la investigación.





CAPÍTULO II

2. Soportes informáticos

La tecnología de las comunicaciones está en un período revolucionario. Los cambios en la técnica y la tecnología se producen a una velocidad enorme. Están implicados nuevos inventos y descubrimientos.

Es una realidad el crecimiento sin precedentes de la industria y comercio de las computadoras y el lanzamiento de satélites de comunicación. El vertiginoso desarrollo de las redes, de los medios informáticos y telemáticos ha producido notable cambio en el intercambio de la información y en el desarrollo del comercio y contratación on line.

Se debe observar que los trámites bancarios pueden hacerse desde el hogar o la oficina, como también compras de distintas clases. Se transmiten y negocian documentos a través de las computadoras. Se pueden hacer reuniones y simposios estando los participantes en localidades distantes unas de otras. Desde el hogar o la oficina se puede adquirir boletos aéreos, reservas en hoteles, en trenes o ir a subastas.

Hoy se tiene terminales de bolsillo que tienen una diversidad de aplicaciones casi infinita, desde enviar mensajes hasta acceder a muchas computadoras y bancos de datos, y obviamente realizar operaciones. Ya son muy comunes los cursos universitarios on line.

Los canales de comunicación proporcionan excelentes servicios médicos, algunos computarizados y otros a través de videófonos y grandes pantallas de televisión. Los pacientes pueden ser monitoreados durante sus actividades diarias normales. Hoy día, muchos hombres de negocios, de letras, de investigación, de gobierno, entre otros, llevan un portafolio con un teclado chato y una pantalla de plasma en la tapa.



En revisión del crecimiento industrial debe observarse que: “En los últimos años ha habido un incremento de las industrias blandas, aquellas que no requieren una gran planta fija: por ejemplo, creación de software, diseño de chips, diseño de juegos electrónicos, programación de video discos, creación de material para la industria de enseñanza electrónica.”⁷ En la fuerza de trabajo de los países avanzados el porcentaje de obreros decae constantemente, en tanto que aumenta el de los empleados, muchos de los cuales son altamente móviles a causa de la infraestructura de telecomunicaciones.

Eso plantea que se está frente a un nuevo modo de producción cuyo motor principal es la inteligencia que se expresa en las formas electrónicas y la inteligencia artificial.

Todo esto conduce a un cambio de paradigmas. Es obvio, que se tiene que dar respuesta a ese movimiento y a esas nuevas formas de relaciones. De allí surgen nuevos paradigmas, nuevas formas de relaciones y por supuesto la necesidad de nuevas regulaciones. Es cierto que se puede ir derecho al infierno, o elevarse hasta al cielo. Lo más probable es que se permanecerá en la tierra, enfrentados con nuevos problemas que se buscará solucionar creando otros problemas. Para el derecho es un reto.

Se ha de admitir que se siente comodidad con ese avance o revolución microelectrónica, que es agradable la utilización de los celulares, las videoconferencias, las comunicaciones satelitales y todas esas tecnologías de la información y comunicación.

Sin darse cuenta, se está atravesando en período de transición, se está caminando decididamente, sin vuelta atrás, hacia una era informática de masas que va invadiendo todos los estamentos sociales, como en su tiempo lo hizo la electricidad, con la diferencia de que la telemática no transmite una corriente inerte, sino información.

⁷ Mires, Fernando. **La revolución que nadie soñó o la otra posmodernidad.** Pág. 15.



La sociedad va adaptándose a su uso. Pero esa satisfacción se quebranta cuando alguien incumple lo pactado, no se cumple el contrato, no es el producto que se solicitó, o cuando se conoce que por esos medios se transmiten cuestiones que afectan la moral social o a los niños. El problema, entonces, es como ir a juicio y probar el contrato, la ofensa, la oferta engañosa, el delito, entre otros.

Es cierto que la tecnificación en los últimos tiempos le ha prestado grandes servicios a la administración de justicia agilizando sus procedimientos y posibilitando un acceso más expedito a las leyes, a la doctrina y a la jurisprudencia. La gestión de los juzgados se apoya cada vez más en la informática. Pero, a su vez, el progreso ha traído consigo nuevos problemas sobre todo en lo referente a la validez y valoración de las pruebas soportadas en medios informáticos.

2.1. Los bienes informáticos

Son todos aquellos elementos que forman el sistema, ordenador, en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, así como todos los equipos que tienen una relación directa de uso con respecto a ellos y que, en conjunto, conforman el soporte físico del elemento informático. Asimismo, se consideran bienes informáticos los bienes inmateriales que proporcionan las ordenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático.

Como Servicios informáticos se entiende todos aquellos servicios que sirven de apoyo y complemento a la actividad informática en una relación de afinidad directa con ella.

2.2. Base de datos

Una base de datos o banco de datos es un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por



documentos y textos impresos en papel e indexados para su consulta. En la actualidad, debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos tienen formato electrónico, que ofrece un amplio rango de soluciones al problema de almacenar datos

“Surgen desde mediados de los años sesenta la historia de las bases de datos, en 1970 Codd propuso el modelo relacional, este modelo es el que ha marcado la línea de investigación por muchos años, ahora se encuentran los modelos orientados a objetos.”⁸

Entre las ventajas de las bases de datos se encuentran las siguientes:

Independencia de datos y tratamiento: Cambio en datos no implica cambio en programas y viceversa (Menor coste de mantenimiento): Como: Coherencia de resultados: Reduce redundancia: Acciones lógicamente únicas y se evita inconsistencia. Mejora en la disponibilidad de datos: No hay dueño de datos (No igual a ser públicos), ni aplicaciones ni usuarios y guardamos descripción (Idea de catálogos). Cumplimiento de ciertas normas: Restricciones de seguridad. Accesos (Usuarios a datos) y operaciones (Operaciones sobre datos). Otras ventajas: Más eficiente gestión de almacenamiento.

La arquitectura de una base de datos se encuentra conformada de la siguiente manera:

a) Nivel Físico: Este se refiere a los datos que se encuentran almacenados dentro de los dispositivos electrónicos. Es decir, como se almacenan los datos, ya sea en registros, o como sea. Este se utiliza por una minoría de los usuarios debido a que no todos se encuentran en capacidad de utilizarlo. “Este nivel lleva asociada una representación de los datos, que es lo que denominamos Esquema Físico.”⁹

⁸ Elmasri, Ramez y Shamkant B. Navathe. **Fundamentos de base de datos**. Pág. 24.

⁹ Ramos Martín, Alicia. **Sistemas gestores de bases de datos. Grado superior**. Pág. 54.



- b) Nivel Conceptual: Este es el que se refiere a la base de datos enfocado desde un punto de vista real. Es decir, se trata con la entidad u objeto representado, sin importarnos como está representado o almacenado. Este nivel lleva asociado el Esquema Conceptual.

- c) Nivel Visión: Son partes del esquema conceptual. El nivel visión es el encargado de dividir estas parcelas. Un ejemplo sería el caso del empleado que no tiene por qué tener acceso al sueldo de sus compañeros o de sus superiores. El esquema asociado a este nivel es el Esquema de Visión.

Los 3 niveles vistos, componen lo que conocemos como arquitectura de base de datos a 3 niveles.

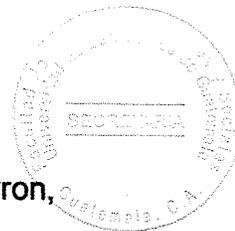
A menudo el nivel físico no es facilitado por muchos DBMS, esto es, no permiten al usuario elegir como se almacenan sus datos y vienen con una forma estándar de almacenamiento y manipulación de los datos.

La arquitectura a 3 niveles se puede representar de la siguiente manera: Subesquema de Visión, Subesquema de Visión, Subesquema de Visión.

Las estructuras de bases de datos: Existen multitud de estos modelos que se conocen como Modelos de Datos, algunos de estos modelos son: Modelo relacional de datos, modelo de red y modelo Jerárquico

2.3. El ordenador y la computadora

La máquina analítica: “También en el siglo XIX el matemático e inventor británico Charles Babbage elaboró los principios de la computadora digital moderna. Inventó una serie de máquinas, como la máquina diferencial, diseñadas para solucionar problemas matemáticos complejos. Muchos historiadores consideran a Babbage y a su socia, la



matemática británica Augusta Ada Byron (1815-1852), hija del poeta inglés Lord Byron, como a los verdaderos inventores de la computadora digital moderna.

La tecnología de aquella época no era capaz de trasladar a la práctica sus acertados conceptos; pero una de sus invenciones, la máquina analítica, ya tenía muchas de las características de un ordenador moderno. Incluía una corriente, o flujo de entrada en forma de paquete de tarjetas perforadas, una memoria para guardar los datos, un procesador para las operaciones matemáticas y una impresora para hacer permanente el registro.¹⁰

2.3.1. Primeros ordenadores

Los ordenadores analógicos: “Comenzaron a construirse a principios del siglo XX. Los primeros modelos realizaban los cálculos mediante ejes y engranajes giratorios. Con estas máquinas se evaluaban las aproximaciones numéricas de ecuaciones demasiado difíciles como para poder ser resueltas mediante otros métodos. Durante las dos guerras mundiales se utilizaron sistemas informáticos analógicos, primero mecánicos y más tarde eléctricos, para predecir la trayectoria de los torpedos en los submarinos y para el manejo a distancia de las bombas en la aviación.”¹¹

2.3.2. Ordenadores electrónicos

“Durante la II Guerra Mundial (1939-1945), un equipo de científicos y matemáticos que trabajaban en *Bletchley Park*, al norte de Londres, crearon lo que se consideró el primer ordenador digital totalmente electrónico, el *Colossus*. Hacia diciembre de 1943 el *Colossus*, que incorporaba 1.500 válvulas o tubos de vacío, era ya operativo.”¹²

Fue utilizado por el equipo dirigido por Alan Turing para descodificar los mensajes de radio cifrados de los alemanes. “Este prototipo y las investigaciones posteriores se

¹⁰ Solís, José Antonio. **Historia de las cosas**. Pág. 65.

¹¹ Spagni de Barletta, Beatriz; Augusto Dante Bergagna; Gabriela Roldán y Mirta López de Abdala. **Apéndice de estadística básica**. Pág. 4.

¹² Mari Sáez, Víctor Manuel. **Globalización, nuevas tecnologías y comunicación**. Pág. 22.



realizaron en el anonimato, y más tarde quedaron eclipsadas por el desarrollo del Calculador e integrador numérico digital electrónica (ENIAC) en 1945.”¹³ El ENIAC, que según mostró la evidencia se basaba en gran medida en el ordenador Atanasoff-Berry (ABC, acrónimo de Electronic Numerical Integrator and Computer), obtuvo una patente que caducó en 1973, varias décadas más tarde.

“El ENIAC contenía 18.000 válvulas de vacío y tenía una velocidad de varios cientos de multiplicaciones por minuto, pero su programa estaba conectado al procesador y debía ser modificado manualmente. Se construyó un sucesor del ENIAC con un almacenamiento de programa que estaba basado en los conceptos del matemático húngaro-estadounidense John von Neumann. Las instrucciones se almacenaban dentro de una llamada memoria, lo que liberaba al ordenador de las limitaciones de velocidad del lector de cinta de papel durante la ejecución y permitía resolver problemas sin necesidad de volver a conectarse al ordenador.”¹⁴

A finales de la década de 1950 el uso del transistor en los ordenadores marcó el advenimiento de elementos lógicos más pequeños, rápidos y versátiles de lo que permitían las máquinas con válvulas.

Como los transistores utilizan mucha menos energía y tienen una vida útil más prolongada, a su desarrollo se debió el nacimiento de máquinas más perfeccionadas, que fueron llamadas ordenadores o computadoras de segunda generación. Los componentes se hicieron más pequeños, así como los espacios entre ellos, por lo que la fabricación del sistema resultaba más barata.

2.3.3. Circuitos integrados

A finales de la década de 1960 apareció: “El circuito integrado (CI), que permitió la fabricación de varios transistores en un único sustrato de silicio en el que los cables de

¹³ **ibid.**

¹⁴ Solís. **Op. cit.** Pág. 65.



interconexión iban soldados.”¹⁵ El circuito integrado permitió una posterior reducción del precio, el tamaño y los porcentajes de error. El microprocesador se convirtió en una realidad a mediados de la década de 1970, con la introducción del circuito de integración a gran escala (LSI, acrónimo de Large Scale Integrated) y, más tarde, con el circuito de integración a mayor escala (VLSI, acrónimo de Very Large Scale Integrated), con varios miles de transistores interconectados soldados sobre un único sustrato de silicio.

2.3.4. Microminiaturización

Una tendencia constante en el desarrollo de los ordenadores es la microminiaturización, iniciativa que tiene a comprimir más elementos de circuitos en un espacio de chip cada vez más pequeño. Además, los investigadores intentan agilizar el funcionamiento de los circuitos mediante el uso de la superconductividad, un fenómeno de disminución de la resistencia eléctrica que se observa cuando se enfrían los objetos a temperaturas muy bajas.

Las redes informáticas se han vuelto cada vez más importantes en el desarrollo de la tecnología de computadoras. Las redes son grupos de computadoras interconectados mediante sistemas de comunicación. La red pública Internet es un ejemplo de red informática planetaria. Las redes permiten que las computadoras conectadas intercambien rápidamente información y, en algunos casos, compartan una carga de trabajo, con lo que muchas computadoras pueden cooperar en la realización de una tarea. Se están desarrollando nuevas tecnologías de equipo físico y soporte lógico que acelerarán los dos procesos mencionados.

Otra tendencia en el desarrollo de computadoras es el esfuerzo para crear computadoras de quinta generación, capaces de resolver problemas complejos en formas que pudieran llegar a considerarse creativas. Una vía que se está explorando

¹⁵ López Aldea, Eugenio. **Arduino. Guía práctica de fundamentos y simulación.** Pág. 42.



activamente es el ordenador de proceso paralelo, que emplea muchos chips para realizar varias tareas diferentes al mismo tiempo.

El proceso paralelo podría llegar a reproducir hasta cierto punto las complejas funciones de realimentación, aproximación y evaluación que caracterizan al pensamiento humano.

Otra forma de proceso paralelo que se está investigando es el uso de computadoras moleculares. En estas computadoras, los símbolos lógicos se expresan por unidades químicas de ADN en vez de por el flujo de electrones habitual en las computadoras corrientes. Las computadoras moleculares podrían llegar a resolver problemas complicados mucho más rápidamente que las actuales supercomputadoras y consumir mucha menos energía.

2.3.5. Desarrollo de computadoras

Pueden identificarse dos tendencias dentro del desarrollo de computadoras, en primer lugar, una tendencia dentro del desarrollo de los programas y lenguajes usados en la operación de las computadoras y la otra dentro de equipos y computadoras.

En primer lugar, los programas y lenguajes están evolucionando hacia autonomía propia que les permita realizar más y más tareas sin ayuda del humano, además de copiar la forma de razonar propia de sus creadores. Dentro de esta idea podemos citar las filosofías de inteligencia artificial y sistemas expertos.

El concepto de inteligencia artificial se refiere a la idea de que un programa o lenguaje sea capaz de aprender y de razonar, tal y como lo haría un humano. Un programa de inteligencia artificial es capaz de aprender de sus propios errores corrigiendo su operación en función de sus propios resultados almacenando de alguna forma esta experiencia adquirida para situaciones futuras.



Como podemos ver las tendencias de los programas y lenguajes es independizarse de sus creadores dejando de ser ya una simple herramienta tener más bien la cualidad de un colaborador dentro del trabajo a desempeñar.

Los equipos de computación modernos incluyen nuevas y mejores capacidades de generación de sonido, imagen y otros usados en las presentaciones, producción de prensa, cine y televisión por computadora, que es lo que se ha dado por llamar la revolución de los medios múltiples. Por otro lado, el desarrollo futuro de los equipos de computación debe seguir en alguna medida el desarrollo de los programas que los alimentan, buscando una mayor autonomía por parte del equipo en sí.

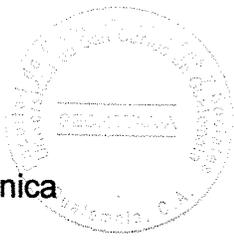
Cobran interés en esta área los términos robótica y cibernética, que identifican a las ramas de la ciencia que se encargan de producir elementos con movilidad propia y que imitan los movimientos y funciones del cuerpo humano o de animales y seres naturales, brazos mecánicos, ojos electrónicos y otros elementos robóticos avanzados han de pasar a formar parte de los equipos de computación futuros.

Estos desarrollos nos acercaran a esas máquinas con autonomía propia que tan comúnmente nos presentan las obras de ciencia-ficción, pero definitivamente esa a de ser la tendencia futura de la computadora ya robot o sistema robótica, totalmente autónomo y capaz de la realización de tareas sofisticadas sin intervención humana.

2.3.6. Computadoras

Es un dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

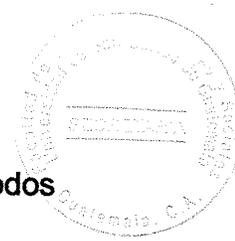
El computador tiene dos partes fundamentales que se complementan para su correcto funcionamiento, a la primera la llamaremos el Hardware: que consiste en su parte física, es decir lo que podemos ver, tocar, armar y desarmar.



La segunda es el Software esta es el alma del computador, toda su parte electrónica que le permite realizar las tareas correspondientes.

Estructura Interna:

- a) **Procesador:** Es la parte fundamental de los ordenadores, es el cerebro de este. Por medio de un chip son ejecutadas las instrucciones que el usuario envía, para posteriormente ser procesados estos datos por el cerebro del ordenador.
- b) **Memoria ROM:** Esta es la que contiene los comandos principales con los cuales funcionan los ordenadores.
- c) **Puertos:** Son las entradas para conectar distintos dispositivos. Los puertos son de dos tipos. **Serial:** Conecta el ratón, el módem, el escáner y, en ciertos casos la impresora. El computador los reconoce internamente con las letras COM.
- d) **Paralelo:** Estos puertos se diferencian entre sí por las características para transmitir datos a determinada velocidad.
- e) **Memoria RAM:** Es una tarjeta utilizada para el almacenamiento de los datos mientras se encuentra ejecutando el ordenador. Esta memoria es la que le brinda la velocidad para la búsqueda de los documentos que se buscan dentro del sistema operativo.
- f) **Tarjeta Madre:** Esta es otro tipo de tarjeta en la cual se unen todos los componentes del computador, en la cual cuenta con conectores para el funcionamiento de las demás tarjetas.
- g) **Bus:** Este es el medio por el cual se transmiten los datos que son conectados entre ellos a los distintos componentes del ordenador, tanto internos como externos.



- h) Disco Duro: Este es el dispositivo interno del ordenador, en el cual se guardan todos los datos como los programas y archivos.
- i) Disco Blando: Estos eran los llamados diskettes, en los cuales se almacenaba la información para ser trasladada de un dispositivo a otro, los que en la actualidad son poco utilizados, en su reemplazo se utilizan las memorias USB o los CD's.

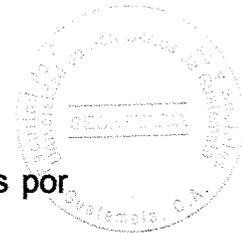
La estructura externa se encuentra compuesta por los siguientes componentes:

- a) La Pantalla: Muestra las imágenes que elaboramos en el computador.
- b) Teclado: Periférico de entrada para digitalizar textos.
- c) El Mouse: Dispositivo para entrada de información
- d) Impresora: Periférico para salida de información en forma física como en papel, acetato o adhesivos.
- e) Escáner: Este es un dispositivo para la entrada de información, permite capturar imágenes y texto para ser trabajadas en el computador.
- f) Fax Modem Externo: Dispositivo de salida permite enviar y recibir faxes, algunos tienen contestador automático y otros servicios.

2.3.7. Las computadoras en la oficina

En las últimas décadas, las computadoras y la tecnología de la computación se han introducido más y más en los lugares de trabajo, a menudo transformando considerablemente los tipos de trabajos que las personas realizan y la manera en que los hacen. Algunas personas respondieron a estos cambios con entusiasmo, recibiendo con agrado la oportunidad de aprender nuevas técnicas y sintiendo emoción por las eficiencias que las nuevas tecnologías hicieron posibles.

Otros respondieron de manera diferente, se encontraban a gusto con sus empleos como eran, resintió la necesidad de volver a ser capacitados y sintieron temor, a



menudo con razón, de que las nuevas tecnologías podrían eliminar sus empleos por completo.

Actualmente los sistemas computacionales son más fáciles de utilizar, y ahora es clara su importancia en el campo de trabajo.

Pero la tecnología de la computación sigue desarrollándose a un paso increíblemente rápido, y no es posible saber con certeza cuáles serán todas las aplicaciones de esta tecnología en el futuro, porque hay que mantenerse al día con los nuevos adelantos en el campo de la computación.

2.3.8. Beneficios y efectos de la computadora

Los sistemas computacionales se han convertido en una parte tan importante en la actualidad de la vida moderna. Su capacidad de clasificar enormes cantidades de datos y de producir rápidamente información útil para cualquier clase de usuario desde el empleado que hace la nómina hasta el Presidente los hace indispensables en una sociedad como la nuestra. Sin las computadoras, por ejemplo, el Gobierno posiblemente no podría tabular todos los datos que colecta para hacer el censo de población cada diez años.

Los bancos se verían agobiados por el trabajo de mantener al día todas las transacciones que deben procesar. El eficiente servicio telefónico que todos utilizamos sería imposible. La exploración de la Luna y el transbordador espacial serían todavía fantasías de la ciencia-ficción.

Pero junto con los beneficios que las computadoras brindan a la sociedad se han originado algunos conflictos, que van desde la salud hasta la seguridad e intimidad personales.



Los sistemas computacionales siguen paso a paso las cuentas bancarias y las compras realizadas con tarjetas de crédito. Controlan los sistemas de reservaciones masivas de las aerolíneas, ejecutan millones y millones de cálculos necesarios para enviar a los astronautas al espacio exterior y para traerlos de regreso seguros.

Asimismo, dirigen la producción de las fábricas y proporcionan a los ejecutivos información actualizada necesaria para tomar decisiones, además se encuentran montadas en relojes y costosos satélites. Las aplicaciones parecen no tener fin.

Hace apenas 50 años, estas máquinas eran parte de una oscura tecnología que sólo resultaba de interés para un puñado de científicos. Actualmente son parte de la vida diaria de millones de personas.

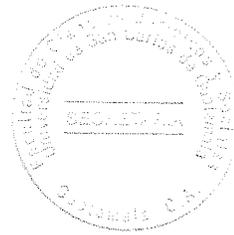
2.4. La red de información internet

La llamada autopista de la información es, realmente, un conjunto de miles de redes informáticas unidas entre sí. Comenzó con el propósito de crear una infraestructura comunicativa entre computadoras con fines militares. Hoy en día existen miles de redes que interconectan por vía telefónica millones de computadoras personales de todo el mundo.

El espíritu inicial de las primeras experiencias era simplemente académico: pretendían unir bases de datos de centros de investigación de todo el mundo para intercambiar información.

El concepto Internet significa Inter – red o sea una red internacional de comunicación.

Cuando hablamos de Internet hacemos referencia a una red que no pertenece a nadie, sino que está conformada por la información que le brindan los millones de usuarios que se conectan a ella.



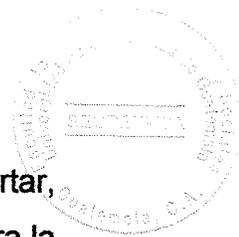
2.4.1. La historia de vida de internet

“Internet fue creada a partir de un proyecto del departamento de defensa de los Estados Unidos llamado ARPANET (Advanced Research Project Network según su sigla en inglés) fue iniciado en 1969 y cuyo principal propósito era la investigación y desarrollo de protocolos de comunicación para redes de área amplia, para ligar redes de transmisión de información de diferentes tipos; capaces de resistir las condiciones de operación más difíciles y continuar funcionando aún con la pérdida de una parte de la red.

Estas investigaciones dieron como resultado el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) un sistema de comunicaciones muy sólido y robusto bajo el cual se integran todas las redes que conforman lo que se conoce actualmente como Internet.

Durante el desarrollo de este protocolo se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando origen así a la red de redes más grande del mundo, las funciones militares se separaron y se permitió el acceso a la red a todo aquel que lo requiriera sin importar de que país provenía la solicitud siempre y cuando fuera para fines académicos o de investigación (y por supuesto que pagara sus propios gastos de conexión), los usuarios pronto encontraron que la información que había en la red era por demás útil y si cada quien aportaba algo se enriquecería aún más el cúmulo de información existente.

Después de que las funciones militares de la red se separaron en una sub-red de Internet (llamada MILNET), la tarea de coordinar el desarrollo de la red recayó en varios grupos, uno de ellos, la *National Science Foundation* fue el que promovió bastante el uso de la red ya que se encargó de conectar cinco centros de contención de información a los que se accedía desde cualquier nodo de la red.



Debido al tráfico de datos se superaron las cargas de información que podía soportar, entonces se dio la concesión a *Merit Network Inc.* para que administrara y actualizara la red, se mejoraron las líneas de comunicación dando un servicio mucho más rápido, pero este proceso de mejora nunca termina debido a la creciente demanda de los servicios que se encuentran en la red.¹⁶

El enorme crecimiento de Internet se debe en parte a que es una red basada en fondos gubernamentales de cada país que forma parte de Internet lo que proporciona un servicio prácticamente gratuito.

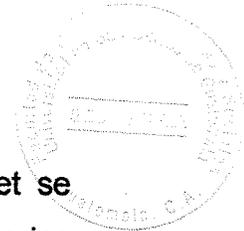
A principios de 1994 comenzó a darse un crecimiento explosivo de las compañías con propósitos comerciales en Internet, dando así origen a una nueva etapa en el desarrollo de la red.

2.4.2. Servicios varios de internet

El avance de la manera de comunicarse permite a Internet ofrecer variados servicios entre los cuales se enumeran algunos como: bibliografía o clases a distancia (e-learning), la opción de jugar partidas multiplayer de un mismo juego en un servidor, la posibilidad de buscar información, enviar y distribuir correo y mensajes, intercambiar información en los foros que tratan distintos temas, mantener charlas en los canales de chat, realizar videoconferencias en tiempo real, "bajar" de Internet programas o software para la computadora, realizar compras por medio de entidades que ofrecen sus productos o por medio del e-commerce, realizar llamadas telefónicas o compartir encuestas y curiosidades.

La red Internet ofrece también otros servicios para corporaciones o empresas supranacionales. Algunas empresas establecidas ofrecen soporte técnico a través de Internet o de una página web.

¹⁶ Guevara Gamboa, Félix Antonio. **Computación paso a paso**. Pág. 54.



a) **Buscadores de información, una alternativa en la red:** En la red de Internet se encuentran varias formas de buscar información, estas son: buscadores, directorios y portales temáticos.

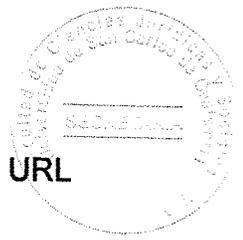
Comenzando por los buscadores, podemos decir que todos ellos poseen un motor de búsqueda, gracias al cual, escribiendo una palabra clave en la caja de búsqueda se encuentran hipervínculos hacia páginas que contienen dicha palabra clave, aunque a veces el contenido de la página no representa los datos que se desean encontrar.

Uno de los buscadores más efectivo es el que se encuentra en el sitio web www.altavista.com. Si en este buscador deseamos encontrar una receta de sushi por ejemplo cuando busquemos, el motor de búsqueda descartara los resultados que no se hayan relacionado con la palabra buscada. Otros motores de búsqueda bien calificados por los usuarios son www.google.com.ar, www.lycos.com.

La otra manera de buscar información es mediante un directorio (por ejemplo: www.yahoo.com.ar) donde deberemos hacer clic en las diferentes secciones para ir avanzando en la búsqueda.

Por lo tanto, se puede decir que un directorio es una manera jerárquica de organizar la información. Otra definición de directorio: es una base de datos con la peculiaridad de que esta optimizado para realizar lecturas, navegaciones y grandes búsquedas sobre él; como ya vimos la información en él está organizada de modo jerárquico y este contiene objetos de una clase determinada con distintos atributos que son los que realmente contienen la información.

Otro método para encontrar información en la red es la búsqueda en portales temáticos. Se llama así a los sitios que agrupan la información de un mismo tema (por ejemplo: gastronomía, deportes, computación, entre otros); existen varias formas de encontrar estos portales: una de ellas es entrar en el sitio web www.buscaportal.com.



Estos sitios parecen lo mejor para encontrar información, pero de no conocer el URL correcto, no nos serán de mucha utilidad.

2.4.3. Módems y formas de conexión a internet

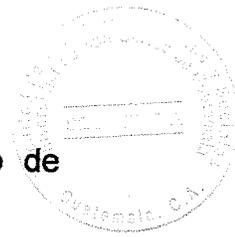
Para conectarse a Internet existen varios métodos y modelos del hardware necesario. Si deseamos tener conexión a Internet, deberemos buscar el módem adecuado para la necesidad o uno que ofrezca los resultados que queremos.

Entre los distintos tipos de módem que se encuentran en el mercado podemos citar varios tipos, los primeros son los módems que utilizan la línea telefónica, estos módems se pueden conectar internamente o externamente al CPU de la computadora. Ambos cumplen la misma función, la única diferencia es que los módems externos son más fáciles de extraer y transportar hacia otros equipos.

En el caso de comprar un módem interno, se debe tener en cuenta que slot utiliza: existen módems que se conectan en puertos PCI o AMR (recomendados, todos utilizan los puertos COM1, COM2, COM3 y COM4) y otros que utilizan el puerto ISA que simplemente han quedado en el pasado. En el caso de los módems externos los mejores son los que se conectan vía USB, pero aún existen los que utilizan el puerto serie de la computadora.

Otro tipo de módem que se encuentra a la venta son los DSP (sigla en inglés que significa Digital Signal Processor) que son chips con la función de realizar los complejos cálculos matemáticos, transformando la señal digital a analógica o viceversa. También se encuentran los llamados winmódems o HSP que eliminan el procesador y trabajan directamente con el CPU de la computadora, lo que abarata los costos de producción.

Por último, vamos a hablar de la característica que le permite a los módems especiales funcionar como un fax pero con una velocidad mucho mayor. Hay módems que, con la



ayuda de una placa de sonido y el software apropiado, brindan un servicio de contestador automático.

Otros permiten que cada miembro de la familia posea un buzón de voz desde el cual enviaran sus *voice mail*; con el módem que los soporte obviamente.

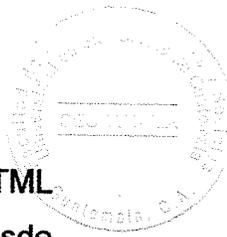
2.4.4. Protocolos de comunicación

Los módems anteriormente nombrados poseen un estándar de comunicaciones, el actual se llama V.90, es decir el que funciona con los módems de 56 kbps (kilo bites por segundo). Hasta el año 1998 existían otros dos estándares de comunicación que eran utilizados solo por una marca de módems. El primero de estos estándares era el X2 de US Robotics y el otro era el K56 Flex, utilizado por Motorola.

Gracias a las mejoras producidas existen protocolos de detección y corrección de errores en la transferencia, estos protocolos sirven para detectar distorsiones en la línea telefónica. Los protocolos de detección más usados son MNP (Microcom Networking Protocol) y LAMP (Link Acces Procedure for Módem); el último de ellos es el de mayor difusión por lo que es útil que nuestro hardware lo soporte.

Actualmente existe otro protocolo de transferencia de datos que se llama V.24 bis, que permite transmitir datos hasta cuatro veces más rápido, previa compresión de dichos datos. En cuanto a los sitios web se refiere, también son gobernados por protocolos (set de reglas estándar que determina como se comunicaran las computadoras con cada una de las otras a través de la red), uno de ellos es:

- a) HTTP: es el protocolo que controla la transferencia de hipertexto entre las computadoras, su significado es *Hypertext Transfer Protocol*.



Para el uso del protocolo anterior las páginas web se diseñan en el lenguaje HTML (significa *Hiper Text Markup Language*), las cuales pueden ser navegadas desde cualquier browser o visualizador.

2.5. El documento electrónico

Este es el que fue creado a partir de un dispositivo electrónico, Tomando la clasificación de documento electrónico que hace el mismo autor, es documento electrónico tanto el formado por el elaborador como el documento formado por medio del elaborador.

Es de considerarse que en la actualidad la tecnología ha incursionado tanto en Guatemala que los documentos creados en soporte papel hasta cierto punto están siendo reemplazados por este sistema que brinda mayores ventajas en la creación y registro de los documentos y la validez es la misma como que constaran en un soporte papel.

El desarrollo del documento electrónico visto desde una forma material es de vital importancia ya que, en el exclusivamente figurará como medio de prueba una declaración de voluntad hecha por las personas que lo hacen mediante medios electrónicos. En sentido amplio el documento electrónico se considera como tales inclusive a los que han sido realizados por cualquier medio informático, y que se pueden o no encontrar en soporte de papel.

Pero en el sentido estricto es el que se refiere al documento electrónico que tiene su soporte de manera electrónica.

Las ventajas que ofrece el documento electrónico es que se evita tanto papeleo, él envío de los documentos es rápido no solo a nivel nacional sino internacional y además los avisos que se deben dar en los diferentes registros es más viable y rápido porque se hace a través del correo electrónico.



Evidentemente en los documentos electrónicos, el concepto original de documento en soporte de papel desaparece, al ser sustituido por la base magnética que contiene impulsos electrónicos convertidos en bits, siendo estos visibles y perceptibles a la percepción humana tan sólo gracias a la transmisión de la computadora, pantalla, e impresora, entre otros.

En el ámbito jurídico, los documentos electrónicos deben representar hechos de relevancia jurídica, o sea que sean susceptibles de ser probados en un proceso judicial, en este sentido, dentro del contexto jurídico. Tomando en cuenta que el documento electrónico para servir como prueba en un proceso judicial es hasta cierto punto difícil su valoración porque la ley aun no regula el procedimiento de como presentar y diligenciar el medio de prueba electrónico.

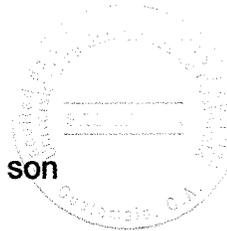
2.5.1. Características

Lo que interesa ahora es determinar si existe identidad entre el documento tradicional y el electrónico, para lo cual se efectuará un análisis sobre la base de las características del primero y su manifestación en el entorno digital.

Reconociendo que existe diversidad conceptual entorno al documento, quizás resulta más relevante el establecer las características esenciales que podríamos rescatar de todas ellas. En este sentido es posible señalar que el documento tiene las siguientes particularidades, es de tipo material y tiene un objetivo específico de un acto, además es una garantía permanente e inmutable.

Entonces, ¿es posible decir que el soporte digital del documento electrónico puede cumplir con las mismas características antes referidas y que, por lo tanto, no se deberían generar discriminaciones entre ambos?

Quienes plantean que no se puede equiparar el documento electrónico al soporte analógico fundamentan que éstos son susceptibles de alteración, no existe en los



mismos la diferenciación entre original y copia y, en último término, porque no son escritos.

Para nosotros, en los mismos términos que para nuestro legislador, como lo veremos más adelante, no existen suficientes diferencias sustanciales entre ambos tipos de documentos, y por lo tanto es perfectamente posible hablar de equiparación. En virtud de ello analizaremos, en lo que sigue, los caracteres que más conflicto generan en el proceso de homologación:

a) La escritura: Aun cuando es difícil de entender para los operadores jurídicos, los documentos electrónicos también están escritos, pero en un lenguaje que les es propio: el binario. En este sentido, un documento electrónico no sería más que un conjunto de bits, una combinación de 1 y 0, que al ser convertido a algo legible es lo que se muestra en las pantallas del ordenador, como los textos, imágenes y sonidos.

Por lo tanto, no se debe discriminar un documento electrónico y pensar que no posee escritura por el sólo hecho de no estar expresado en los términos del lenguaje tradicional.

Situación diversa es que los documentos electrónicos se diferencien de los de papel en relación a su continente, ya que, en éstos, tanto la estructura como el contenido y su visualización, se confunden con el mismo soporte en el que se fija la escritura; en cambio, en aquéllos, dichos aspectos se dan por separado.

b) La alterabilidad: Se señala que uno de los aspectos fundamentales de los documentos que constan en papel es que tienen la particularidad de fijar situaciones o hechos, y que de esta forma, permiten que los mismos permanezcan en el tiempo con ciertos grados de inalterabilidad. Por ello se piensa que los documentos electrónicos pudieran ser inestables o volátiles, y en tal sentido, no dar cumplimiento a dicho objetivo de fijeza.



Efectivamente los soportes digitales son susceptibles de alteración, pero en ningún caso lo sería más que en su símil analógico, por lo cual no puede ser cuestionado el valor jurídico de este, se deben de implementa protocolos más estrictos sobre estos.

Por ello, se entiende que el documento electrónico debiera estar revestido de ciertos márgenes de seguridad para que no pierda su naturaleza documental, y como tal pueda ser inalterable, legible y estable o que permanezca en el tiempo.

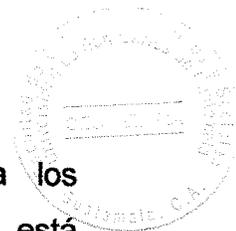
Con todo, estimamos que es fundamental tener presente, que por requerir el documento electrónico de programas informáticos capaces de convertir el lenguaje binario en lenguaje humano, se hace indispensable velar no sólo por la conservación del documento en sí, sino también del código que permite tenga éxito la conversión de lenguajes.

c) Las copias: En el mundo analógico no se presentan problemas respecto de distinguir entre un original y una copia, lo cual reviste de gran importancia, en el entendido que el ordenamiento jurídico les otorga distinto valor.

En el caso especial de los documentos electrónicos, la discusión va desde el entender que el único original sería el conservado en la memoria del soporte informático que lo crea y toda otra representación sería copia, a señalar que, por su especial naturaleza, no se podría diferenciar entre original y copia. El punto es que, por ser poco operativo, finalmente se termina grabando en soportes de todo tipo, como disquete, CD, u otros.

Por estas razones, se considera que, en lo que dice relación con los documentos electrónicos, carece de sentido distinguir entre originales y copias. Lo que importa es que éste tenga la virtud de asegurar autoría e integridad.

Como se observa, de las características analizadas podemos concluir que el documento electrónico reúne los elementos comunes del documento tradicional, en



cuanto materialidad, permanencia e inmutabilidad, sólo que adaptado a los requerimientos que exige su propia naturaleza electrónica; y más aún, que está capacitado para cumplir con las funciones del documento, que en último término, es aquello que lo distingue como medio probatorio.

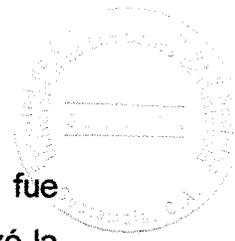
2.5.2. Clases

Los documentos electrónicos son una especie dentro del género de los documentos, y los mismos han nacido del uso cada vez más generalizado de las tecnologías de la información, así como de la masificación de las telecomunicaciones, y con ellos el comercio electrónico, obligando al derecho a desarrollar regulaciones que permitan el uso de dichas tecnologías. Al igual que todos los documentos, los electrónicos son cosas, aunque intangibles, capaces de representar un hecho relevante jurídicamente en tiempo, modo, y lugar, siendo su diferencia fundamental con los demás documentos la forma como viene dada la representación de dicho hecho.

2.6. Firma electrónica

La firma electrónica es solo un componente de la Infraestructura de Clave Pública (PKI), la cual incluye hardware, software y políticas de seguridad, para que funcione la firma electrónica y otros procedimientos como el cifrado de información, el estampado cronológico, la custodia de documentos, y puedan garantizar la integridad, la confidencialidad, la disponibilidad, la autenticación y el no repudio de la información.

Debido a que la firma electrónica y la Infraestructura de Clave Pública (PKI) representan una alternativa eficiente y confiable para las comunicaciones, en muchos países del mundo se le ha dado la misma validez jurídica que a los métodos tradicionales de comunicación basados en el papel. Guatemala no es la excepción, por medio de la “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” se ha equiparado los medios físicos de comunicación a los medios electrónicos de comunicación, así como la firma manuscrita con la firma electrónica.



La Ley para el reconocimiento de las comunicaciones y firmas electrónicas fue publicada en el diario oficial el 23 de septiembre de 2008 y a partir de eso, empezó la implementación práctica de ciertas entidades necesarias.

La Cámara de Comercio de Guatemala, quedó constituida como la primera prestadora de servicios de certificación, el Ministerio de Economía fue el encargado de desarrollar el reglamento respectivo que fue publicado el 13 de mayo de 2009 y también fue el encargado de crear el Registro de Prestadores de Certificación, entidad en la cual se deben registrar todos los prestadores de servicios de certificación, el cual abrió sus puertas el 17 de junio de 2009.

2.7. Elementos que componen un documento electrónico

Los documentos electrónicos poseen los mismos elementos que un documento escrito en soporte papel; a) constan en un soporte material (cintas, diskettes, circuitos, chips de memoria, redes); b) contiene un mensaje, el que está escrito usando el lenguaje convencional de los dígitos binarios o bits, entidades magnéticas que los sentidos humanos no pueden percibir directamente; c) están escritos en un idioma o código determinado; d) pueden ser atribuidos a una persona determinada en calidad de autor mediante una firma digital, clave o llave electrónica.

2.8. Leyes vigentes que contemplan la utilización de medios computarizados

En Guatemala se encuentran varias leyes relacionadas con los medios computarizados, las cuales se citan a continuación:

- a) La Constitución Política de la República de Guatemala: artículo 80. Promoción de la ciencia y la tecnología. El Estado reconoce y promueve la ciencia y la tecnología como bases fundamentales del desarrollo nacional, La ley normará pertinentemente.



b) El Decreto 27-92 Ley del Impuesto al Valor Agregado (IVA): Artículo 28. Información de la Dirección General de Aduanas. “La Dirección General de Aduanas deberá llevar un registro computarizado, en base al NIT, de todas las importaciones que se realicen. A requerimiento de la Dirección, aquella le deberá proporcionar la información que ésta le solicite al respecto.”

Artículo 29. Establece que la dirección está facultada para autorizar, a solicitud del contribuyente, el uso de facturas emitidas en cintas o tiquetes, en forma mecanizada o computarizada, pro máquinas registradoras reguladas conforme lo establece el Artículo 31 de esta ley, siempre que por la naturaleza de sus actividades que realice se justifique plenamente. El reglamento desarrollará los requisitos y condiciones.

c) Ley de Derecho de Autor: “Artículo 4. Para los efectos de esta ley se entiende por... Programa de ordenador: La obra constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o cualquier otra forma que al ser incorporadas a un soporte legible por máquina, es capaz de hacer que un ordenador ejecute determinada tarea u obtenga un resultado.”

d) Acuerdo número 041/002 de la Corte Suprema de Justicia: En el presente acuerdo, se plasma evidentemente la modernización y avance tecnológico que debe prevalecer en la creación, preservación, archivo y reproducción de información electrónica.

“Artículo 1. Registro Electrónico de Notarios. La información del registro manual de notarios sustentada en expedientes, tarjetas y en libros físicos existentes será trasladada digitalmente...”

“Artículo 2. Características. El Registro Electrónico de Notarios, tendrá las características siguientes: interactivo, ágil, acorde a la tecnología moderna...”



“Artículo 3. Contenido del Registro Electrónico de Notarios... Por medio del Registro Electrónico de Notarios, se archivará, registrará, consultará y comunicará la información recibida, accesada, procesada y desplegada...”

“Artículo 5. Actualización de la base de datos. Se faculta a la Dirección del Archivo General de Protocolos, para actualizar la información del Registro Electrónico de Notarios, generada por la información digitalizada que comprende la base de datos, firma, sello y fotografía de notarios.”

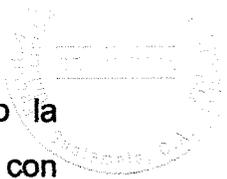
“Artículo 6. Certificaciones. Toda reproducción por cualquier medio que provenga del Registro Electrónico de Notarios, extendida por el Archivo General de Protocolos, tendrá los mismos efectos legales de las certificaciones extendidas manualmente por el citado archivo.”

e) Decreto número 9 de la Asamblea Constituyente de la República de Guatemala, Ley de Emisión del Pensamiento:

“Artículo 2. Se considera impreso la fijación del pensamiento por medio de la imprenta, la litografía, la fotografía, el mimeógrafo, multígrafo, el fonógrafo o cualesquiera procedimientos mecánicos empleados actualmente o que puedan emplearse en el futuro para la reproducción de las ideas.

Para los efectos de esta ley se equiparán a los impresos, cualesquiera otras formas de representación de las ideas, con destino al público, tales como estampas, fotografías, grabados, emblemas, diplomas, medallas, discos, cintas alambres fonográficos, ya sean fijados en papel, tela u otra clase de materia.”

f) Código Civil: Artículo 1221. (Reformado por Artículo 16 Decreto 124-85). “El registrador llevará, asimismo, los libros que sean necesarios para las inscripciones especiales y los demás que determine el reglamento del Registro.



Queda facultado para innovar progresivamente al actual sistema, adoptando la microfilmación de los documentos, la computarización el teleproceso, de acuerdo con las posibilidades económicas del Registro.”

La Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008 (En todo su contenido).

CAPÍTULO III



3. Bien jurídico tutelado en los delitos informáticos

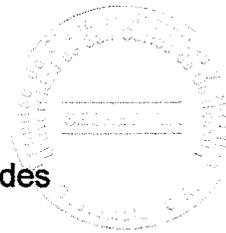
“Derecho protegido, bien garantizado, interés jurídicamente tutelado, objeto jurídico, núcleo del tipo, kernel, objeto de protección.”¹⁷ El bien jurídico tutelado se refiere a aquel valor que se encuentra establecido por la sociedad y que goza de legitimidad por cuanto es fundamental para la vida, la subsistencia, el bienestar del ser humano y por ende de una sociedad.

Se denominan de tal manea, porque constituyen bienes de valor incalculable para la sociedad y que jurídicamente necesitan de una tutela, de una protección, que debe proporcionar el Estado, en ejercicio del poder punitivo. Para profundizar un poco más respecto a ese valor jurídico que ostenta la norma y que es obligación del Estado proteger para bienestar comunal, es importante establecer que más precisa sería la expresión bien jurídico penal por lo que sería deseable que se generalizara su uso.

El bien jurídico tutelado es una garantía para el ciudadano con triple función, la primera considerada como función instrumental, porque permite clasificar los distintos delitos en torno a sus respectivos bienes jurídicos; la segunda función denominada sistemática, puesto que constituye una función interpretativa ya que permite interpretar los varios preceptos a la luz y desde la perspectiva del bien jurídico que viene a tutelar, por tanto es esencial para identificar cual es el bien protegido en cada delito; y la tercera función llamada político-criminal puesto que establece los límites a la acción del legislador al momento de definir conductas como delitos.

Cabe resaltar que el derecho penal ofrece garantías que sirven como límite y obstáculo al uso desmedido del ius puniendi, en cuanto no sometido al ius poenale. El bien jurídico ofrece un límite en cuanto no es posible crear legislativamente delitos carentes de bien jurídico, en cuanto no pueden elevarse a la categoría de delito conductas que

¹⁷ Pavarini, Massimo. **Castigar al enemigo: Criminalidad, exclusión e inseguridad**. Pág. 109.



solamente atentan contra intereses políticos e ideologías, y no contra realidades valoradas socialmente.

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 el Estado se denominan bienes jurídicos.

En el ámbito del derecho penal deberán ser protegidos únicamente bienes jurídicos reconocidos, pero eso no significa que todo bien jurídico haya de ser protegido penalmente, ni tampoco que todo ataque a los bienes jurídicos penalmente protegidos deba necesariamente determinar la intervención del derecho penal, así por ejemplo en el caso que medie el consentimiento del disponente en algunos delitos.

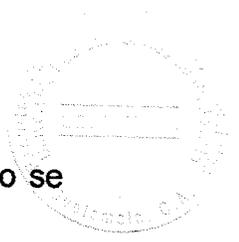
El objeto del bien jurídico encuentra su origen en el interés de la vida, previo al Derecho, que surge de las reacciones sociales, aunque dicho interés vital no se convierte en bien jurídico hasta que es protegido por el derecho, es este el que decide entre los intereses sociales cuáles deben convertirse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

Por su parte: “Los neo-kantianos, que constituyeron la doctrina dominante a partir de los años veinte, buscaron una sustancia material del bien jurídico en una realidad previa al Derecho, pero en lugar de verla en el terreno de los intereses sociales, la situaron en el mundo espiritual subjetivo de los valores culturales.”¹⁸

Sin embargo, una importante dirección acude hoy al concepto, de bien jurídico como bandera de una política criminal liberal, que fija un límite al Derecho Penal, es decir una frontera de lo que puede ser objeto de protección penal.

Es menester, por lo tanto, observar cómo se entiende a la democracia y cuál es la justificación de demandar su protección jurídico penal, pues de otro modo, se llegaría al

¹⁸ Andrade Castro, Jason Alexander y otros. **Lecciones de derecho penal. Parte especial.** Pág. 46.



extremo de la sentencia de Montesquieu: en el sentido de que toda pena que no se deriva de la absoluta necesidad, es tiránica.

3.1. Los bienes jurídicos protegidos en el delito informático

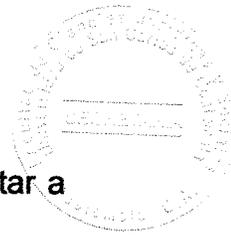
Con relación a los delitos informáticos, se puede expresar que tiende a la protección de los bienes jurídicos, que se realicen desde el punto de vista de los delitos tradicionales, reinterpretando teológicamente los tipos penales ya existentes, para así aliviar los vacíos legales originados por los nuevos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos reinterpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

Y basado en lo anterior se puede decir que los bienes jurídicos protegidos 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.

En el derecho de propiedad, sobre la información que se ve 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 protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo."¹⁹. En conclusión, no se afecta un solo bien jurídico, sino una diversidad de ellos.

¹⁹ Reyes Echandía, Alfonso. **Tipicidad**. Pág. 42.



De esta manera podemos indicar que este tipo de delincuencia, además de afectar a un bien jurídico determinado.

Por lo tanto, se puede decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos, respecto de la figura del fraude informático las acciones de fraude informático afectan a distintas actores, en cada una de las clases se ven afectados por un interés económico, como la recaudación de impuestos, al sistema crediticio y el patrimonio, sobre todo las de los intereses vinculados al funcionamiento de los sistemas informáticos.

Por tanto se puede decir que el nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes, intimidad, seguridad nacional, patrimonio, entre otros, sin embargo han ido adquiriendo importancia nuevos bienes, en tal razón se considera que este tipo de conductas criminales son de carácter netamente pluriofensivo.

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 éste y averiguar la información que más pueda sobre una determinada persona, esto en primer lugar podríamos decir que el bien jurídico lesionado o atacado es el derecho a la intimidad que posee esa persona al ver que su información personal es vista por un tercero extraño que sin autorización ha vulnerado el sistema informático donde dicha información está contenida.

Pero detrás de ese bien jurídico encontramos otro 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 solo importan la afección de bienes jurídicos clásicos.



3.2. Definición y el concepto de delitos informáticos

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 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 víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena.”²⁰

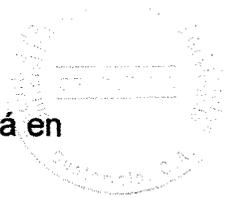
Los delitos informáticos son acciones ilícitas realizadas por computadoras como herramienta de las conductas típicas, ilegales y culpables. Un delito informático es todo comportamiento antijurídico, que está relacionado con procesos automatizados o transferencia de datos. Es considerado como un comportamiento ilícito que conlleva la interrupción y/o modificación de datos ajenos que se encuentran en cualquier dispositivo tecnológico, como computadoras, dispositivos móviles o tabletas electrónicas. Esto con el fin de capturar información sin consentimiento de o de los dueños.

A través de los años el termino delito informático ha evolucionado notablemente, anteriormente contemplaba todos aquellos virus que albergaban en los sistemas operativos de los ordenadores; actualmente se le conoce como delitos informáticos a toda aquella acción antijurídica que ha sido cometida a través de computadoras o dispositivos móviles con el objeto de tener acceso a información restringida y hacer uso de esta para causar daño a una o varias personas.

3.3. Sujetos del delito informático

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o

²⁰ Del Peso Navarro, Emilio y otros. **Peritajes informáticos**. Pág. 162.



varias personas naturales o jurídicas. 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. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo.”²¹

3.3.1. Sujeto activo

Este está constituido por la persona física que con su proceder establece un resultado lesivo para los demás, lesionando o poniendo en peligro el bien jurídicamente tutelado, ahora bien si nos referimos a los delitos informáticos y electrónicos, en este caso son las personas que los cometen, las cuales tienen ciertas características que no tienen el perfil común de los delincuentes, esto quiere decir que estas personas habilidades especiales para el manejo de la informática.

Y generalmente por su estado laboral 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 autores que cometen este tipo 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.

Sin embargo al tener en cuenta las características mencionadas de los individuos que cometen estos delitos, los estudiosos en esta materia los han nombrado como delincuentes de cuello blanco, lo cual quiere decir, que este tipo de conducta no tiene

²¹ Huerta Miranda, Marcelo. **Delitos informáticos**. Pág. 194.



tipificación en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes como la Ley de Patentes y Marcas, ahora Ley de Propiedad Industrial, a la Ley de Derechos de Autor, el mercado negro, el contrabando en las empresas, la revelación de secretos industriales, la evasión fiscal, corrupción de altos funcionarios, etcétera.

Conforme la persona que comete el delito, tiene características similares que poseen ambos delincuentes, se encuentran que el sujeto activo del delito es una persona de cierto estatus económico, su comisión no puede explicarse por pobreza, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por estabilidad emocional.

3.3.2. Sujeto pasivo

En primer término, es necesario recordar que el sujeto pasivo del delito, es la persona física o moral que resiente la actividad delictiva, es el titular del bien jurídicamente tutelado que es dañado o puesto en peligro por la conducta del agente, y en los casos de los delitos informáticos pueden ser individuos particulares, personas morales como sociedades mercantiles, instituciones crediticias, gobiernos etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo que me ocupa y preocupa, es sumamente importante para el estudio de los delitos objeto de este estudio, ya que, mediante él, es posible conocer los diferentes ilícitos que cometen los activos informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos por casualidad, desconociendo el modus operandi de los agentes delictivos.

Debido a lo anterior, ha sido casi imposible conocer la verdadera magnitud de estos ilícitos, 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 por parte de los



funcionarios encargados de la procuración y administración de justicia, para comprender, investigar 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, y 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 procuración, administración e impartición de justicia para atender e investigar estas conductas ilícitas, se avanzaría mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, 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 judiciales para detectar, investigar y prevenir los delitos informáticos.

3.4. Tipos de delitos informáticos

Existen muchos tipos de delitos informáticos, los cuales varían según la diversidad de comportamientos constitutivos de esta modalidad de delitos, los cuales son limitados únicamente por la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas.

La Organización de las Naciones Unidas (ONU) reconoce varios tipos de delitos por lo que le han dado un carácter internacional. A continuación, se describen algunos de ellos.



3.4.1. Los fraudes

- a) Manipulación de los datos de entrada: Este tipo de fraude no requiere poseer mayores conocimientos de informática y lo puede cometer cualquier individuo que tenga acceso a un procesador de datos.

- b) La manipulación de programas: Este no es fácil de descubrir y muchas veces no se advierte debido a que la persona que delinque tiene conocimientos técnicos concretos de informática, consiste en alterar en la forma operativa los programas de las computadoras, para luego incorporar a estos nuevos programas con nuevas funciones. Entre estos el más utilizado es del denominado troyano, el cual hace que el ordenador realice acción de forma paralela a las funciones preestablecidas por el programa que se intenta modificar.

- c) Manipulación de los datos de salida: La manipulación de los datos de salida se realiza constantemente, estableciéndose como un objetivo para alterar el funcionamiento dentro del sistema informático. El más común y acostumbrado es el fraude que se hace en diversos tipos de dispositivos a través de la falsificación de instrucciones para la computadora, gracias a la persona con intelecto informático que permiten la alteración de los procesamientos de datos.

De forma tradicional y acostumbrada estos fraudes se realizaban a través de dispositivos robados; sin embargo, en la actualidad se usan ampliamente utilizando equipos y programas de computadoras especializadas para codificar información electrónica falsa.

- d) Fraude efectuado por manipulación informática: Es la conducta de alterar, modificar u ocultar datos informáticos de manera que, se realicen operaciones de forma incorrecta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener. De esta forma un sujeto puede introducir instrucciones incorrectas en un programa de contabilidad de manera que no anote

cargos a su cuenta corriente por ejemplo, o que desplace a su cuenta bancaria todos los ingresos efectuados un determinado día a las cuentas cuyos números terminen en determinado número, entre otros.

3.4.2. El sabotaje informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

a) Bombas lógicas: Es una especie de bomba de tiempo que debe producir daños posteriormente.

“Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente.

La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.”²²

b) Gusanos: Se fábrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

²² Segunda Cohorte del Doctorado en Seguridad Estratégica. **Seguridad de la Información: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.** Pág. 42.



En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

- c) **Virus informáticos:** Son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

- d) **Ciberterrorismo o terrorismo informático** es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos.

3.4.3. El espionaje informático y el robo o hurto de software

- a) **Fuga de datos:** También conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. “La facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera.”²³

²³ Camacho Losa, Luis. **El delito informático**. Pág. 74.



La forma más sencilla de proteger la información confidencial es la criptografía.

- b) Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

3.4.4. El robo de servicios

Entre estos se encuentran los siguientes:

- a) Hurto del tiempo del computador: El cual consiste en el hurto del tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

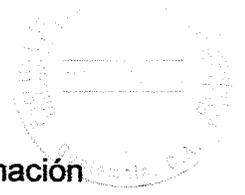
- 
- b) Apropriación de informaciones residuales: Es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado.
 - c) Parasitismo informático: Se alude a las conductas que tienen por objeto el acceso ilícito a los equipos físicos o a los programas informáticos, para utilizarlos en beneficio del delincuente. Suele asociarse a esta figura la de la suplantación de personal que se refiere a toda la tipología de conductas en las que los delincuentes sustituyen a los legítimos usuarios informáticos. Un ejemplo es el referente al uso ilícito de tarjetas de crédito.

3.4.5. El acceso no autorizado a servicios informáticos

- a) Las puertas falsas: Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.
- b) La llave maestra: Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador. Su nombre deriva de un programa utilitario llamado *superzap*, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador.

Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación.

- c) Pinchado de líneas: El cual consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

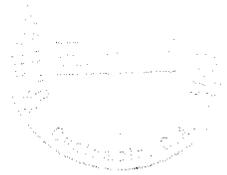


Como se señaló anteriormente el método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la que se envió en origen.

d) Piratas informáticos o hackers: El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación.

El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

CAPÍTULO IV



4. El valor probatorio de los soportes informáticos en el delito de fraude electrónico

Solo mediante la prueba se destruye el estado de inocencia; lo cual permite a las partes utilizar los medios de prueba pertinentes. Lo que pone de manifiesto la importancia que tiene la prueba para la administración de la justicia.

“La palabra prueba viene del latín *probus* bueno, honrado, que te puedes fiar en él. Razón, argumento instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo.”²⁴

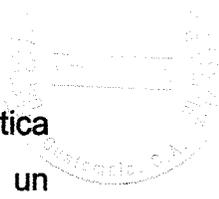
Cuando un individuo se encuentra al momento de cometerse un acto delictivo y que es captado ya sea por su vista, por su audición o por el tacto, genera un recuerdo en su mente, lo cual lo convierte en un medio de prueba.

Se puede indicar que el simple conocimiento no es prueba. Porque para constituirse en tal cosa, debe estar incorporado en un proceso, en forma legal y ser valorada debidamente por un tribunal de sentencia. El hecho de ser valorado judicialmente es lo que hace que el conocimiento de un particular sea prueba; conduciendo a la averiguación y reconstrucción de la verdad real y material sin violentar el debido proceso.

El conocimiento requiere del aspecto procedimental, para ser considerado prueba en sentido propio y jurídico, es decir, cumplir aspectos legales para ser tomada como medio de prueba.

La informática, como teoría de la información; es algo abundante y repetitivo. Su principal herramienta es el computador, el cual hace que la informática sea un

²⁴ Real Academia Española. **Diccionario de la Lengua Española**. Pág. 984.



instrumento liberador de actividades tediosas. En el campo del derecho, la informática jurídica, tiende a ser particularmente liberadora de tareas; pero también, plantea un nuevo campo de estudio, al cual debe de tratársele cuidadosamente; esta materia, plantea numerosas limitaciones; en virtud de que la misma no posee jurisdicción; por lo tanto, debe de investigarse meticulosamente los aspectos que pueden ser sujetos a codificarse en nuevas leyes o a modificarse en las ya existentes.

Como es el caso, del proceso penal guatemalteco y así implementar el uso de la tecnología y establecer la modalidad de incorporarla al mismo. “El término informática, tiene su origen en el idioma francés (1962); informatique es un término formado por dos elementos (acrónimo) información y automatique que significa información automática.”²⁵

La informática, es una ciencia a través de la cual, se puede manejar una cantidad abundante de información en un corto lapso de tiempo, con el uso de un computador y un usuario; por lo tanto, las tareas se realizan de una forma más eficaz y eficiente.

“El surgimiento de las computadoras lo marcó la denominada cuarta generación de computadoras, que abarca los años de 1975 a 1977; la cual influyo en el derecho y permitió reducir el tamaño de los equipos, a través del invento de los microprocesadores y microchips; dando así como resultado, el poder llevar las computadoras a las empresas y no solo a universidades o grandes consorcios, inclusive se instalaron en algunos hogares.”²⁶

“La empresa *International Business Machines* –IBM- desarrolló el hardware más accesible de esa época y Microsoft fundada por Bill Gates y Paul Allen fue la encargada de desarrollar el software. El desarrollo de la tecnología ha hecho posible la reducción de su tamaño y costo. Tras el desarrollo de las primeras computadoras surgió la necesidad de programarlas para que realizaran las tareas deseadas.”²⁷

²⁵ Barrios Osorio, Omar Ricardo. **Derecho e informática aspectos fundamentales.** Pág. 2.

²⁶ **Ibid.** Pág. 4.

²⁷ **Ibid.** Pág. 5.



Con la aparición de los distintos lenguajes, solían aparecer diferentes versiones de un mismo lenguaje; por lo que surgió la necesidad de estandarizarlos para que fueran más universales. Las organizaciones que se encargan de regularizar los lenguajes son: “ANSI Instituto de las Normas Americanas e ISO Organización de Normas Internacionales.”²⁸

A juicio propio, la época de la información ha producido el que haya nuevos bienes y por lo tanto nuevas formas de apropiación de cosas y de propiedades intelectuales entre ellas: bases de datos, programas, transferencia de tecnología, *gadgets*, entre otros.

En la medida que se utilizan más los recursos electrónicos para todas las actividades de cualquier tipo, se ha ido perdiendo el soporte físico en papel, el cual le brindaba a las personas una sensación de seguridad, debido a esto los delincuentes han ideado nuevas formas para vulnerar los contratos o realizar negocios fraudulentos utilizando las deficiencias de los medios electrónicos.

El desarrollo de la informática, ha impactado en el proceso penal; por ejemplo: en lo referente a la citación y notificación, se plantea la posibilidad de efectuarla a través del correo electrónico; así mismo, la ejecución de actos probatorios a través de video conferencia, como la prueba de testigos a distancia. Es más, se habla de alternativa de presentar un proceso *on line*.

La combinación de las formas simbólicas con la reproducción de imágenes y sonido, abre inmensas posibilidades para la celeridad, la concentración y la inmediación; que son principios que sustentan cualquier clase de proceso.

Se puede indicar que la prueba es cualquier elemento que confirme o desvirtúe los supuestos de un delito.

²⁸ *Ibid.*

De lo anterior se puede opinar que la prueba es el medio del cual disponen las partes procesales, para probar la existencia o inexistencia de un hecho o acto controvertido, mediante los procedimientos que señala la ley y no por medios análogos, los cuales servirán de base para que el juzgador fundamente su decisión.



4.1. Hechos jurídicos informáticos como medios probatorios convencionales

Se puede advertir que el dictamen de los peritos, no son propiamente medios de prueba; son tan sólo uno de los muchos elementos integrantes del conjunto de operaciones intelectuales que es necesario se realicen para dictar sentencia. Se analiza el dictamen de expertos como medio para incorporar el medio de prueba informático.

“El sistema para rendir prueba de expertos varía de un derecho procesal a otro; sin embargo, como norma general se establece que cada parte tiene el derecho de designar un experto o perito y proponerlo al juez para que lo nombre y, a su vez, nombrar a un tercero para que vaya número impar en caso de contradicciones entre los dictámenes. En el proceso penal, todo experto tiene la obligación de sentir como tal bajo la responsabilidad de incurrir en multa.”²⁹

“Es por medio de peritos, que se obtiene un dictamen; estos pueden ser llamados para dos propósitos: para la comprobación de un hecho, en el cual, no es necesario que emitan opinión y para la determinación de las cusas y efectos aceptados por las partes; pero con respecto al cual controvierten normalmente desempeñan ambas funciones, para auxiliar al juez; es decir, no solo comprueban el hecho, sino que, también contribuyen a su apreciación. En todo caso, se trata de colaboradores del juez que salvan una imposibilidad física o suplen una insuficiencia técnica del juzgador.”³⁰

Se puede observar que la institución de peritación, se encuentra regulada en el Código Procesal Penal en el Libro primero, disposiciones generales de los Artículos 225 al 243.

²⁹ Ruiz Castillo De Juárez, Crista. **Teoría general del proceso**. Pág. 168.

³⁰ Orellana Donis, Eddy Giovanni. **Derecho procesal civil**. Pág. 154.



En el Artículo 225 establece: “El Ministerio Público o el tribunal podrán ordenar peritación a pedido de parte o de oficio, cuando para obtener, valorar o explicar un elemento de prueba fuere necesario o conveniente poseer conocimientos especiales en alguna ciencia, arte, técnica u oficio...” Según se puede indicar, la pericia o experticia no aporta hechos al proceso, sino que hace una valoración de estos desde el punto de vista de un conocimiento especial, evidentemente, los peritos deben tener el nivel de conocimientos exigidos para su práctica en medios informáticos en otras palabras, debe de tener el título académico facultativo.

“Son diversos los aspectos que se pueden realizar como objeto de la experticia; por ejemplo, se puede pedir la autenticidad del documento electrónico, el momento de emisión, lugar de emisión si ha sido abierto, descifrado del documento, comprobaciones de la firma electrónica, identificación de entrada y salida de usuarios, identificación de re acceso a páginas o sitios etc.; como también aspectos mecánicos; funcionamiento, capacidad identificación de partes y originalidad, etc.”³¹

En el Código Procesal Penal en el Artículo 234 se encuentra establecido lo referente al dictamen: “El dictamen será fundado y contendrá una relación detallada de las operaciones practicadas y sus resultados, las observaciones de las partes o de sus consultores técnicos, y las conclusiones que se formulen respecto de cada tema pericial, de manera clara y precisa. Los peritos podrán dictaminar por separado cuando exista diversidad de opiniones entre ellos. El dictamen se entregará por escrito, firmado y fechado, y oralmente en las audiencias, según lo disponga el tribunal o la autoridad ante quien será ratificado.”

El dictamen, es el resumen de los trabajos y conclusiones de los expertos; uno de los problemas que pueden presentarse con relación al dictamen pericial, estriba en que, las consideraciones o conclusiones de este pueden contemplar puntos no pedidos por la resolución judicial; que determina las bases de la pericia y que no posee el carácter de un medio de prueba, toda vez que los peritos o expertos son únicamente auxiliares

³¹ Rivera Morales, Rodrigo. **Los medios informáticos: Tratamiento procesal**. Pág. 138.



del Juez que por razones de experiencia este último no posee. El medio de prueba documental como medio para incorporar el medio de prueba informático.

Algunos de los inconvenientes que podrían surgir en esta clase de medio de prueba, se puede indicar que es al momento del diligenciamiento, ya que muchos de los litigantes e inclusive el juzgador por falta de conocimiento, no saben cómo tratar dicho medio informático, con lo que se hace evidente la necesidad de instruirlos para no causar daños graves a los medios de prueba, los mismos no son manipulados únicamente por peritos.

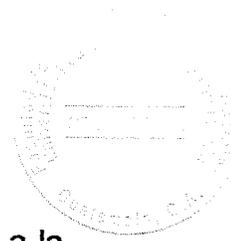
Es claro que debe existir un lineamiento a seguir para el correcto manejo de medios de prueba informáticos. Otros de los problemas son el hecho de no tener el equipo informático para su verificación y las impugnaciones que traería la acción de imprimir el documento electrónico.

4.2. Problemática actual de la prueba electrónica

La obtención de elementos de convicción, establece uno de los aspectos útiles dentro de la consecución de una investigación delictiva, índole que demanda de los fiscales encargados de la recolección, preservación, análisis y presentación de las evidencias digitales; una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente.

Para entender el alcance del tema, Acurio establece varios principios básicos que deben seguirse para la obtención de evidencias digitales y en entornos informáticos entre los que están:

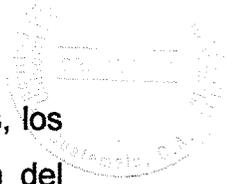
- a) Ninguna acción debe tomarse por parte de la Policía Judicial, la Fiscalía o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de un sistema informático o medios magnéticos, a fin de que esta sea presentada fehacientemente ante un tribunal.



- b) En circunstancias excepcionales una persona competente puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación, siempre que después se explique detalladamente y de manera razonada cual fue la forma en la que se produjo dicho acceso, su justificación y las implicaciones de dichos actos.
- c) Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.
- d) El Fiscal del Caso y/o el oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y el acceso a la información almacenada en el sistema informático. De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios.³²

El recabar evidencia informática, requiere de un formalismo, para poder proteger la autenticidad de esta y siendo la tecnología una nueva forma de delinquir, los investigadores en este caso el Ministerio Público, deben contar no solo con la autorización legal, si no también, con los conocimientos básicos para esta clase de evidencia informática, el Artículo 187 del Código Procesal Penal establece: “Cuando fuere necesario inspeccionar lugares, cosas o personas, porque existen motivos suficientes para sospechar que se encontrarán vestigios del delito, o se presuma que en determinado lugar se oculta el imputado o alguna persona evadida, se procederá a su registro, con autorización judicial.

³² Acurio del Pino, Santiago. **Manual de manejo de evidencias digitales y entornos informáticos.** Pág. 6.



Mediante la inspección se comprobará el estado de las personas, lugares y cosas, los rastros y otros efectos materiales que hubiere de utilidad para la averiguación del hecho o la individualización de los partícipes en él. Se levantará acta que describirá detalladamente lo acontecido y, cuando fuere posible, se recogerán o conservarán los elementos probatorios útiles...”

La ejecución al obtener evidencia informática es delicada, ya que, el solo hecho de apagar o encender un computador; puede dar lugar a ejecutar programas de autoprotección, en el caso de encenderla y si se apaga, puede perderse información volátil. Por lo que se debe tener la debida diligencia con el manejo de estos equipos.

Para garantizar que la evidencia digital sea tenida en cuenta por el juez, se debe describir la propiedad con lujo de detalles, incluyendo sus componentes internos, en el caso del hardware; como instrumento del crimen. Si es imposible, realizar la búsqueda de evidencia digital en el sitio en el cual se encuentra.

Se debe justificar y documentar las razones para el retiro de los elementos que se presume, contienen evidencia, si el elemento es removido del lugar de la búsqueda de evidencia, debe hacerse lo más eficientemente posible, garantizando la obtención de copias a fin de reflejar la información en el estado original.

Mantener la integridad de la evidencia digital a lo largo de un proceso, presenta diferentes problemas, desde el manejo de los tradicionales documentos físicos, equipos de hardware y sus correspondientes archivos de datos; algunos de estos problemas son: la extremada complejidad de las redes de computo, el alarmante tamaño de los archivos de computo tanto de datos como multimedia, así como las bases de datos.

En estos procedimientos, se asume, que se cuenta con los recursos necesarios para almacenar la información relevante a la investigación y mantenerla en custodia sin alteración. En el tema de investigación forense, en materia informática, se debe



generar las pautas de credibilidad y manejo de la información recolectada a fin de impulsar el desarrollo y actualización del proceso penal.

4.3. Régimen jurídico de la prueba electrónica

Se puede afirmar que, dentro de los principios constitucionales que regulan esta institución jurídica, puede ser invocado el principio de seguridad jurídica contenida en el Artículo 2 de la Constitución Política de la República de Guatemala, establece que: “Es deber del Estado garantizarle a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona.”

La Corte de Constitucionalidad Sentencia 17.09.86, Gaceta No.1, expediente No. 12-86, interpreta lo siguiente: “...El principio de seguridad jurídica que consagra el Artículo 2º de la Constitución, consiste en la confianza que tiene el ciudadano, dentro de un Estado de Derecho, hacia el ordenamiento jurídico; es decir, hacia el conjunto de leyes que garantizan sus seguridades en el ejercicio de sus facultades legales, deben actuar observando dicho principio, respetando las leyes vigente, principalmente la ley fundamental...”

Otro principio que es importante dentro de este punto, es el derecho de defensa el cual se encuentra establecido en el siguiente Artículo de la Constitución Política de la República de Guatemala: “Artículo 12. La defensa de la persona y sus derechos son inviolables. Nadie podrá ser condenado, ni privado de sus derechos, sin haber sido citado, oído y vencido en proceso legal ante juez o tribunal competente y preestablecido.

Ninguna persona puede ser juzgada por Tribunales Especiales o secretos, ni por procedimientos que no estén preestablecidos legalmente.”

De este principio constitucional se extrae que, en el proceso penal los medios de prueba son apreciados por un tribunal de sentencia en su fase de juicio o debate, el



cual realizan haciendo uso del sistema de la sana crítica razonada. Es en esta etapa del proceso, que salen a la luz los conflictos que trae la tecnología y la apreciación que el cuerpo colegiado le da al mismo y con el cual surgen un sin número de impugnaciones; ya que los sujetos procesales muchas veces no saben cómo incorporar material o evidencia en formato digital.

Por último, se señala el Artículo 14 constitucional el cual establece: “Toda persona es inocente mientras no se le haya declarado responsable judicialmente, en sentencia debidamente ejecutoriada.

El detenido, el ofendido, el Ministerio Público y los abogados que hayan sido designados por los interesados, en forma verbal o escrita, tienen derecho de conocer, personalmente, todas las actuaciones, documentos y diligencias penales, sin reserva alguna y en forma inmediata.”

La Corte de Constitucional se pronuncia al respecto y dispone: “...el Artículo 14 constitucional reconoce, en su primer párrafo, el derecho fundamental de toda persona a la que se impute la comisión de hechos, acto u omisiones ilícitas o indebidas a que se presuma su inocencia, y hasta en tanto no se le haya declarado responsable judicialmente en sentencia debidamente ejecutoriada. Se trata, entonces, de una presunción *iuris tantum*.”

En otro fallo la Corte de Constitucionalidad establece: “...una presunción *iuris tantum*, dirigida a garantizar al sindicado que no podrá sufrir pena o sanción que no tenga fundamento en prueba pertinente, valorada por un tribunal con eficacia suficiente para destruir la presunción y basar un fallo razonable de responsabilidad, porque, en caso contrario, el principio constitucional enunciado prevalecerá en su favor...”

Este principio es indiscutible, deviene de la génesis de presunción de inocencia, la duda en el proceso penal radia en que no se ha logrado establecer fidedignamente, ni la verdad, ni el error; respecto de la culpabilidad del procesado, a causa de la

insuficiencia de los elementos probatorios; por consiguiente, el hecho de que un dictamen de expertos o peritaje sea tomado como una ayuda hacia el juez y no como medio de prueba en sí y si fuere tomada como medio de prueba se cuestiona el hecho de la apreciación que el tribunal le otorga.

- a) Regulación legal Ley de Derechos de Autor y Derechos Conexos Decreto 33-98: El Decreto 33-98 dio vida a este cuerpo normativo que tiene como fin proteger a los artistas, intérpretes o ejecutores y tutela los derechos de los mismos.

En el segundo considerando señala: "...Que el desarrollo de nuevas tecnologías para la difusión de las obras ha permitido nuevas modalidades de defraudación de los derechos de propiedad intelectual, por lo que es necesario que el régimen jurídico que proteja los derechos de los Autores, los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, contenga normas que permitan que los citados derechos sean real y efectivamente reconocidos y protegidos de acuerdo con las exigencias actuales, para estimular así la creatividad intelectual y la difusión de las obras creadas por los autores..."

En lo referente a la informática, este cuerpo legal tiene un apartado en su sección segunda que desglosa lo relativo a las nuevas tecnologías y su forma de protección y van del Artículo 30 al 35 y establecen lo siguiente:

Artículo 30. Los programas de ordenador se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o código objeto y cualquiera que sea su forma o modo de expresión...

Artículo 31... no es aplicable a los arrendamientos cuyo objeto esencial no sea el del programa de ordenador en sí. La colocación en el mercado del original o copias autorizadas de un programa de ordenador, con el consentimiento del titular...

Artículo 32. La reproducción de un programa de ordenador, incluso para uso personal, exigirá la autorización del titular de los derechos, con excepción de la copia que se haga con el fin exclusivo de sustituir la copia legítimamente adquirida, cuando ésta ya no pueda utilizarse por daño o pérdida...

Artículo 33. Es lícita la introducción de un programa en la memoria interna del ordenador que sirva únicamente para efectos de la utilización del programa por parte del usuario. No es lícito el aprovechamiento del programa por varias personas mediante la instalación de redes, estaciones de trabajo u otro procedimiento análogo, sin el consentimiento del titular de los derechos.

Artículo 34. Los autores o titulares de un programa de ordenador podrán autorizar las modificaciones necesarias para la correcta utilización de los programas. No constituye modificación la adaptación de un programa realizada por el usuario, para su uso exclusivo, cuando la modificación sea necesaria para la utilización de ese programa o para un mejor aprovechamiento de éste.

Artículo 35. Las compilaciones o bases de datos sean que fueren legibles en máquina o en cualquier otra forma, se consideran como colecciones de obras para efectos de su protección de conformidad con esta ley..."

Un programa de computador, permite la realización de diversas tareas que van desde el funcionamiento interno de una computadora, sistema operativo, hasta la obtención de un objetivo específico programa de aplicación. Sin embargo, existen otras formas de programas como: los compiladores, traductores, ensambladores, sistemas organizacionales de multiproceso y sistemas controladores de multiproceso entre otros.

Por lo tanto, los propósitos de los programas de computación, son muy variados y comparten una característica común, permiten al usuario la realización de su trabajo con mucha mayor rapidez, orden y efectividad; que sin estos y son creados ya sea por una o varias personas en conjunto.



Actualmente, los programas de ordenador representan elementos muy importantes de competitividad y desarrollo; con lo cual se considera al software como la parte más valiosa de la informática, por los altos costos a que asciende su desarrollo y los recursos humanos, técnicos, económicos y materiales que se requieren.

No obstante, lo anterior, resulta muy difícil recuperar las sumas que se llegan a invertir en este campo. Situación que se agrava significativamente, en virtud del problema de la piratería de los programas, la falta de medidas de control y protección adecuadas; sumándosele, el hecho de que los medios por los que se puede defender o hacer ver una situación ilícita, no tiene el mismo alcance o apreciación que los ya regulados.

b) Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Decreto 47-2008: Esta ley tiene como objeto, equiparar la firma digital a la firma holográfica, para asuntos relacionados en actos jurídicos públicos o privados; ya sea a nivel nacional o internacional. En el segundo considerando de dicho cuerpo normativo establece: “Que la inmersión masiva de la tecnología en nuestra sociedad es una realidad que no podemos ignorar y por ende se debe revisar los conceptos y visiones tradicionales del mundo físico para adaptarlos al actual contexto del mundo digital.”

La ley citada, ya establece algunas figuras jurídicas referentes a la informática y les da el reconocimiento probatorio siempre que el sujeto que adopta dicho acto jurídico así lo manifieste.

“Artículo 5. Reconocimiento jurídico de las comunicaciones electrónicas. No se negarán efectos jurídicos, validez o fuerza obligatoria a una comunicación o a un contrato por la sola razón de que esa comunicación o ese contrato estén en forma de comunicación electrónica.



Nada de lo dispuesto en esta ley hará que una parte esté obligada a utilizar o a aceptar información en forma de comunicación electrónica, pero su conformidad al respecto podrá inferirse de su conducta. Así mismo, nada de lo dispuesto en la presente ley obligará a que una comunicación o un contrato tengan que hacerse o probarse de alguna forma particular.”

“Artículo 11. Admisibilidad y fuerza probatoria de las comunicaciones electrónicas. Las comunicaciones electrónicas serán admisibles como medios de prueba.

No se negará eficacia, validez o fuerza obligatoria y probatoria en toda actuación administrativa, judicial o privada a todo tipo de información en forma de comunicación electrónica, por el sólo hecho que se trate de una comunicación electrónica, ni en razón de no haber sido presentado en su forma original.”

El Artículo 11 claramente muestra que los distintos medios de comunicación electrónica tienen fuerza probatoria y los contempla como un medio de prueba; siempre y cuando el mismo contenga la firma digital avanzada, la que es otorgada por una entidad certificadora autorizada por el Estado de Guatemala, garantizando que la clave es la que corresponde al emisor y con esto se autentica el origen del mensaje.

“Artículo 12. Criterio para valorar probatoriamente una comunicación electrónica. Toda información presentada en forma de comunicación electrónica, gozará de la debida fuerza probatoria de conformidad con los criterios reconocidos por la legislación para la apreciación de la prueba.

Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje; la fiabilidad de la forma en la que se haya conservado la integridad de la información; la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.”

De este Artículo se infiere que, tanto la cadena de custodia como las etapas de la prueba deben de realizarse de forma tal que no se altere su contenido; por lo tanto,

desde esta ley, sientan las bases o al menos algunos lineamientos a seguir para la manipulación de evidencia digital.



“Artículo 33. Efectos jurídicos de una firma electrónica o firma electrónica avanzada. La firma electrónica o la firma electrónica avanzada, la cual podrá estar certificada por una entidad prestadora de servicios de certificación, que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta, según los criterios de apreciación establecidos en las normas procesales.”

En lo referente a la firma electrónica avanzada, el Banco de Guatemala en su Reglamento del Sistema de Liquidación Bruta establece los requerimientos.

4.4. Recolección y valoración de la prueba electrónica

Se debe señalar que, con el cambio, del sistema inquisitivo al nuevo sistema acusatorio, el proceso penal guatemalteco actualizó muchos de sus métodos o procedimientos; con los cuales, introdujo el uso de la tecnología, aunque solo lo aplicó a determinadas fases administrativas del proceso, esto ya garantiza un cambio y actualización de los procesos a las nuevas tecnologías y avances en el mundo, que cada día se hace más dependiente de la informática.

Sin embargo, al ser la informática tan vasta, compleja y nueva para el proceso penal; los jueces y los fiscales, así como la defensa, se ven en la necesidad de acomodar o encajar las nuevas evidencias a los medios de prueba establecidos. Por lo que se debe de encasillar al medio de prueba informático dentro de lo ya establecido.

Siendo este un medio de prueba diferente, relativamente nuevo y con características que lo hacen desigual de los demás medios de prueba, resulta útil y necesario para el proceso penal, tratarlo con la debida diligencia e importancia que conlleva. Por lo que

aislarlo o acomodarlo a un determinado medio de prueba, como la documental, deja fuera muchos aspectos como la presentación de la misma o su incorporación al proceso.

Como se estableció anteriormente, al obtener evidencia y requerir dictamen del peritaje, este se puede aludir como un medio de auxilio hacia el juez y no, así como un medio de prueba.

Respecto a la valoración de los medios de prueba, el Código Procesal Penal establece en el Artículo 186: "Todo elemento de prueba, para ser valorado, debe haber sido obtenido por un procedimiento permitido e incorporado al proceso conforme a las disposiciones de este Código."

De lo citado se observa, que existe una violación al mismo, puesto que, el medio de prueba informático, como se señaló anteriormente, es incorporado al proceso por medios análogos o presentados de forma tal que pueden ser impugnables o sencillamente no ser admitidos como medios de prueba; por lo cual debe analizarse lo fundamentado en el Artículo 14 del Código Procesal Penal: "El procesado debe ser tratado como inocente durante el procedimiento, hasta tanto una sentencia firme lo declare responsable y le imponga una pena o una medida de seguridad y corrección.

Las disposiciones de esta ley que restringen la libertad del imputado o que limitan el ejercicio de sus facultades serán interpretadas restrictivamente; en esta materia, la interpretación extensiva y la analogía quedan prohibidas, mientras no favorezcan la libertad o el ejercicio de sus facultades.

Las únicas medidas de coerción posibles contra el imputado son las que este Código autoriza, tendrán carácter de excepcionales y serán proporcionales a la pena o medida de seguridad y corrección que se espera del procedimiento, con estricta sujeción a las disposiciones pertinente. La duda favorece al imputado."



En virtud de lo anterior, se puede señalar que, la incorporación de un medio de prueba informático al proceso por medios análogos o interpretados de manera extensiva, son prohibidas por la ley; pero también, debe resaltarse el hecho, de que el juez encargado de admitir los medios de prueba ofrecidos al proceso, al momento de tener duda racional sobre los elementos objetivos y subjetivos que integran el tipo, debe aplicar el principio *indubio pro reo*, este principio sólo entra en juego cuando, efectivamente practicada la prueba, esta no ha desvirtuado la presunción de inocencia.

“Sin embargo, el principio in dubio pro reo evidencia que existe una prueba, ya sea de cargo y de descargo, según sea el caso, aunque esto no sea suficiente para convencer a quien se encuentre encargado de juzgar el caso en cuestión; si en el caso existieren dudas queda absuelto el sujeto. En ningún caso se debe de entender que sea un derecho del imputado la duda de un tribunal, si llegar a existir una duda debe de ser absuelto.

Anteriormente se afirmaba que, el principio in dubio pro reo, no se podía alegar en un recurso; sin embargo, cabe considerarlo dentro de la presunción de inocencia, pudiendo invocarse en casación si resulta acreditado que el tribunal condenó a pesar de su duda. Pero, no procede invocarlo para exigir al tribunal que dude, sino que sólo es posible su invocación cuando el tribunal ha planteado o reconocido la existencia de dudas en la valoración de la prueba sobre los hechos y los ha resuelto en contra del acusado.

El párrafo final del Artículo 343 del Código Procesal Penal establece: “...El juez resolverá inmediatamente y admitirá la prueba pertinente y rechazará la que fuere abundante, innecesaria, impertinente o ilegal.”

Es en esta fase procesal, es decir, en la segunda audiencia de la etapa intermedia que el juez, resuelve admitir o no los medios de prueba ofrecidos por el Ministerio Público, la defensa y demás sujetos procesales.



La no admisión de un medio de prueba, debe ser protestada en el momento oportuno para no transgredir el principio de preclusión procesal y dar lugar a arbitrariedades, como la inacción de los sujetos procesales. Mediante previa protesta formal, una ulterior impugnación, por afectar el rechazo de la petición probatoria al derecho a la tutela judicial efectiva; este recurso, igualmente, debería contemplarse para el supuesto de que la prueba acordada de oficio alterase sustancialmente la debida imparcialidad del juzgador.



CONCLUSIÓN DISCURSIVA

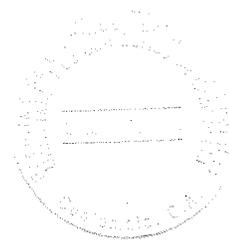
La comisión de delitos emergentes en la internet es un problema que afecta a la sociedad mundialmente, tanto niños como adultos, no importando edad ni género, se ven vulnerables a caer en las redes de algún delito o crimen cibernético, por lo que es necesaria la capacidad del perito o investigador en la escena del crimen y el correcto procedimiento en la misma para lograr la resolución óptima del caso.

La generalidad de los delitos informáticos en Guatemala únicamente provoca la ignorancia de la sociedad en el tema y es imperativa la existencia de normas que especifiquen los hechos o actos que se consideran delitos informáticos para un mejor control del mismo.

Guatemala es uno de los muchos países que se encuentra atrasado en lo que a la regulación de la tecnología respecta, siendo el uso de la misma como un medio comúnmente utilizado para la comisión de los delitos es por ello que es necesaria la regulación de términos como internet, redes sociales, sitios de web ilegales, entre otros. Pues vivimos en un mundo tecnológico y por ello Guatemala debe de apegarse a este nuevo mundo, para combatir de forma eficiente el ciber-crimen, que surge de las redes sociales.

Es indispensable y necesaria la correcta instrucción para agentes de investigación de crímenes informáticos, ya que son estos quienes tienen bajo su control los elementos o indicios que pueden ser considerados como evidencias y pruebas durante el proceso penal, por lo que la manipulación de estos debe resguardar su contenido.

La evidencia digital debe ser meticulosamente recaudada y procesada para luego ser presentada en la corte cumpliendo los requisitos de admisibilidad. Es esencial garantizar la veracidad de la evidencia digital durante el proceso de investigación, y para ello es indispensable contar con los conocimientos y habilidades especiales en la recaudación, embalaje y manipulación de este tipo de evidencia.





BIBLIOGRAFÍA

- ACURIO DEL PINO, Santiago. **Manual de manejo de evidencias digitales y entornos informáticos**. Quito, Ecuador: Ed. Pontificia Universidad Católica del Ecuador, 2000.
- ANDRADE CASTRO, Jason Alexánder y otros. **Lecciones de derecho penal. Parte especial**. 3ª. ed., Bogotá, Colombia: Ed. Universidad Externado de Colombia, 2019.
- BARRIOS OSORIO, Omar Ricardo. **Derecho e informática aspectos fundamentales**. Guatemala, Guatemala: Ed. Mayte, 2007.
- CAMACHO LOSA, Luis. **El delito informático**. Madrid, España: Ed. L. Camacho Losa, 1987.
- Corte de Constitucionalidad. **Gaceta No. 1, Expediente 12-86, Sentencia 17-09-86**. Guatemala, Guatemala: Corte de Constitucionalidad, 1986.
- Corte de Constitucionalidad. **Gaceta No. 47, Expediente 1011-97, Sentencia 31-03-98**. Guatemala, Guatemala: Corte de Constitucionalidad, 1998.
- Corte de Constitucionalidad. **Gaceta No.60, Expediente No.288-00, Sentencia 02-05-11**. Guatemala, Guatemala: Corte de Constitucionalidad, 2011.
- DEL PESO NAVARRO, Emilio y otros. **Peritajes informáticos**. 2ª. ed., Madrid, España: Ed. Díaz de Santos, 2001.
- DOMÍNGUEZ, Mario. **Temas de derecho probatorio penal**. Guatemala, Guatemala: Ed. Universidad de San Carlos de Guatemala, 2011.
- ELMASRI, Ramez y Shamkant B. Navathe. **Fundamentos de base de datos**. Trad. Verónica Canivell Castillo y Beatriz Galán Espiga, 3ª. ed., Madrid, España: Ed. Pearson Educación, 2000.
- GUEVARA GAMBOA, Félix Antonio. **Computación paso a paso**. Lima, Perú: Ed. Félix Guevara, 2013.
- HERNÁNDEZ VILLAREAL, Gabriel. **Actualidad y futuro del derecho procesal: Principios, reglas, y pruebas**. Bogotá, Colombia: Ed. Universidad del Rosario, 2010.
- HUERTA MIRANDA, Marcelo. **Delitos informáticos**. 2ª. ed., Santiago, Chile: Ed. Jurídica Cono Sur, 1996.
- LÓPEZ ALDEA, Eugenio. **Arduino. Guía práctica de fundamentos y simulación**. Madrid, España: Ed. RA-MA Editorial, 2016.



- MARÍ SÁEZ, Víctor Manuel. **Globalización, nuevas tecnologías y comunicación**. 2ª ed., Madrid, España: Ed. Ediciones de la Torre, 2002.
- MIRES, Fernando. **La revolución que nadie soñó o la otra posmodernidad**. Caracas, Venezuela: Ed. Nueva Sociedad, 1996.
- ORELLANA DONIS, Eddy Giovanni. **Derecho procesal civil**. Guatemala, Guatemala: Ed. Vásquez, 2006.
- OSSORIO, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**. 33ª. ed., Buenos Aires, Argentina: Ed. Heliasta S.R.L., 2006.
- OVIEDO SILVA, Lino César. **La injusticia de la justicia**. Asunción, Paraguay: Ed. Unión Nacional de Colorados Éticos, 2001.
- PAVARINI, Massimo. **Castigar al enemigo: Criminalidad, exclusión e inseguridad**. Quito, Ecuador: Ed. FLACSO, 2009.
- RAMOS MARTÍN, Alicia. **Sistemas gestores de bases de datos. Grado superior**. Madrid, España: Ed. McGraw-Hill Interamericana, 2006.
- Real Academia Española. **Diccionario de la Lengua Española**. 22ª. ed., Madrid, España: Ed. Espasa Calpe, 2007.
- REYES ECHANDÍA, Alfonso. **Tipicidad**. 6ª. ed., Bogotá, Colombia: Ed. Temis, 1997.
- RIVERA MORALES, Rodrigo. **Los medios informáticos: Tratamiento procesal**. Bogotá, Colombia: Ed. Pontificia Universidad Javeriana, 2008
- RUIZ CASTILLO DE JUÁREZ, Crista. **Teoría general del proceso**. Guatemala, Guatemala: Ed. Praxis, 2015.
- Segunda Cohorte del Doctorado en Seguridad Estratégica. **Seguridad de la Información: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica**. Guatemala, Guatemala: Ed. Universidad de San Carlos de Guatemala, 2014.
- SOLÍS, José Antonio. **Historia de las cosas**. La Coruña, España: Ed. Cien Editores, S.L., 2008.
- SPAGNI DE BARLETTA, Beatriz; Augusto Dante Bergagna; Gabriela Roldán y Mirta López de Abdala. **Apéndice de estadística básica**. Santa Fe, Argentina: Ed. Universidad Nacional del Litoral, 2005.



Legislación:

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

Código Procesal Penal. Decreto 51-92 y sus reformas. Congreso de la República de Guatemala, 1992.

Ley de Derecho de Autor y Derechos Conexos. Decreto 33-98. Congreso de la República de Guatemala, 1998.

Ley de Emisión del Pensamiento. Decreto 9. Asamblea Nacional Constituyente de la República de Guatemala, 1966.

Ley del Impuesto al Valor Agregado (IVA). Decreto 27-92. Congreso de la República de Guatemala, 1992.

Ley para el Reconocimiento de telecomunicaciones y firmas electrónicas. Decreto 47-2008. Congreso de la República de Guatemala, 2008.

Registro electrónico de notarios. Acuerdo Gubernativo 041/002. Corte Suprema de Justicia, Guatemala, 2002.