UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

CENTRO UNIVERSITARIO DE OCCIDENTE

DEPARTAMENTO DE ESTUDIOS DE POSTGRADO

MAESTRÍA EN DERECHO PENAL

“EL DILIGENCIAMIENTO, OFRECIMIENTO Y VALORACION DE LA PRUEBA ELECTRONICA Y DIGITAL EN CASOS DE DELINCUENCIA ORGANIZADA”

Por:

Lic. Julio Estuardo Santos Velásquez

Quetzaltenango, febrero 2022.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

CENTRO UNIVERSITARIO DE OCCIDENTE

DEPARTAMENTO DE ESTUDIOS DE POSTGRADO

MAESTRÍA EN DERECHO PENAL

TESIS:

"EL DILIGENCIAMIENTO, OFRECIMIENTO Y VALORACION DE LA PRUEBA ELECTRONICA Y DIGITAL EN CASOS DE DELINCUENCIA ORGANIZADA"

Presentada al Honorable Consejo Académico

de Postgrados del Centro Universitario de Occidente,

Universidad de San Carlos de Guatemala

Por:

Julio Estuardo Santos Velásquez

Previo a conferírsele el grado académico de:

Maestro en Derecho Penal

Quetzaltenango, febrero 2022.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

CENTRO UNIVERSITARIO DE OCCIDENTE

DEPARTAMENTO DE ESTUDIOS DE POSTGRADO

AUTORIDADES

RECTOR MAGNIFICO	M A. Pablo Ernesto Oliva Soto
SECRETARIA GENERAL	Inga. Marcia Ivónne Véliz Vargas

CONSEJO DIRECTIVO

DIRECTORA GENERAL DEL CUNOC	Dr**.** César Haroldo Milián Requena.
SECRETARIO ADMINISTRATIVO	MSc. José Edmundo Maldonado Mazariegos.

REPRESENTANTE DE CATEDRATICOS

M Sc. Freddy de Jesús Rodríguez

REPRESENTANTES DE LOS EGRESADOS DEL CUNOC

Lic. Víctor Lawrence Díaz Herrera

REPRESENTANTES DE ESTUDIANTES

Br. Aleyda Trinidad de León Paxtor

Br. Romeo Danilo Calderón

DIRECTOR DEL DEPARTAMENTO DE POSTGRADOS

M Sc. Walter Valdemar Poroj Sacor.

TRIBUNAL QUE PRACTICO EL EXAMEN PRIVADO DE TESIS

Metodólogo: **M Sc. Edgar Benito Rivera**.

Examinador: **M Sc**. **Jorge Luis Cano.**

Examinador: **M Sc. José Ignacio Camey**.

Examinador: **M Sc. Milton Estrada Morales**.

Coordinador y secretario: **Dr. Carlos Calderón Paz**.

Asesora de Tesis:

Dra. Sonia Doradea Guerra de Mejía.

NOTA: Únicamente el autor es responsable de las doctrinas y opiniones sustentadas en la presente tesis (artículo 31 del Reglamento de Exámenes Técnicos y Profesionales del Centro Universitario de Occidente de la Universidad de San Carlos de Guatemala)

.

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala
Centro Universitario de Occidente
Departamento de Estudios de Postgrado

ORDEN DE IMPRESIÓN POST-CUNOC-077-2021

El Infrascrito Director del Departamento de Estudios de Postgrado del Centro Universitario de Occidente de la Universidad de San Carlos de Guatemala, luego de tener a la vista el dictamen correspondiente del asesor y la certificación del acta de examen privado No. 49-2021 de fecha 01 de octubre de 2021, suscrita por los Miembros del Tribunal Examinador designados para realizar Examen Privado de la Tesis Titulada **"El diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada"** Presentada por él (la) maestrante **Julio Estuardo Santos Velásquez** Registro Académico **No. 200430392,** previo a conferírsele el título de **Maestro(a) en Derecho Penal,** autoriza la impresión de la misma.

Quetzaltenango, Noviembre 2021

IMPRIMASE

"ID Y ENSEÑAD A TODOS"

Dr. Percy Iván Aguilar Argueta
Director Postgrados CUNOC

Guatemala, 15 de abril de 2021.

Doctor:
Carlos Abraham Calderón Paz
Coordinador de Maestrías y Doctorado de
Ciencias Jurídicas y Sociales
Centro Universitario de Occidente, CUNOC
Universidad de San Carlos de Guatemala.

Estimado Doctor:

De manera atenta y respetuosa me dirijo a usted, deseándole éxitos en sus labores, me permito informarle que he finalizado con mi labor como asesora de la tesis del Licenciado Julio Estuardo Santos Velásquez, por lo que procedo a emitir DICTAMEN FAVORABLE.

De conformidad con el Acta de Postgrado 013-2018 de fecha dos de octubre de 2018 suscrita por el Consejo Académico de Postgrados del Centro Universitario de Occidente, fui nombrada como asesora de la tesis titulada "EL DILIGENCIAMIENTO, OFRECIMIENTO Y VALORACIÓN DE LA PRUEBA ELECTRÓNICA Y DIGITAL EN CASOS DE DELINCUENCIA ORGANIZADA".

Por lo que habiendo concluido con el trabajo de revisión el cual reúne los requerimientos y sugerencias efectuadas como asesora, rindo el Dictamen Favorable, porque cumple la tesis satisfactoriamente los objetivos trazados tanto en el contenido como en los aspectos fundamentales de la misma, se cotejó minuciosamente con el plan inicial, cabe destacar la importancia de la investigación pues conlleva un análisis técnico y jurídico de los beneficios que ofrecen los avances de la tecnología en el proceso penal.

Por lo anterior, me permito concluir que el trabajo realizado por el Licenciado Julio Estuardo Santos Velásquez, llena los requisitos establecidos por el Artículo 14 del Normativo de Tesis de Maestría y Doctorado, recomendando que se prosiga con el trámite de rigor.

Sin otro particular, me suscribo de usted.

Dra. Sonia Doradea Guerra de Mejia
Tutora
Teléfono: 58745454

Sonia Doradea de Mejía
Abogado y Notario
Colegiado: 4,188

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala
Centro Universitario de Occidente
Departamento de Estudios de Postgrado

EL INFRASCRITO DIRECTOR DEL DEPARTAMENTO DE ESTUDIOS DE POSTGRADO DEL CENTRO UNIVERSITARIO DE OCCIDENTE DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA.

CERTIFICA:

Que ha tenido a la vista el libro de Actas de Exámenes Privados del Departamento de Estudios de Postgrado del Centro Universitario de Occidente en el que se encuentra el acta No. 49-2021 la que literalmente dice:- - - - - - - - - - - - - - - - - -

En la ciudad de Quetzaltenango, siendo las diecisiete horas del día viernes uno de octubre del año dos mil veintiuno, reunidos en la plataforma virtual Meet, el Honorable Tribunal Examinador, integrado por los siguientes profesionales: **Experto:** M Sc. Milton Estrada Morales, con registro de personal No. 20200204; **Experto:** M Sc. José Ignacio Camey, con registro de personal No. 20160894; **Experto:** Jorge Luis Cano, con registro de personal No. 20200361; **Experto Metodólogo:** M Sc. Edgar Benito Rivera, con registro de personal No. 15972; **Secretario que certifica:** Dr. Carlos Calderón Paz, con registro de personal No. 930388; con objeto de practicar el **Examen Privado** de la Maestría en **Derecho Penal** en el grado académico de **Maestro(a) Ciencias** de él (la) Licenciado(a) **Julio Estuardo Santos Velásquez** identificado(a) con el registro Académico No. **200430392** procediéndose de la siguiente manera:- - - - - - - - - - - - - - - -
PRIMERO: El (La) sustentante practicó la evaluación oral correspondiente, de conformidad con el Reglamento respectivo.- -
SEGUNDO: Después de efectuadas las preguntas necesarias, los miembros del tribunal examinador procedieron a la deliberación, habiendo sido el dictamen **FAVORABLE** -
TERCERO: En consecuencia él (la) sustentante **APROBO** examen privado de tesis Con mención honorifica de CUM LAUDE para otorgarle el título profesional de **MAESTRO(A) EN DERECHO PENAL** -
CUARTO: No habiendo más que hacer constar, se da por finalizada la presente, en el mismo lugar y fecha una hora con treinta minutos después de su inicio, firmando de conformidad, los que en ella intervinieron.- - - - - - - - - - - - - - - - - - - -

Y para los usos legales que a él (la) interesado(a) convengan, se extiende, firma y sella la presente CERTIFICACIÓN en una hoja membretada del Departamento de Estudios de Postgrado del Centro Universitario de Occidente de la Universidad de San Carlos de Guatemala a los dieciséis días del mes de noviembre del año dos mil veintiuno. -

"ID Y ENSEÑAD A TODOS"

Certifica: Vo. Bo.

Yomara Yamileth Rodas de León
Secretaria de Postgrados

Dr. Percy Iván Aguilar Argueta
Director de Postgrados

DEDICATORIA.

A DIOS: Alfa y Omega, Señor y Padre mío, tu bondad y misericordia es grande y de todo lo que poseo, llegaré a conocer y poner en práctica tu eres el artífice y alfarero, gracias por tu infinito amor y por abrir puertas justas, mi corazón en ti sigue confiando. Dadme la oportunidad de compartir con mi prójimo el don de Ciencia que se me ha conferido en forma perpetua en mis proyectos, acompañado siempre del fruto de la luz con bondad, justicia y verdad. Te suplico para que sigas siendo mi torre fuerte ante las adversidades y otórgame tu bendición y sabiduría para luchar por las causas justas.

A DULCE VIRGEN MARIA: Madre Santa que intercedes en mis plegarias, me das alivio ante la adversidad y que con tu manto bendito me has dado protección y auxilio en mi diario caminar; gracias por ser mi refugio de amor santo. Sigue intercediendo por mí y con el amparo de San Miguel Arcángel te suplico que él guíe, libre y acompañe mis batallas. Gracias por tu infinita bondad y atención a tu hijo.

A MI FAMILIA: Especialmente a mis padres Julio César y Norma Angélica, por ser pilar fundamental de mis logros, quienes han sido inspiración viva para convertir mis sueños en metas, quienes han estado presentes para seguir forjando mi carrera profesional; su presencia en los momentos difíciles ha sido vital para seguir adelante con mis metas, con responsabilidad, entrega, humildad y perseverancia. Todo esto es por ustedes, por lo mucho que valen y lo importantes que son en mi vida, porque los amo; admiro su fortaleza, confianza y apoyo, por lo que han hecho de mí. Dedicatoria especial a cuatro torrecitas especiales: Julián, André, Jostyn y Pablito, gracias por sus detalles y ocurrencias.

A MIS AMIGOS: quienes me han brindado su amistad y atención incondicional, gracias por permitirme ser parte de su vida.

A MI ASESORA DE TESIS: Dra. Sonia Guerra, por su atenta y amable atención, por el tiempo que empleó en orientarme en este trabajo de investigación y en la memoria del respetable Dr. Bonerge Mejía (Q.E.P.D) mi más sincera admiración y respeto.

A MI MADRINA DE GRADUACION: Dra. Brenda Dery Muñoz Sánchez de Molina, por aceptar y compartir este momento especial y demostrarme con su ejemplo, carisma y trayectoria la forma en que debe ser desarrollada y dignificada tan valiosa profesión.

AL OBSERVATORIO GUATEMALTECO DE DELITOS INFORMATICOS: Con especial cariño a José Leonett, profesional de la informática forense y Ciberseguridad, por ser mi mentor y guía, por darme la oportunidad de formarme como Perito Forense Digital, agradecido por los espacios de preparación en el área de la informática forense y disciplinas afines, con cariño especial a mis compañeros Peritos Forenses Digitales de Guatemala y Latinoamérica.

A REVISTA JURIDICA: Con especial cariño a su fundador Mayco Maldonado por brindarme los espacios y así compartir diferentes temas académicos, gracias por la deferencia y la confianza.

A MI QUERIDA ALMA MÁTER: A la Tricentenaria Universidad de San Carlos de Guatemala, especialmente al Centro Universitario de Occidente, por darme la oportunidad de seguir formándome en sus aulas, con mucho orgullo y cariño.

A MI QUERIDA XELAJÚ (QUETZALTENANGO): Mi tierra, mi ciudad de los altos, que me vio nacer y sigue siendo el lugar donde guardo los mejores recuerdos de mi trayectoria profesional y personal.

INDICE.

A. RESUMEN EJECUTIVO.

El trabajo de investigación que a continuación se presenta fue desarrollado bajo un enfoque criminalístico, técnico, jurídico y social que desarrolla temas sobre la forma en que es diligenciada, ofrecida y valorada la prueba electrónica y digital en el proceso penal guatemalteco en el contexto básico de la delincuencia común y posteriormente en el escenario de la delincuencia organizada. Se desarrollan temas hasta ahora son poco estudiados en el escenario jurídico guatemalteco, no obstante, son esenciales para el conocimiento y aplicación del derecho contemporáneo debido a la inminente y constante influencia de las nuevas tecnologías de la información y comunicación. Se ha considerado estudiar la visión de la norma jurídica vigente, incluyendo preceptos de legalidad y reglamentación de procedimientos utilizados por el Ministerio Publico, Organismo Judicial y Colegio de Abogados y Notarios de Guatemala, éste último, a través de las prácticas de sus agremiados. La información que aporta este sector ese esencial para conocer aspectos interesantes tales como la forma en que se da tratamiento a la evidencia electrónica y digital en el escenario criminal y su posterior ofrecimiento como prueba en el momento procesal correspondiente.

Dentro de la diversidad de temas que se desarrollan en esta investigación, se incluye la valoración judicial que se le da a la prueba electrónica y digital por los órganos jurisdiccionales que conocen casos relacionados a delincuencia organizada, sin embargo, también se toma como base casos de delincuencia común. De esa cuenta, se realiza una investigación de campo utilizando instrumentos de recolección de información tales como encuestas y entrevistas que sirvieron para medir el nivel de conocimiento sobre estos temas, cuyo epicentro es el derecho informático y la informática forense, además en las conclusiones y sugerencias de ésta tesis se evidencia la postura y argumentos de fiscales del Ministerio Público, abogados litigantes, jueces de instancia penal y otros abogados institucionalizados sobre el tratamiento de la prueba electrónica y digital.

B. INTRODUCCION

La investigación desarrollada fue titulada como “El diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada” trabajo fundamental previo a obtener el grado académico de Maestro en Derecho Penal en el Centro Universitario de Occidente de la Universidad de San Carlos de Guatemala. Este trabajo se fundamenta sobre las bases de las nuevas tendencias de la criminalística moderna, siendo que a diario se observa que a nivel internacional avanza el estudio del Derecho Informático en todas sus aristas, en el entendido que dentro de esta nueva rama del derecho se aprecia todo lo relacionado a la tecnología y telecomunicaciones en pequeña, mediana y gran escala. Actualmente en legislaciones del derecho comparado se pueden apreciar normativas jurídicas que regulan lo relativo al Cibercrimen, ciberdelitos, metodología y técnicas criminalísticas para el manejo de la evidencia electrónica y evidencia digital mediante estándares internacionales.

Lo anterior, se ha implementado en diferentes Estados a nivel mundial en virtud que es de conocimiento popular, que las tecnologías de la información están al alcance de todo público de forma sencilla y esto ha ocasionado que tanto la iniciativa privada como el sector público se hayan visto en la necesidad de crear mecanismos de control, prevención, análisis y corrección en el manejo de información. Esto se puede explicar que derivado de estos controles y mecanismos para proteger información sensible se incluye lo referente a la protección de software y hardware, normativa jurídica que proteja la información de las personas y sus comunicaciones, entre otros.

Esta investigación nos da la oportunidad de abrir nuevos espacios de conocimiento en virtud que estamos trascendiendo del mundo convencional al mundo digital a través de una mutación tecnológica en donde el derecho y todas sus ramas son influenciados de gran forma. De esta forma anticipo que conceptos como lo son la inteligencia artificial, el internet de las cosas, Blockchain[1], la Big Data [2] son conceptos

[1] Una cadena de bloques, conocida en inglés como blockchain, es una estructura de datos cuya información se agrupa en conjuntos (bloques) a los que se les añade metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal. De esta forma, gracias a técnicas criptográficas, la

que actualmente tienen una íntima relación con el derecho en todas sus ramas; por lo que se invita al lector a tomar esta investigación como una oportunidad de tener un conocimiento integro en donde se incluye el derecho, la auditoría, la informática, la criminalística y la criminología y con ello vencer las barreras digitales.

Este trabajo tomó como base a usuarios del Centro Regional de Justicia de la ciudad de Quetzaltenango, enfocado a profesionales que realizan sus funciones en la ciencia del derecho penal, dirigido a abogados litigantes e institucionalizados, fiscales y jueces, tomando en consideración que otros profesionales que no obstante siendo originarios de otros departamentos tales como Guatemala, Huehuetenango, San Marcos, Totonicapán, Retalhuleu, Suchitepéquez desarrollan sus labores profesionales en la cabecera departamental de Quetzaltenango.

La investigación tuvo como objetivo principal establecer si existe seguridad jurídica y legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada.

Tomando en consideración que es poco utilizada la ciencia de la informática forense como auxiliar del sector justicia y en virtud que considera que no existen procedimientos reglamentados vigentes y aplicables para el manejo de la evidencia electrónica y digital para su posterior utilidad como prueba dentro del proceso penal, se planteó la siguiente hipótesis:

- No existe seguridad jurídica ni legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada dentro del proceso penal guatemalteco, como consecuencia de la inexistencia de procedimientos uniformes y reglamentados, poco conocimiento y uso

información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores. https://es.wikipedia.org/wiki/Cadena_de_bloques

[2] También llamados datos masivos, inteligencia de datos, datos a gran escala o big data (terminología en idioma inglés utilizada comúnmente) es un término que hace referencia a conjuntos de datos tan grandes y complejos que precisan de aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente. https://es.wikipedia.org/wiki/Macrodatos

escaso de los procedimientos adecuados para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la información.

La hipótesis tiene un respaldo de carácter cuantitativo y cualitativo, mismo que se evidencia al comparar sus diferentes variables y el desarrollo del trabajo de campo, consecuentemente se consideró viable ésta investigación en virtud que tiene la sustentación teórica necesaria, así como con recursos e información fidedigna y permite estudiar a fondo “El diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada”

Actualmente dentro del sector justicia, se conocen una gran variedad de casos de diferente complejidad y es que en los últimos años se conoce la proliferación del uso de dispositivos digitales que son utilizados para la comisión de diferentes actos ilícitos, más aún, el flagelo de las estructuras criminales que aprovechan las bondades de la versatilidad de dispositivos electrónicos y digitales, tanto Ministerio Publico como los órganos jurisdiccionales tienen la ardua tarea de estar preparados y conocer la forma correcta en que deben ser diligenciadas las evidencias electrónicas y digitales para que en su momento puedan ser ofrecidas como prueba legal, útil, legitima y necesaria dentro de un proceso penal y con ello se le dé una valoración judicial que sea determinante en la averiguación de la verdad histórica del caso concreto, logrando que la prueba electrónica y digital posea un alto grado de efectividad y certeza jurídica indubitable, claro está que nos encontramos con un panorama nacional en el cual se acepta y valora una prueba electrónica y digital tal cual es una prueba documental o una prueba científica sin tomar en cuenta las particularidades de la pericia digital e informática

Para realizar la investigación se procedió a la revisión de fuentes bibliográficas respecto a temas afines como el derecho informático, protección de datos, delitos informáticos, informática jurídica, informática forense, el perito forense digital, delincuencia organizada y las nuevas tecnologías de la información y comunicación, entre otros temas con relación intrínseca.

Esta información se enriqueció con la información obtenida al encuestar a ochenta y cinco profesionales y entrevistar a ocho personas, tomando en cuenta a abogados litigantes e institucionalizados, fiscales y personal de la Dirección de Investigaciones Criminalísticas del Ministerio Público y jueces en materia penal. Áreas como el derecho, la informática, la criminalística, la criminología, la psicología y la oratoria forense, se entrelazan en las investigaciones como las que se presenta en esta ocasión. Este trabajo se desarrolla en diez capítulos con una íntima relación en su aspecto formal y de fondo.

En el capítulo uno efectuamos un análisis de diferentes conceptos y definiciones que sobre el "Derecho Informático" el cual se considera vital para saber de dónde surge la necesidad de manejar con propiedad las instituciones y figuras de la prueba electrónica y digital. Es de conocimiento popular que en nuestro gremio de Abogados y Notarios de Guatemala existe muy poca formación y fuentes de información al respecto, no cabe duda, que en los últimos años se han publicado algunos textos de diferentes abogados tales como el texto de Introducción de la Nuevas Tecnologías en el derecho escrito por el Licenciado Omar Ricardo Barrios que en forma introductoria y básica abordan estos temas. Observaremos la evolución que ha tenido el derecho hasta nuestra era en donde existe una discusión aun en considerar al derecho informático como una rama autónoma o que se vale del resto de áreas del derecho para crear sus instituciones juntamente a la informática per se.

En el capítulo dos abordaremos un tema que es de relevancia internacional y que en estos tiempos de crisis mundial es necesario abordarlo con seriedad y objetividad, hablamos de los "datos". Reflexionemos que hoy en día vemos como fluye la información de las diferentes plataformas virtuales y tecnológicas y es que la prueba digital es precisamente eso, "los datos" que se obtienen a raíz de un peritaje informático. Veremos en el desarrollo de este capítulo lo relativo a las bases datos y la necesidad de tener mecanismos funcionales que coadyuven a su protección siendo relevantes, entre tantos, los contratos informáticos en virtud que muchos de los problemas que hoy surgen es debido a la inexistencia de estos instrumentos. Es importante destacar que este capítulo se aborda, toda vez que los datos son la materia

prima, viva y dinámica del procedimiento forense de identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la información.

En el capítulo tres apreciaremos el fenómeno socio jurídico de los delitos informáticos, interesante resulta conocer las diferencias entre delito informático como objeto y como medio cuyas diferencias se aprecian en forma notable desde el momento de la consumación del acto ilícito. El lector podrá inferir que Guatemala está en crisis en con este flagelo social que trasciende a lo digital, porque a diario se cometen una infinidad de delitos informáticos y muchos ataques por parte de diferentes atacantes y que no necesariamente son víctimas grandes empresas si no también las persona particulares quienes se ven invadidos en su privacidad cuando se usan aplicaciones o programas que tienen códigos ocultos o malware[3] pudiendo alojarse en teléfonos celulares, computadoras o cualquier dispositivo electrónico.

El repunte de los delitos informáticos o ciberdelitos no es un problema aislado sino un problema de Estado en el cual podremos observar algunos ejemplos de la grave afectación que causa a los distintos usuarios. Es interesante indicar que en este capítulo es de suma importancia realizar un análisis pormenorizado a cada uno de sus subtemas, toda vez que muchos de los actos ilícitos que ocurren dentro del ciberespacio no tienen una regulación legal determinada y que pocas legislaciones contemplan un catálogo nutrido de tipología penal en materia informática tanto como objeto o instrumento del delito.

En el capítulo cuatro podremos contextualizar el ámbito de aplicación de la informática jurídica, siendo importante en el ámbito criminalístico y la criminología y la necesidad de implementación en los órganos jurisdiccionales especialmente en la justicia penal, tomando en cuenta que al auxiliarse de ésta área del derecho informático, podremos advertir que es de beneficio para los sujetos procesales especialmente para que se celebren las audiencias en la respuesta pronta a los postulados de justicia. Y es que veremos también la forma en que se manifiesta la

[3] Se llama programa malicioso, programa maligno, programa malintencionado, en inglés malware (acortamiento de malicious software), badware o código maligno, a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada. https://es.wikipedia.org/wiki/Malware

informática jurídica reflejada en el uso de videoconferencias para la celebración de debates en algunas judicaturas con competencia en procesos de mayor riesgo; desde el uso del software idóneo para la videoconferencia hasta la forma en que se deben trasladar los atestados y audios de la audiencia hacia los sujetos procesales mediante la utilización de servicios de alojamiento de archivos tales como Google Drive.

En el capítulo cinco entraremos a conocer los aspectos fundamentales de la cadena de custodia digital y la diferencia y relación con la cadena de custodia física. Además, analizaremos cada uno de los pasos que se desarrollan en la informática forense siendo ellos identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la evidencia electrónica y digital donde también se emitirá un comentario crítico sobre el papel que juegan las ciencias forenses en Guatemala y la forma en que actualmente en el ente encargado de la persecución penal maneja y procesa un escenario criminal. Al realizar este análisis también se podrá apreciar un cuadro comparativo en donde se hace una discriminación objetiva sobre la evidencia física, electrónica y digital.

En el capítulo seis abordaremos uno de los contenidos centrales de la investigación que consiste en la metodología y protocolos utilizados en la Informática Forense y para ello se describen protocolos que son funcionales a nivel internacional y que son reconocidos por expertos en la materia y que después de hacer una análisis minucioso de estos estándares internacionales, presento una propuesta general y concreta de la forma en que se podría analizar e interpretar la evidencia electrónica y digital tanto en el ámbito privado como en el ámbito público y que a juicio del autor, es de relevancia para el sector justicia en materia penal. No obstante, se observará que estos protocolos a pesar de ser funcionales también es necesario que más investigadores de derecho informático e informática forense nutran esta propuesta.

En el capítulo siete abordaremos y conoceremos el rol del Perito Forense Digital y sus ámbitos de actuación, veremos que en Guatemala existen profesionales de las diferentes ramas que a pesar que tiene una formación en su área profesional, no reúnen el perfil adecuado para realizar un Peritaje Forense Digital, no obstante, son aceptados como consultores técnicos o fungen como peritos en materia de informática

forense sin tener los conocimientos adecuados, causando con ello una confusión a todos los sujetos procesales, esto por implementar seudoprocedimientos o inconsistencias técnicas que pretenden validar bajo la capa de un seudotitulo o una carrera profesional que no equipara a la de un Perito Forense Digital. Es interesante destacar la labor de este profesional de la informática forense, en el avance de la lectura de todos los capítulos anteriores y especialmente en éste podremos apreciar y comparar la diferencia que existe entre la labor que desempeñan los técnicos de la Dirección en Investigaciones Criminalísticas del Ministerio Público y los Peritos Forenses digitales en materia de evidencia electrónica y digital.

En el capítulo ocho conoceremos en síntesis la forma en que se diligencia, ofrece y valora la prueba electrónica y digital en casos de delincuencia organizada, tomando como punto de partida una integración de todos los conceptos estudiados y abordados en esta investigación, desde la Informática Forense, documentos electrónicos, entre otros; se abordará este capítulo estudiando algunos temas del derecho comparado de cómo es aplicable la validez procesal, cuyos extremos, nos da la pauta de cómo debería realizarse en Guatemala. Importante es, conocer la relevancia que tienen las plataformas de mensajería instantánea y de cómo se aborda en otros países la valoración de la prueba electrónica y digital, se pretende entonces, además de estudiar estos conceptos, crear una motivación al lector para que estas líneas de investigación puedan ser aplicables en un proceso penal y de estudio crítico para mejorar los procedimientos que se emplean actualmente en Guatemala referente a este tema de estudio.

En el capítulo nueve haremos un recorrido sobre la dinámica en que la delincuencia organizada en esta era digital hace un uso ilimitado de las Nuevas Tecnologías de la Información y Comunicación para consumar actos ilícitos en variedad cuya interacción se desarrolla en el ciberespacio. En este apartado también se comentan algunos aspectos legales de la delincuencia organizada en Guatemala, algunos mecanismos de investigación criminal para combatir la delincuencia organizada y como punto central la valoración de la misma prueba digital y electrónica en casos de delincuencia organizada, para ello utilizamos una técnica de

cuestionamientos que propicia el debate y la respuesta abierta a aspectos que pueden originar diversos puntos de vista.

En el capítulo diez, se presentan los resultados de la investigación realizada, apuntando nuevamente el contexto en el que se realiza la investigación de campo y recordando el planteamiento del problema y la hipótesis formulada al inicio de la tesis. Veremos que unos de los fines de la investigación fijados al inicio y que me motivaron fue conocer la forma en que actualmente es utilizada y valorada la prueba electrónica y digital en el proceso penal guatemalteco en casos delincuencia organizada, la normativa jurídica vigente sobre este tema y la forma en que el Ministerio Publico como ente encargado de la persecución penal procesa la evidencia electrónica y digital, además, estudiar la valoración legal que los jueces le dan a este tipo de prueba tomando como base casos de delincuencia común y posteriormente casos delincuencia organizada.

La hipótesis del estudio se confirmó debido a que actualmente no existe seguridad jurídica ni legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada dentro del proceso penal guatemalteco, como consecuencia de la inexistencia de procedimientos uniformes y reglamentados, existe poco conocimiento y uso escaso de los procedimientos adecuados para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la información digital.

Se sugieren algunos puntos tales como una urgente actualización sobre temas de derecho informático e informática forense en la preparación de la profesión de Abogado y Notario en Guatemala y de manera más puntual el Ministerio Público, Organismo Judicial y el Colegio de Abogados y Notarios de Guatemala deben propiciar formaciones integrales sobre las nuevas tecnologías de la información y comunicación que tienen intima relación con el derecho consecuentemente con la investigación criminal, de esa cuenta también se sugiere a la Dirección de Postgrados de la Universidad de San Carlos de Guatemala propiciar una actualización en temas como el

derecho procesal tecnológico o digital, Big Data, Blockchain, inteligencia artificial e internet de las cosas, entre otros.

Por último, se presenta la bibliografía que sustentó teóricamente éste trabajo de investigación.

CAPITULO I
Derecho Informático.

1.1. Antecedentes históricos.

En las diferentes etapas de evolución de la humanidad se ha observado que siempre se encuentra presente la innovación y creatividad de diferentes objetos para facilitarle al hombre la realización de sus diferentes actividades y aparejada a ello la creación de mecanismos de control y procedimientos eficaces que ayuden a proteger a su familia, sus bienes y mejorar las relaciones comerciales con otros sujetos. En este caso las llamadas TIC –Tecnologías de la Información y Comunicación- han tomado mucha fuerza desde hace veinticinco años cuyo avance ha tenido gran impacto a la sociedad, es evidente que también se ha observado el desarrollo de las TIC en los diferentes sistemas judiciales de muchos países.

En el transcurrir de la historia se ha observado que el hombre dentro de sus roles en los grupos sociales ha propiciado la creación e innovación para mejorar sus condiciones de vida y dentro de ello ha surgido la tecnología como una forma de superación y satisfacción de diferentes necesidades y como una pequeña parte de ese gran campo se encuentra la informática, entendida esta como la forma en que automáticamente se maneja y trata la información a través de diferentes dispositivos electrónicos, entre ellos las computadoras. La incidencia de la informática con el paso de los años ha ocasionado que diferentes países modifiquen sus legislaciones a raíz de los grandes desafíos que presenta día a día a los institutos clásicos del derecho, al afirmar esto también debemos aceptar que la informática influye directamente en varios espacios de interacción social, comunicación, documentación y desarrollo.

Como lo señala el autor Chirinos,

> la informática surge en el seno de la cibernética, ciencia que apareció como respuesta a una inquietud racional del hombre. El asidero histórico de la aparición de la cibernética como género y de la informática como especie, se encuentra en la acción del factor social (la necesidad social de un aumento en la producción y en el capital), el factor

> técnico-científico (los avances de la ciencia y la técnica en diversas áreas del conocimiento humano) y el factor histórico (la necesidad de unificar los avances científico-técnicos de ese momento histórico para que funcionara como unidad multitudinaria) de una época de convulso desarrollo intelectual. De esta forma, el hombre se enfrenta a una necesidad de información y gestión eficaz de la misma, por lo que recurrió a reformular postulados y técnicas que fueran capaces de solucionar esta problemática con la implementación de nuevas formas de manejo, organización y utilización de la información. Sin embargo, el desarrollo y evolución de la informática no culminó en ese momento sino encontró su inicio jugando un papel trascendental en todos los órdenes del desarrollo humano, impulsando novedosos cambios y entretejiendo otros horizontes para las ciencias. Adjuntamente, se alcanzaron objetivos como la transferencia de información, la potenciación de las comunicaciones, la explotación de programas de uso institucional y privado, la implementación de la ofimática, el perfeccionamiento de la formulación de políticas, planeación y conducción de estrategias organizacionales; el perfeccionamiento de la comunicación, dirección y supervisión de empleados, el eficiente control de nóminas, contabilidad o inventarios, y la consolidación de los sistemas de pago automatizado, entre otros aspectos. La informatización de la sociedad llegó a alcanzar insospechados niveles. Desde hace ya algún tiempo, en el área industrial escuchamos sobre robótica e implicaciones como el aumento de la productividad con reducciones de tiempo y costos. Así mismo, el área de la medicina se ha beneficiado de esta revolución informática con la creación e implementación de programas para gestionar historias clínicas, exámenes, diagnósticos y pruebas de laboratorio con mayor exactitud. (Chirinos, 2017)

Sigue afirmando Chirinos que en el campo del Derecho ha surgido la Informática Jurídica que actúe en el campo legal y esta es una técnica que da lugar a que puedan converger tanto el Derecho como la Informática cuya sustancia es la automatización de

la información jurídica y la elaboración del aprovechamiento de los instrumentos de análisis y tratamiento de dicha información (2017). Por último, concluye esta autora que "La Informática Jurídica es la aplicación de la computación y sus instrumentos para la búsqueda de la solución de problemas jurídicos"

Arean Velasco explica lo relativo a las nuevas Tecnologías señalando que,

> para enfrentar de manera adecuada los retos que las TIC plantean al Derecho se requiere como punto de partida por el operador jurídico, la comprensión de los aspectos tecnológicos que, desde la informática, las telecomunicaciones y la convergencia, están presentes en el tráfico de bienes y servicios, así como en la economía, pues sin esta comprensión es difícil entender los problemas que giran en torno al desarrollo de software, integración de sistemas informáticos, diseño de hardware, voz IP, servicios y redes de telecomunicaciones, propiedad intelectual de intangibles digitalizables, bases de datos, servicios convergentes, entre otras problemáticas. Sigue manifestando este autor que es necesario que se estudie las Tecnologías de la Información y el Derecho y es por ello que ha surgido una nueva rama del Derecho encargada de estudiar este fenómeno informático y telemático denominado Derecho Informático. (Velasco Melo, 2008)

Al respecto Velasco Melo (2008) cita al profesor (Suñe, 2000) quien afirma que:

> el Derecho de la informática, por seguir aportando razones singulares que avalan su autonomía, tiene mucho de Derecho Global, al tratarse de un Derecho muy internacionalizado, probablemente por el tipo de comunidades humanas que están en su base. La regulación jurídica de Internet, por ejemplo, plantea problemas globales, que requieren soluciones globales. Las grandes multinacionales del sector teleinformático, que lo dominan casi todo por completo, no pueden –ni quieren–

adaptarse a regulaciones estatales injustificadamente diversas y dispersas, cuando el mercado no es nacional, sino global. (Velasco Melo, 2008).

1.2. Generalidades, conceptos y definiciones.

Desde tiempos muy remotos el estudio del Derecho ha evolucionado de conformidad a las diferentes necesidades de la gran cantidad de poblaciones que se han asentado en diferentes partes del mundo. Tal es el caso que al inicio todo estaba concentrado en el Derecho Civil en virtud que regulaba diferentes actos en los cuales intervenían las personas como parte de su interrelación con los demás sujetos de la misma población, cercanos o lejanos y era necesario una normativa a seguir para que se adquiriera seguridad jurídica. En el caso del Derecho penal también ha evolucionado y día a día la Ultima Ratio que es una de las características de esta rama del Derecho se va quedando limitada en virtud de la complejidad de elementos que se deben tomar en consideración para tener un mejor abordaje y estudio de esta rama del Derecho, claro está que en forma paralela coexiste la epistemología jurídica aplicada que se pone de manifiesto en la práctica tribunalicia.

Es necesario recordar algunos términos que definen al Derecho, para ello debemos traemos como referencia lo que dice Immanuel Kant sobre, la filosofía kantiana (Kant 1724-1804) conocida también como filosofía crítica, que formula el concepto de Derecho como " una postura del Derecho Natural, que está representado por intereses sobre la naturaleza humana, valores jurídicos, justicia y bien común que sería el ideal jurídico: Es el complejo de las condiciones por las cuales el arbitrio de cada uno puede coexistir con el arbitrio de los demás, según una ley universal de libertad" (Anónimo). Siguiendo con la filosofía de Immanuel Kant que indicaba que el Derecho era parte el Derecho natural basados la naturaleza humana y establecía que el derecho es el deber ser, manifestando que las cosas no deben estar sometidas explícitamente a un bien individual sino debe ser más amplio en el sentido de tutelar el bien común.

El Derecho se estructura de una serie de principios y preceptos normativos de carácter obligatorio dentro de un territorio determinado a efecto que los sujetos que

habiten en dicho lugar, las cumplan y en caso de negativa exista los mecanismos necesarios para obligarlos a hacerlos efectivos. Paralelamente es necesario establecer la forma en que se conceptualiza al Derecho Objetivo y subjetivo que nos da la pauta que el primero se refiere al andamiaje jurídico existente dentro de un Estado y que depende del accionar de una persona para hacerlo valer frente a otro (Derecho Subjetivo).

Otro concepto define al Derecho como un "conjunto de normas, tratase de preceptos imperativo-atributivo, es decir, de reglas que además de imponer deberes, conceden facultades. Es el conjunto de normas jurídicas declaradas obligatorias por la autoridad, por considerarlas justas a los problemas surgidos de la realidad histórica." (Garcia Maynez, 2002)

El término información toma relevancia junto al término Derecho siendo que "la palabra información proviene del latín clásico, donde presumiblemente era de uso común. El término *informatio* es una sustantivación del verbo informare, que por ser transitivo encuentra su mayor generalidad en la expresión *aliquid informare*. Esto último significa literalmente dar forma a un objeto. (Ostale García)

Como se comentaba la evolución del Derecho se está dando a grandes pasos y con ello también el avance de la tecnología que está presente en todos los contextos en que una persona se desenvuelve, es por eso que se califica a nuestra sociedad que está en la era de la información o de la revolución electrónica en vista de la gran versatilidad de dispositivos electrónicos con que se cuenta hoy en día y derivado de ello los diversos usos que se le dan en muchas esferas de la vida cotidiana.

Existen varias definiciones de Derecho y es por ello que previo a definir lo que es Derecho Informático hemos dedicado algunas líneas para conocer el antecedente y concepción del término Derecho teniendo en cuenta que existen un sinnúmero de definiciones que nos ayudan a comprender de mejor forma este concepto, es por ello que acudimos a lo que indica (Pérez Luño, Soriano Diaz, & Gómez Torres) en su Filosofía y Teoría del Derecho e Informática Jurídica que indica que "Derecho

Informático como el conjunto de normas que dentro de un determinado sistema jurídico regulan los procesos de información."

La información es un término que se relaciona con el tema del Derecho Informático y de acuerdo a lo que analiza (Montaño, 2017) quien cita a (Ruyer, 1992) indica que,

> la información, es la transmisión a un ser consciente, por medio de un mensaje más o menos convencional y por un soporte espacio-temporal (…) la era de la información y del llamado Habeas Data está íntimamente ligada al Derecho Informático ya que los datos o información se encuentra en toda esfera del ser humano, como puede ser desde lo personal, comercial, industrial, empresarial, estatal y asuntos de carácter reservado. Es por ello que en la actualidad el auge que y relevancia que ha tenido las Tecnologías de la Información y de las Comunicaciones, también conocidas como TIC- tiene un vínculo estrecho en el campo judicial e investigación criminal. En diferentes países del mundo ha ido evolucionando el tema el Derecho Informático abarcándolo desde diferentes concepciones y aristas, para ello es necesario que el lector pueda conocer algunos elementos de este concepto para su mayor crítica y análisis.

A. Conceptos.

El Maestro Raúl Martín hace alusión a diferentes conceptos del Derecho Informático de otros autores indicando que se debe entender como:

> "el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones".

Otros autores lo definen como "conjunto de leyes, normas y principios aplicables a los hechos y actos derivadas de la informática" Podríamos conceptualizar el Derecho de la Informática como: el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la

misma en las que existe algún bien que es o deba ser tutelado jurídicamente por las propias normas.

Hoy es cuestionable si existe esta disciplina como tal, por ello, la mayoría de estudiosos de esta materia prefieren estudiar los siguientes puntos:

a) Protección jurídica de la información personal.
b) Protección jurídica del software
c) Flujo de datos fronterizos
d) Convenios o contratos informáticos
e) Delitos informáticos.
f) Valor de los documentos electromagnéticos (Firma digital)" (Martin)

B. Definiciones.

Dentro del campo del derecho informático encontramos que la información es uno de los elementos más importantes para que esta rama del derecho tenga sustento y así como lo señala Ernesto Villanueva en su obra de Derecho a la Información, quien manifiesta que:

> el derecho a la información es el objeto de estudio del derecho de la información, entendido éste como la "Rama del Derecho Público que tiene por objeto el estudio de normas jurídicas que regulan las relaciones entre Estado, medios y sociedad, así como los alcances y los límites del ejercicio de las libertades de expresión y de información y el derecho a la información a través de cualquier medio" (Villanueva, 2006) Julio Téllez Valdés en su libro Derecho Informático lo define "como una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica y como objeto de estudio (Derecho de la información)" (Téllez, 2008).

De conformidad a las definiciones citadas por los autores mencionados que la definición de "Derecho Informático" se aplica a los sistemas informáticos en función de las diferentes ramas del Derecho, con ello debemos advertir que es necesario sacarle

provecho a los recursos que provee la informática aplicada a la esfera del derecho da el quehacer jurídico actual. Definimos entonces el Derecho Informático como el conjunto de normas jurídicas, principios e instituciones que regulan las relaciones jurídicas que surgen de la actividad informática. El derecho informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento y como objeto de estudio.

C. Diferencia entre derecho informático e informática jurídica.

Nos corresponde ahora delimitar estos dos términos, óbice para comprender de mejor forma su ámbito de estudio y aplicación desde las perspectivas informática y jurídica, es importante que el lector defina desde un inicio estas concepciones para que pueda asimilar de mejor forma el objeto de esta investigación. Para ello citamos lo que dice Julio Téllez que define la informática jurídica como:

> "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la Informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación" (Téllez, 2008).

Entendiendo entonces que la informática jurídica nos provee de instrumentos y mecanismos para conocer todo lo relativo a la informática.

Yarina Amoroso Fernández señala una interesante definición sobre lo que es la informática jurídica, estableciendo que:

> "La Informática ha llegado a constituirse en infraestructura del quehacer moderno, dado que bases de datos y redes telemáticas captan, procesan inmediatamente y trasmiten a gran velocidad cantidades ilimitadas de información. Por la connotación adquirida por las nuevas tecnologías, se han producido un conjunto de aplicaciones de la Informática

en el ámbito del Derecho en que la Informática es instrumento del Derecho lo que se conoce como Informática Jurídica" (Amoroso, 2000)

El Doctor Hernán Ramón Peñaranda Quintero estudió en su obra denominada "Iuscibernética" sobre la importancia y avance de la informática opinando que esta es utilizada en el campo del derecho y en el momento que la informática se aplica en el Derecho busca el tratamiento lógico y automático de la información legal. (Peñaranda). Analizando los conceptos que hemos estudiado podemos diferenciar e ilustrar que dentro del campo del derecho existe la rama jurídica del Derecho Informático y dentro de las disciplinas que forman parte de esta rama se encuentra la informática jurídica, siendo ésta el instrumento y que el derecho informático es el objeto de estudio.

En conclusión, tomamos lo que acertadamente señala Téllez Valdez, definiendo que,

"el Derecho informático es el conjunto de normas jurídicas que se encargan de regular los actos y aspectos de la tecnología informática y su finalidad es evitar quebrantar los derechos fundamentales para mantener el orden de una sociedad y la Informática Jurídica es una herramienta tecnológica puesta al servicio del derecho para hacerlo más eficiente ya que facilita el procedimiento, almacenaje y recuperación de información jurídica". (Téllez, 2008). Por último, en relación a los avances tecnológicos este autor señala que "el uso de la computadora mejora la productividad, sin menoscabo de las consecuencias negativas tales como el desplazamiento laboral, menos pago en centro de trabajo y problemas jurídicos en el tema de la confidencialidad, la seguridad de la información, comisión de ilícitos penales a través del uso de sistemas computacionales"

1.3. Características y principios del derecho informático.

El autor Julio Valdez menciona las diferentes acepciones con que se le conoce al Derecho Informático siendo estos: Derecho de la Sociedad de la Información, Derecho de las Nuevas Tecnologías, Derecho Telemático, Iuscibernética, Derecho Tecnológico, Derecho del Ciberespacio, Derecho de Internet, entre otros. (Téllez, 2008)

De conformidad a lo expuesto por Edgar Salazar Cano esta rama jurídica del derecho se puede comprender de mejor forma entendiendo lo analizado los siguientes aspectos:

1) No se encuentra sectorizado o ubicado en una sola actividad, sino que es amplio y general, debido a que la informática se aplica en numerosos sectores de la actividad socioeconómica;

2) Su unidad viene dada por la originalidad técnica, impuesta por el fenómeno informático;

3) Es un derecho complejo, porque los aspectos técnicos de la informática, en su interrelación con el Derecho, recaen sobre diversas ramas o especialidades jurídicas.

Sigue manifestando Salazar Cano que:

"el carácter interdisciplinario que caracteriza al Derecho Informático ha producido un amplio debate, entre los autores que lo entienden, como un conjunto de normas dispersas de varias disciplinas jurídicas, y aquellos que lo consideran como un sistema unitario de normas" (Cano, 2017).

Es así que el mundo globalizado necesita que la tecnología vaya avanzando a un ritmo acelerado para que cumpla con sus expectativas, para nadie es un secreto que el desarrollo de las nuevas tecnologías de la información y de las comunicaciones, se acelera día a día y para el campo del derecho debemos estudiarlo como fuente material del Derecho, es decir, seguirá dando origen a la evolución y desarrollo de esta rama de las ciencias jurídicas.

Ahora bien, en cuanto a los principios del derecho informático debemos detenernos para analizar cada uno de los motivos que lo inspiran, informan y robustecen, Carlos Monsálvez detalla lo siguiente:

A. Protección/respeto de la dignidad de las personas.
B. Interpretación progresiva de los derechos.
C. Autonomía de la voluntad.
D. Buena fe.
E. Debido proceso.

F. Seguridad jurídica.

G. Neutralidad tecnológica.

H. Libertad de prestación de servicios.

I. Libre competencia

J. Protección a la identidad cultural.

K. Compatibilidad internacional.

L. Equivalencia funcional de los soportes.

M. Libre circulación de la información" (Monsálvez, 2015)

Asimismo, existen principios del derecho informático stricto sensu, dentro de los cuales el autor Carlos Reusser Monsálvez en su obra Manual chileno de Derecho Informático señala los siguientes:

a. Mínima intervención. De acuerdo a este principio del Derecho Informático, las reformas legislativas necesarias para adecuarse a la realidad tecnológica deben ser por regla general las mínimas y suficientes y sólo excepcionalmente se requerirán cuerpos legislativos completamente nuevos.

b. No alteración de categorías jurídicas. Las reformas normativas a que el fenómeno tecnológico de lugar no debe modificar las estructuras fundamentales del Derecho ni pretender establecer nuevas figuras jurídicas si las existentes son hábiles para comprender el proceso de que se trate. Por ejemplo, no debe establecerse la "buena fe tecnológica" cuando se trate de contratos celebrados por medios electrónicos si la figura tradicional de la buena fe es perfectamente válida y aplicable al caso.

c. Convergencia jurídica. El Derecho Informático se hace cargo del proceso de convergencia tecnológica de las infraestructuras derivada de la digitalización de los contenidos, y comprende que en el ordenamiento jurídico ya no existen los compartimientos estancos (televisión, telefonía, radio, Internet, etc.), sino que todos estos pueden confluir en plataformas de red que tienen la capacidad de, pese a su naturaleza diversa, trasmitir y recibir el mismo tipo de información. Como

consecuencia, ya no es razonable ni útil crear sistemas de regulación o tipos de soluciones jurídicas aisladas, sino que deben considerarse las interrelaciones entre los distintos productos y servicios, poniendo especial atención al hecho de que las empresas de telecomunicaciones, de informática y de contenidos audiovisuales ya no están en áreas separadas de la actividad económica. (Monsálvez, 2015)

El derecho informático es un derecho autónomo. Acertadamente el autor Carlos Reusser efectúa un análisis sobre la ubicación del derecho informático dentro del área de las ciencias jurídicas, indicando que;

> uno de los temas más debatidos en las áreas emergentes del Derecho fue la existencia o no del Derecho Informático, es decir, el cuestionamiento de si sus contenidos y entidad eran una mera actualización del Derecho tradicional al ámbito de la tecnociencia o se extienden más allá (…) se ha respondido en forma mayoritaria que no se trata de una mera actualización de los contenidos clásicos del Derecho, sino que se trata de una revisión integral del Derecho y las instituciones jurídicas ya conocidas a las cuales se suman otras completamente nuevas y desconocidas que tienen como presupuesto el proceso de revisión ya señalado.” (Monsálvez, 2015)

Tomando en consideración este postulado se estima que el Derecho Informático es dinámico, autónomo y especialísimo en virtud de las características que lo integran, así como de los postulados jurídicos e informáticos que lo vuelven integral.

1.4. Clasificación y características de la informática jurídica.

Como lo hemos visto en los párrafos que anteceden, el derecho informático y la informática jurídica parecieran que son términos similares, no siendo así, en virtud que el derecho informático es una rama de las ciencias jurídicas con autonomía evolutiva y dinámica, mientras que la informática jurídica es una ciencia que se estudia desde el área informática, no obstante ello esta ciencia ha ido evolucionando y penetrando en el sistema judicial y pericial del campo jurídico, el cual ha servido de soporte y auxiliar

para el desarrollo de diferentes procedimientos, es decir la informática jurídica actualmente es base fundamental en el medio forense y judicial.

La informática jurídica estudia el tratamiento automatizado de: “las fuentes del conocimiento jurídico a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (Informática jurídica documental). Las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial (Informática jurídica decisional). Los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (Informática jurídica de gestión.” (Téllez, 2008)

Puntualizó que la informática jurídica es una ciencia que estudia la utilización de aparatos o dispositivos electrónicos, como la computadora en el campo del derecho o la extracción y análisis de información que se obtiene de dispositivos físicos para su posterior análisis forense por medio de un perito especializado. Con esto vemos que la informática jurídica se presta al desarrollo y aplicación del derecho.

1.5. Fuentes del derecho informático.

En nuestra actualidad, que se caracteriza por ser un mundo globalizado con cambios constantes, el origen que da la pauta para que surja la legislación, doctrina y consulta en materia de derecho informático se va marcando a raíz del desarrollo de diferentes escenarios dentro de ellos podemos comentar algunos: las eventualidades en vulneración a los sistemas de información, la proliferación de los ciberdelitos, los protocolos que manejan los Estados para la protección de datos y de información, la existencia de contratos electrónicos que llevan inmersa la adaptabilidad y funcionalidad de la firma electrónica, los estándares internacionales en materia de Ciberseguridad, uso de las redes sociales, los protocolos forenses de la evidencia electrónica y digital, entre otras. Es menester recordar al estimado lector, que las fuentes del derecho *stricto sensu* se encuentran en la ley, la costumbre, la jurisprudencia y la doctrina.

Ahora bien, en el ámbito del Derecho Informático sucede algo particular y es que a raíz de la constante innovación de la tecnología y de las practicas que se realizan en ella, la fuente se encuentra en los aspectos fácticos de cada Estado y que a raíz del

desarrollo y complejidad de diferentes situaciones que ameritan un estudio, reglamentación y control por parte de un Estado.

Según como lo establece en su blog personal la autora Mayra Romina:

> la ley, se encuentra en un proceso de concreción en los distintos Estados, teniendo como antecedentes la normativa internacional que se ha generado partiendo de un orden cronológico inverso al expuesto, es decir, desde la autonomía de la voluntad se han generado usos, prácticas comerciales y costumbres, que han dado origen a recomendaciones, resoluciones, directivas y leyes modelos, tendientes a orientar las conductas de los sujetos intervinientes y las legislaciones, las cuales constituyen fuente de inspiración de la normativa interna de los Estados que la van incorporando a sus normativas internas. (Romina, s.f.)

La autora antes referida, continúa manifestando que:

> una de las características del Derecho Informático que más incide en el tema de sus fuentes es el de la transversalidad, con relación al resto de las ramas del Derecho y que aún enfocados en el tema de la contratación informática obliga a referirnos especialmente al Derecho Internacional Privado y al Derecho Internacional Público, dada la predominancia de la contratación internacional por este medio, sin perjuicio de la aplicabilidad de las normas de todas las ramas del Derecho, según el caso concreto de que se trate.(Civil, Procesal, Penal, Administrativo, Laboral, Comercial, Marítimo, Aeronáutico, Ambiental, Constitucional, etcétera. (Romina, s.f.)

A consideración de lo anterior podemos concluir que esa característica de la Transversalidad del Derecho Informático significa que las fuentes que nutren a esta rama del Derecho se encuentran en diferentes fuentes del Derecho *lato sensu*, consecuentemente se torna complejo una ubicación específica, esto se da por las relaciones jurídicas que se mezclan con las otras ramas del derecho.

Teniendo ya estas generalidades podemos clasificar *Las Fuentes del Derecho Informático*, según como lo explica el Doctor Carlos Reusser en su Manual de Derecho Informático, quien indica que existen fuentes materiales y fuentes formales, explicándolo así:

a) "Ley o legislación. Aunque la ley es la fuente formal por excelencia en los sistemas jurídicos continentales de raigambre europea, la dictación de leyes es más bien un fenómeno tardío dentro del proceso de configuración del Derecho Informático. Pero nos referimos acá al concepto de legislación en sentido amplio, y dentro de ese contexto no puede desconocerse que de manera muy significativa, y ante la ausencia de leyes formales, la administración pública hizo uso de su potestad reglamentaria dictando normas que fueron generalmente acatadas y permitieron avances sustantivos, más allá de los cuestionamientos sobre su constitucionalidad…..En la actualidad los países poseen ya una nutrida legislación sobre estas materias, como las relativas a delitos informáticos, firma electrónica, protección de datos, contratación electrónica, etc., y la dictación de normas reglamentarias para suplir la ausencia de leyes formales ha caído en desuso.

b) Costumbre jurídica. Relegada en cuanto a importancia a los últimos escalones del ordenamiento jurídico como lógica consecuencia de los procesos de codificación del siglo XIX, se le creía agotada cuando renace con inusitada fuerza de la mano de la Sociedad de la Información, modelando y uniformando los patrones de comportamiento y estableciendo factores comúnmente aceptados de entrada y exclusión en mundos reales y virtuales. Conocida primariamente como *neti quette (*buenos modales en la red), rápidamente sus reglas se configuraron como conductas exigibles entre los usuarios de las redes de comunicaciones y como tales fueron comúnmente aceptadas.

c) Jurisprudencia. En la construcción del Derecho Informático ha sido la labor de los jueces resolver problemáticas no contempladas literalmente por la legislación, proceso que han llevado adelante integrando o interpretando el

Derecho. Muchos de los avances alcanzados en esta materia están basados en razonamientos judiciales que se han ido perfeccionando con el tiempo y adecuando a las nuevas realidades, e incluso han sido recogidas posteriormente por la legislación positiva, como son los fallos del tribunal constitucional español sobre protección de datos, cuyo razonamiento fue recogido en la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos (LORTAD) de 1992, de gran impacto en América Latina.

d) Doctrina. Está constituida por las opiniones, comentarios y en general por los trabajos e investigaciones de los autores relativos a materias del Derecho Informático. Aunque tradicionalmente se le señala como fuente formal, en estricto rigor la doctrina no genera normas jurídicas, ni posee fuerza obligatoria, sino más bien es una fuente material del Derecho Informático, cuya importancia e influencia estará determinada por la calidad y relevancia del autor de ella y su capacidad para comprender los fenómenos tecnológicos que subyacen a su opinión. Sin embargo, debe señalarse que, en esta rama del conocimiento, por la novedad de las materias, los criterios de los autores tienen una inusitada influencia en la resolución de conflictos de relevancia jurídica, particularmente en los supuestos no previstos por la ley." (Monsálvez, 2015)

La relación del derecho informático con otras ramas del derecho.

El Profesor Raúl Martín hace un importante análisis indicando que

las fuentes y estructuras del Derecho informático no están aparte del "Derecho tradicional", así se inscriben en el ámbito del Derecho público el problema del a regulación del flujo internacional de datos informatizados, la libertad informática o la defensa de las libertades frente a posibles agresiones realizadas por las tecnologías de la información y la comunicación, o los delitos informáticos que tienden a configurar un ámbito propio en el Derecho penal actual. Mientras que en el Derecho Privado estarían recogidas cuestiones tales como: los contratos informáticos, que pueden afectar lo mismo al hardware que al software, dichos contratos pueden ser de compraventa,

alquiler, copropiedad, multipropiedad. Dentro del Derecho privado están también recogidos los distintos sistemas para la protección jurídica de los programas de ordenados, temas que afectan a los objetos tradicionales de los Derechos civil y mercantil. El hecho de que el Derecho informático afecta a distintas disciplinas dentro del Derecho ha suscitado un debate teórico sobre si se trata de una nueva disciplina jurídica o si por el contrario se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas" (Martin)

Es necesario entonces detallar la relación que tiene con las diferentes ramas del derecho, para ello mencionamos las siguientes:

i. **Con el Derecho Constitucional**: Tal y como se ha descrito ya, el avance incesante de la tecnología en la era de la información y de las bases de datos, es necesario que las diferentes legislaciones de los Estados del mundo regulen de manera concreta e integral los diferentes ámbitos de competencia y alcance del Derecho Informático, consecuentemente ello debe ser tratado como una garantía constitucional y desarrollada en la legislación ordinara y reglamentaria.

Jorge Castillo en su texto la Constitución Política de la República de Guatemala Comentada, explica sobre la transversalidad de los derechos humanos, indicando que:

> la interpretación jurídica busca la aplicación o actualización de los artículos de la Constitución, es un proceso intelectual basado en el conocimiento del contenido de los artículos, en la referencia histórica de los artículos precedentes y en el avance doctrinario jurídico de las materias (sic) tratadas por la Constitución Política. La interpretación jurídica de un artículo lo relaciona con otros para conseguir una interpretación integral…la interpretación integral conduce al exacto significado de la norma constitucional" (Castillo González, 2016-2017)

Tomando como base el aporte del autor anteriormente referido se estima que el Derecho Informático al estar disperso en diferentes normativas debe interpretar en

forma armónica con otros preceptos legales, especialmente constitucionales. Como ejemplo podemos citar los artículos dos (libertad, justicia, seguridad, paz, desarrollo integral de la persona); cuatro (libertad); cinco (libertad de acción); doce (derecho de defensa y debido proceso); diecisiete (no hay delito ni pena sin ley anterior); veinticuatro (inviolabilidad de correspondencia, documentos y libros); veintiocho (derecho de petición); treinta (publicidad de los actos administrativos); treinta y cinco (libertad de emisión del pensamiento); cuarenta y dos (derecho de autor o inventor); cuarenta y tres (libertad de industria, comercio y trabajo); cuarenta y cuatro (derechos inherentes a la persona humana); cuarenta y seis (preeminencia del Derecho Internacional); entre otros.

Ahora bien, la relación directa que existe entre el Derecho Informático y Derecho Constitucional estriba en la forma y manejo de la estructura y órganos fundamentales del Estado. Dicho esto, nos enfocamos al tema del Habeas Data que es una acción de naturaleza constitucional que puede estar en un registro o base de datos para conocer la información sobre determinada persona.

German Mojica en su blog de Relación con el Derecho Constitucional (Habeas Data) refiere que:

> con el desarrollo de Internet y las autopistas de la información, esta acumulación de datos es automatizada y es realizada por defecto en cualquier operación de comercio electrónico. La posibilidad de que estos datos sean incorrectos, desactualizados, o caducos como así también el poder que el conjunto de toda esta información otorga a quien la detenta, llevaron a regular estos usos de distintas maneras. Esta preocupación llevó a incluir en los textos constitucionales de América Latina una garantía contra los abusos del "poder informático". Esta garantía, que se denominó habeas data, permite acceder a los datos personales y corregir informaciones erróneas, desactualizadas o discriminatorias. A lo largo de los últimos quince años las constituciones de América Latina se han ido reformando para incluir esta clase de garantías constitucionales" (Mojica, 2009)

En Guatemala es vigente y positivo el Decreto Legislativo número 57-2008 “Ley de Acceso a la Información Pública” que en el artículo 30 regula lo concerniente al Habeas Data, tema que más adelante desarrollaremos.

ii. **Con el Derecho Penal**. Debemos recordar que el derecho Penal en un sentido amplio comprende tres áreas de estudio: la parte sustantiva, la adjetiva y de ejecución y que específicamente en la parte sustantiva en su parte especial se encuentra el catálogo de tipos penales y sus respectivas sanciones y que en el caso que nos amerita en el presente trabajo de investigación, tendríamos que encontrar todo aquellos supuestos que regulen las conductas ilícitas que constituyan una vulneración al uso incorrecto de la tecnológica. Es menester hacer mención que dentro de los ejes que aborda el Convenio de Budapest está el tema de los Delitos Informáticos y ahí se describen cuatro categorías las cuales las podemos detallar de la siguiente forma:

- ***Delitos que tienen a la tecnología como fin****:* son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, entre otros.
- ***Delitos que tienen a la tecnología como medio***: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.
- ***Delitos relacionados con el contenido***: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.
- ***Delitos relacionados con infracciones a la propiedad intelectual***: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, etc.

Haciendo un análisis sobre esta clasificación podríamos entonces adoptar un nuevo término “Derecho Penal Informático” el cual evolucionará en terminología, conceptos, características y principios que podrán abordar su estudio.

iii. **Con el Derecho de Autor.** La forma en que interactúa el Derecho informático con la propiedad intelectual contribuye a lograr un mejor control por ejemplo la sanción de los plagios, la piratería y en sí cualquier ilícito en contra de los Derechos de autor o conexos, en sentido del perjuicio que se podría estar produciendo mediante ilícitos en contra de intereses de terceros y por medio de los instrumentos informáticos**.** En Guatemala se encuentra vigente el Decreto Legislativo número 33-98 “Ley de Derechos de Autor y Derechos Conexos”

iv. **Con el Derecho Civil y Mercantil**. Existen innumerables escenarios en los cuales existe esta estrecha relación, como ejemplo está el faccionamiento del contrato electrónico, comercio electrónico, firma electrónica, entre otros, los cuales se basan en el acuerdo de voluntades, misma que originan la existencia del Derecho Informático en el ámbito privado.

v. **Con los Derechos Humanos**. La forma en que el Derecho Informático acciona junto a los Derechos Humanos toma su curso al momento que se tutela a la persona mediante el funcionamiento de los órganos de justicia y sectores afines, es decir el correcto funcionamiento del aparato de justicia mediante el uso de los medios telemáticos que coadyuven a la consecución de sus fines. Otra forma en que se da esta relación entre ambas ramas del derecho es la tutela y seguridad jurídica que el Estado debe proveer en el tema de la privacidad e intimidad que podría ser afectada si es vulnerada mediante técnicas o medios telemáticos o informáticos.

1.6. El fenómeno informático y su relación con las ciencias jurídicas.

Como lo señala el Profesor Raúl Martín el tema de la comunicación a través de internet, el desarrollo de programas y procesamiento de información no es ajeno al ámbito del Derecho y es ahí donde el Estado actúa como garante de certeza jurídica, en este caso la propiedad intelectual o industrial. (Martin). Sigue afirmando el autor

anteriormente aludido que “El derecho debe regular los nuevos fenómenos. Por ejemplificar de alguna manera, podemos pensar en: a) La disposición de un bien, sin el consentimiento del propietario del mismo, realizada mediante equipos informáticos. b) El apoderamiento de información contenida en registros electrónicos. c) Destrucción de la información” (Martin)

El rol de la tecnología en cada ámbito social se caracteriza porque el usuario final debe acoplarse a los diferentes protocolos de reglamentación y funcionamiento para que pueda desarrollar su función. En el ámbito laboral por ejemplo tenemos el lector de huella, que es un dispositivo electrónico que es útil para llevar el control de ingreso y egreso de las instalaciones laborales y que al final del mes reflejará información pertinente, si el empleado ha cumplido satisfactoriamente su horario, de lo contrario el registro que reflejaría el software serviría como base para iniciar una llamada de atención, procedimiento administrativo o hasta un despido justificado, es decir, se convierte en una necesidad. El ejemplo aludido es solo uno de tantos que se pueden citar en donde se puede observar como el fenómeno informático toma auge y si se trata de estudiar en su funcionamiento e interacción con las diferentes disciplinas o ciencias jurídicas podremos percatarnos que están presentes como auxiliar o como objeto final de estudio (Sociología jurídica, Filosofía del derecho, Derecho Comparado, entre otros)

- **El escenario del jurista en el ámbito del Derecho Informático**

El autor Valentín Carrascosa, en cuanto al estudio que realiza en su texto La Regulación Jurídica del fenómeno Informático, refiere las opciones que los Juristas podrían asumir ante la presencia de la Era Digital siendo las siguientes:

> (…)1.- Aceptar y someterse al Derecho tal como está regulado, sin tener en cuenta la discrepancia entre la evolución tecnológica y la reglamentación jurídica. 2.- Desarrollar una nueva legislación adecuada a los cambios que sufre la sociedad, formulando propuestas a fin de que el Derecho asuma nuevas formas que no sólo obstaculicen el uso de las nuevas tecnologías, sino que lo regulen adecuadamente, revisando y

> adecuando las viejas leyes a las necesidades y situaciones jurídicas que van apareciendo con las nuevas tecnologías. (Carrascosa, 1998)

Siendo la opción dos la que el estudiante de derecho debe asumir, consecuentemente se logrará tener un mejor manejo, control, regulación y aplicación del Derecho Informático, tomando en consideración que el nuevo estudiante de derecho debe contemplar en su ámbito de preparación profesional el abordaje de temas tales como dominio de software hardware, páginas web, comercio y contratos electrónicos, delitos informáticos, derechos digitales transfronterizos, entre otros.

CAPITULO II

Protección Jurídica de los Datos, Software y Contratos Informáticos.

2.1. El escenario actual de las bases de datos y su vulnerabilidad.

Cuando nos referimos a las bases de datos lo primero que viene a nuestra mente es un escenario en donde se encuentran una serie de computadoras, servidores y procesadores de texto u hojas de cálculo que contienen información. Adicional a ello debemos contextualizar que al hablar de los dispositivos de almacenamiento que resguardan información debe estar regulado en la legislación correspondiente con las instituciones jurídicas que coadyuven a la protección, adquisición, uso, dominio o propiedad de los mismos y es ahí en donde entra en función el Derecho Civil y Derecho Mercantil, además de la regulación legal de los Derechos de Autor en cuanto a la protección del software que en Guatemala actualmente es limitada, en varias legislaciones la tutela no se extiende a las bases de datos, solamente a la selección o disposición de los componentes del software.

Como lo refiere el autor Arean Velasco en su obra La Gestión de la Seguridad de la Información,

> la información puede ser protegida de muchas maneras. Desde el Derecho pudiera pensarse que se logra contar con un adecuado nivel de protección, con la encriptación, teniendo en cuenta que la mayor de las veces la compresión del tema tecnológico es poca; sin embargo, la encriptación es un mecanismo para otorgar a la información atributos de confidencialidad, integridad, autenticidad, y dependiendo del mecanismo de encriptación, podría reputarse el no repudio. En la protección de la información intervienen diferentes disciplinas, desde la informática, la gerencial, la logística, la matemática hasta la jurídica, entre muchas otras. (Velasco Melo, 2008).

Sigue señalando Arean Velasco que:

> tratándose de proyectos informáticos o telemáticos, que la mayoría de las veces son desarrollados por terceros para una organización, es importante tener en cuenta que éstos no pueden ejecutarse al margen de las políticas generales de seguridad del ente empresarial. En la medida en que se trata de terceras personas que tienen acceso a las redes, sistemas informáticos, infraestructura e información estratégica de la compañía, se debe tener presente que estos terceros, al interactuar con la organización, deben asumir una serie de obligaciones, cargas y deberes, así como los riesgos y responsabilidades que conlleva el indebido tratamiento de la información para el titular de tales activos; sin esta concepción holística del tema, es frágil cualquier sistema de gestión de la seguridad de la información. (Velasco Melo, 2008)

Actualmente tanto organizaciones públicas y privadas tienen esa preocupación de cómo atender las necesidades ante el imperioso volumen de información que día a día se acrecienta (Big Data), se dice además que quien tiene la información tiene el poder y eso es algo que se ha convertido en un lucro exageradamente oneroso para quienes se aprovechan de esa vulnerabilidad en el resguardo y tutela de la información o datos. Esto se debe a una débil legislación que atienda estas necesidades, además de los ciberataques[4], que sufren las diferentes organizaciones en contra de sus bases de datos o información y es que esto surge debido a que los usuarios finales no tienen la cultura de seguridad en el resguardo de la información.

A. Protección Jurídica de los Datos.

El profesor Arean Velasco puntualiza algunos aspectos que deben considerarse en la protección de datos desde el punto de vista jurídico, señala entonces que “La seguridad informática ha hecho tránsito de un esquema caracterizado por la implantación de herramientas de software, que neutralicen el acceso ilegal y los ataques a los sistemas de información, hacia un modelo de gestión de la seguridad de

[4] Un ciberataque o ataque informático, es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo de tomar el control, desestabilizar o dañar un sistema informático. https://es.wikipedia.org/wiki/Ciberataque

la información en el que prima lo dinámico sobre lo estacional. Para lograr niveles adecuados de seguridad se requiere el concurso e iteración de las disciplinas que tengan un impacto en el logro de este cometido, teniendo siempre presente que un sistema de gestión no garantiza la desaparición de los riesgos que se ciernen con mayor intensidad sobre la información. Entonces, el problema es determinar cómo desde una disciplina como el Derecho se contribuye a la gestión de la seguridad de la información." (Velasco Melo, 2008)

De conformidad a protocolos internacionales en materia de protección de la información, existe la ISO 27001, en el cual uno de los contenidos se enfoca a las buenas prácticas de seguridad de la información tanto en procesos internos como externos.

El profesor Arean Velasco señala algunos aspectos jurídicos referentes a la ISO 27001 indicando que la nutre normativa internacional y otras fuentes del derecho, señala entonces que este rubro de calidad contempla diez dominios los cuales son "1. Política de Seguridad de la Información 2. Organización de la Seguridad de la Información 3. Gestión de Activos 4. Seguridad de Recursos Humanos 5. Seguridad Física y del Entorno 6. Gestión de Comunicaciones y Operaciones 7. Control de Acceso 8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 9. Gestión de Incidentes de la Seguridad de la Información 10. Cumplimiento" (Velasco Melo, 2008)

Analizando el contenido del párrafo anterior opino que esta gestión de seguridad de información invita a los usuarios a que deben comprender el alcance e importancia de la gestión de la seguridad de la información y para ello deben implementar los mecanismos adecuados para disminuir o erradicar los riesgos que tiendan a la pérdida o alteración de la información.

Arean Velasco puntualiza que: "se identifican seis grandes temas desde la perspectiva jurídica: La protección de datos personales; la contratación de bienes informáticos y telemáticos; el derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos; los servicios de comercio electrónico; la

propiedad intelectual y el tratamiento de los incidentes informáticos.” (Velasco Melo, 2008)

B. Derecho a la privacidad e intimidad de la información.

El derecho a la privacidad en la era digital es un tema que preocupa tanto al sector público y privado en virtud que mucha información se encuentra abierta al público y sin ningún tipo de restricción en diferentes bases de datos y que es accesible desde diferentes motores de búsqueda o también llamados buscadores en internet, como ejemplo están Google, Aol, Duckduckgo, Bing, Yahoo, entre otros.

Guatemala a través de la Misión permanente ante las Naciones Unidas con sede en Ginebra, Suiza fue requerido por la Oficina del Alto Comisionado para los Derechos Humanos en relación a la protección y promoción de este derecho vital específicamente sobre la vigilancia doméstica y las interceptaciones telefónicas y más aún sobre la recolección de datos personales, esto de conformidad a la Resolución 68/167 denominada “El Derecho a la privacidad en la era digital” aprobada el 18 de diciembre de 2013 por la Asamblea General de las Naciones Unidas.

Es necesario recordar que la Constitución Política de la República de Guatemala reconoce y protege el derecho a la privacidad e intimidad, específicamente en el artículo 24 “Inviolabilidad de correspondencia, documentos y libros” cuyo contenido se enfatiza a la protección de datos y actividades personales, documentos y medios de comunicación, no obstante ello, estos extremos son vulnerados en virtud de la escasa regulación, ambigüedad y desconocimiento que se tiene sobre derecho informático, *Lato Sensu*.

La excepción a la regla en cuanto al derecho a la privacidad e intimidad es que al momento de la coexistencia entre la noticia criminal y un expediente de investigación en cuya hipótesis y diligencias a realizar se ve necesaria la implementación de métodos especiales de investigación, tal como las Interceptaciones telefónicas reguladas en la Ley contra la Delincuencia Organizada; es cuando el ente fiscal solicita al Juez contralor de la investigación la implementación de este método donde surge esta excepción, en virtud que se limita el derecho a la privacidad e intimidad de las

comunicaciones, de conformidad a los principios necesidad e idoneidad de la medida, norma jurídica que indica:

"**Artículo 51. Necesidad e idoneidad de la medida**. *Se entenderá que existe necesidad de la interceptación de las comunicaciones cuando, los medios de investigación realizada demuestren que en los delitos cometidos por miembros de grupos delictivos organizados se estén utilizando los medios de comunicación establecidos en la presente Ley. Asimismo, se entenderá que existe idoneidad del uso de la interceptación de las comunicaciones cuando atendiendo a la naturaleza del delito, se puede determinar que la interceptación de las comunicaciones es eficaz para obtener elementos de investigación que permitan evitar, interrumpir o esclarecer la comisión de los delitos ejecutados por miembros de grupos delictivos organizados".* (Guatemala C. d., 2006)

Actualmente existe un incremento y un riesgo critico en la vulneración e intromisión a la privacidad e intimidad de las personas y es por ello que el poder punitivo de Estado entra en función a través de sus diferentes mecanismos, uno de ellos es la regulación que posee el Código Penal Decreto 17-73 del Congreso de la República, en relación a tipos penales informáticos. Dicho esto, también debo apuntar que es necesario tener un control sobre los datos personales registrados en los diferentes entes estatales o en el sector privado ya que la alteración, manipulación, vulneración o divulgación de la misma sin el consentimiento del titular, ocasiona un gran perjuicio a las personas en su entorno personal, social, profesional, consecuentemente se origina un agravio a sus derechos inherentes como el honor, intimidad y la dignidad humana. Un ejemplo claro está la forma en que las entidades bancarias comercializan la información entre sí no obstante que no existe el consentimiento del titular. Muchas veces estas bases de datos son obtenidas en forma anómala y astuta, hay que recordar que existe una normativa legal que es la Ley de Acceso a la Información Pública, Decreto 57-2008 del Congreso de la República, regulando lo atinente a la protección de los datos personales. Esta ley establece estos parámetros en su apartado de Habeas Data en donde se estipula lo relativo al tratamiento de los datos y corrección que solicite la parte afectada.

De conformidad a la Resolución 68/167 “El Derecho a la Privacidad en la era Digital de la Comisión Presidencial de los Derechos Humanos plantea que:

> El Estado de Guatemala reconoce y protege el derecho a la privacidad e intimidad de las personas que es un derecho humano de todas las personas, en donde se debe propiciar el libre desarrollo de la personalidad y la protección sobre sus datos personales, actividades personales, documentos y medios de comunicación. La Constitución Política de la República de Guatemala establece que por ningún motivo se puede violentar la privacidad en correspondencia, documentos y libros, punto desde el cual se garantiza el secreto a la correspondencia y de las comunicaciones digitales, radiofónicas, cablegráficas y otros productos de la tecnología moderna debido a que la tecnología informática de la actualidad da paso a que esta clase de comunicaciones sea susceptible de ser vulnerada. Por otra parte este mismo cuerpo legal establece la protección a la dignidad humana, con el fin de que no se violente este derecho inherente a toda persona humana, al ser espiadas en los ámbitos anteriormente mencionados, debido a que las comunicaciones, programas digitales, de alta tecnología e informática son una herramienta de gran utilidad en la actualidad, también son parte de un medio al cual es fácil de vulnerar y ser medio de intromisión a la privacidad e intimidad de las personas, por tanto se establece tener un control a través del Código Penal que regula los delitos informáticos en donde se prevé la alteración, destrucción, manipulación, de registros o programas informáticos y el uso de información e utilización de programas destructivos…También establece que se debe tener un control sobre todos los datos personales, garantizando la protección sobre el uso indebido en el manejo que se debe dar a cada uno de estos datos, en especial para el tratamiento dentro de las empresas y otros establecimientos, donde el mal manejo de esta información pudiera causar algún prejuicio en el entorno personal, social y profesional de las personas, causando agravios a sus derechos inherentes como la intimidad, el honor y la dignidad humana. La

comercialización de datos personales de los diferentes bancos de datos que se han generado por particulares, ha sido una problemática actual debido a la facilidad en el acceso y manipulación de estos. Por lo que en la Ley de libre acceso a la información se establece la protección de estos derechos, que sin consentimiento de las personas sus datos personales no pueden ser distribuidos y deben estar enterados de la información que conste de ellos en archivos, fichas, registros o cualquier otra forma de registros públicos, y de la finalidad de la misma. La ley establece esto dentro de su apartado de habeas data en donde también se estipula el tratamiento que deberán llevar los datos y la corrección que de ellos se solicite por la parte afectada. (Comisión Presidencial, 2014)

Es necesario entonces citar algunos ejemplos que se citan en el documento relativo a “El Derecho a la Privacidad en la era Digital”, de la Comisión Presidencial de Derechos Humanos, en donde detalla “El Estado de Guatemala cita la opinión emitida por la Corte de Constitucionalidad en relación al derecho a la privacidad” (Comisión Presidencial, 2014), detallando los siguientes expedientes:

i. (Derecho a la privacidad) “Expediente 863-2011 de fecha 21/06/2011*: Esta Corte ha indicado que las doctrinas modernas que ponderan la vigencia y respeto debido a los derechos humanos, sostienen un criterio vanguardista respecto de que el catálogo de derechos humanos reconocidos en un texto constitucional no puede quedar agotado en éste, ante el dinamismo propio de estos derechos, que propugna por su resguardo, dada la inherencia que les insta respecto de la persona humana. Esto es así, porque es también aceptado que los derechos fundamentales no sólo garantizan derechos subjetivos de las personas, sino que, además, principios básicos de un orden social establecido, que influyen de manera decisiva sobre el ordenamiento jurídico y político de un Estado, creando así un clima de convivencia humana, propicio para el libre desarrollo de la personalidad. La Constitución actualmente vigente en la República de Guatemala, que propugna por el reconocimiento de la dignidad humana como su*

fundamento, no puede obviarse que los derechos fundamentales reconocidos en dicho texto no son los únicos que pueden ser objeto de tutela y resguardo por las autoridades gubernativas. Existen otros derechos que por vía de la incorporación autorizada en el artículo 44 de la Carta Magna o de la recepción que también autoriza el artículo 46 del Texto Matriz, también pueden ser objeto de protección, atendiendo, como se dijo, a su carácter de inherentes a la persona humana, aun y cuando no figuren expresamente en este último texto normativo…" Del derecho al reconocimiento de la dignidad humana, implícitamente garantizado, entre otros, en los primeros cinco artículos de la Constitución Política de la República, dimanan, por el contenido esencial de este derecho, aquellos relacionados a la intimidad, al honor y a la privacidad, los cuales, en su conjunto, también garantizan la existencia y goce de otro derecho: el referido a la autodeterminación informativa...

a. *Los derechos a la intimidad y al honor requieren de una protección jurídica especial que posibilite, a su vez, una protección social del "yo" de cada persona en el ámbito jurídico de los demás. Esto debe impedir que, bajo subterfugios, pueda darse a conocer a terceros diversas situaciones calificadas por el conglomerado social como deshonrosas, atentatorias de la honra personal, la propia estimación y el buen nombre o reputación de una persona y que afecten a ella en su propia individualidad; derechos estos últimos que son propios de los principales atributos de la persona humana: la personalidad.*

b. *No es ajeno al conocimiento de este tribunal que el derecho a la intimidad propugna por un mínimo respeto a un ámbito de vida privada personal y familiar, que es aquél que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo aquéllas en las que sea el propio particular quien autorice su divulgación... También es insoslayable que la intromisión a este derecho puede alcanzar niveles insospechados con el avance de la tecnología actual y la transmisión de información por medios de comunicación masiva. Los avances de la tecnología informática*

generan a su vez una dificultad en cuanto a proteger adecuadamente el derecho a la intimidad y a la privacidad de una persona individual. Una solución a esa problemática ha sido la de reconocer el derecho a la autodeterminación informativa del individuo, cuyo goce posibilita a éste un derecho de control sobre todos aquellos datos referidos a su persona y, a su vez, le garantiza la tutela debida ante un uso indebido (es decir, sin su autorización) y con fines de lucro, por parte de un tercero, de todos aquellos datos personales susceptibles de tratamiento automatizado, con los cuales se integra una información identificable de una persona; información que cuando es transmitida a terceras personas sin los pertinentes controles que permiten determinar su veracidad o actualización, puedan causar afectación del entorno personal, social o profesional de esa persona, causando con ello agravio de sus derechos a la intimidad y al honor…" (Expediente 863-2011 , 2011)

ii. (Comercialización de información personal) "Expediente 863-2011 de fecha 21/06/2011*: "La obtención de datos personales que puedan formar una base de datos, susceptible de transmisión por medios de comunicación masiva o electrónica -por medio de la informática-, debería ser objeto de regulación por una ley… En Guatemala no existe tal regulación, y en tanto no la haya, para no incurrir en situaciones legibus solutus, a criterio de esta Corte toda comercialización de información de datos de una persona debe estar sujeta a que esa información fuera proporcionada voluntariamente por la persona, cuyos datos serán objeto de comercialización; y que al momento de obtenerse, se le haya garantizado a dicha persona los derechos de actualización, rectificación, confidencialidad y exclusión antes citados, como una forma de resguardar los derechos fundamentales a su intimidad personal, privacidad y honor. Se acota que si bien la comercialización de datos personales pudiera estar comprendida en el ejercicio del derecho que garantiza el artículo 43 constitucional, este último encuentra una limitación en el derecho a la dignidad humana, el cual prevalece sobre aquél; de manera que ante esa prevalencia y salvo lo que en contrario*

pueda disponerse en leyes específicas, se sostiene que todas aquellas personas individuales o jurídicas que realicen actividades de comercialización de información obtenida de registros o bases de datos personales, deberían, al comercializar tal información, por lo menos, observar: a) los datos que para tal efecto hubiesen obtenido, lo hayan sido conforme una finalidad plenamente definida, de forma legítima y de manera voluntaria por parte de aquél cuyos datos vayan a ser objeto de comercialización; b) la utilización de esos datos personales debe hacerse sin obviar un previo asentimiento de la persona interesada, utilización que debe realizarse con un propósito compatible con aquél para el que se hubiesen obtenido; y c) el registro y utilización de los mismos debe conllevar, necesariamente, la implementación de controles adecuados que permitan, por aquél que disponga de esos datos, la determinación de veracidad y actualización de los mismos por parte y como una responsabilidad de quien comercializa con los mismos, y el amplio goce del derecho a la rectificación de estos por aquél que pudiera verse afectado en caso de una errónea o indebida actualización. Así las cosas, toda comercialización de datos personales que no observe tales parámetros (cuya enunciación es enumerativa y no limitativa), podría derivar en una actividad ilegal, violatoria de derechos fundamentales, que conllevaría responsabilidad legal tanto para aquéllos que proporción en tales datos como para quienes que se sirvan de ellos en la toma de decisiones respecto de situaciones relacionadas con una persona en particular. …" (Expediente 863-2011 , 2011)

iii. (Tutela Judicial de los registros personales) "Expediente 863-2011 de fecha 21/06/2011: *"Reconocida entonces la existencia del derecho de una persona a determinar la existencia o inexistencia de registros o bases de datos en los que consten sus datos personales, y de obtener una rectificación, supresión o eventual bloqueo de los mismos, si en la utilización indebida de éstos se pueda, en efecto, afectar su intimidad y honor, corresponde ahora determinar la manera en la que puede solicitarse la tutela judicial de tales derechos sabido que en la legislación comparada y de acuerdo con la doctrina procesal constitucional*

moderna, la tutela de tales derechos se hace por medio de la acción procesal denominada "hábeas data", misma que en Guatemala está establecida en el Decreto cincuenta y siete – dos mil ocho (57-2008) de la Ley de Acceso a la Información Pública… Por tal razón, esta Corte sostiene que por la amplitud con la que está establecido el ámbito de conocimiento del amparo, este último resulta ser la acción constitucional idónea para garantizar el derecho que a toda persona asiste de acceder a su información personal recabada en bancos de datos o registros particulares u oficiales … o cuando esos datos sean proporcionados por personas individuales o jurídicas que prestan un servicio al público de suministro de información de personas, a fin de positivar aquellos derechos de corregir, actualizar, rectificar, suprimir o mantener en confidencialidad información o datos que tengan carácter personal…" (Expediente 863-2011 , 2011)

En relación a la privacidad: Al analizar el razonamiento contenido en estos expedientes observamos que la Corte de Constitucionalidad emite un análisis sobre la autodeterminación informativa que tiene límites en cuanto la protección y divulgación de información de una persona esto para defenderlo de ataques en contra de su honor y privacidad. Se tiene claro que el avance de la tecnología también implica que se mejoren los controles sociales y legales para proteger los derechos inherentes a la persona humana, en este caso la autodeterminación informativa y esto se alcanza mediante una actualización constante de los diferentes institutos jurídicos en relación a la protección de la información.

En relación a la comercialización de la información personal: Es interesante observar que la Corte de Constitucionalidad emite un razonamiento en donde señala que en Guatemala no existe una regulación legal sobre transmisión de datos personales a través de medios de comunicación masiva o electrónica, misma que en el campo del Derecho Informático se le conoce como BIG DATA, haciendo referencia a que si bien es cierto que la comercialización de la información se fundamenta en el artículo cuarenta y tres de la Constitución Política de la República de Guatemala, este tiene un límite consistente en que prevalezca el derecho a la dignidad humana.

Además indica que si en algún momento se omite esa autorización del propietario de la información personal en divulgarla, para que pudiese ser válida al menos debe ser legitima, su utilización debe ser de la misma naturaleza para la que fue creada y con la flexibilidad de rectificación por el sujeto de quien se divulga la información, de lo contrario se estaría vulnerando unos de los principios fundamentales que es el derecho a la privacidad e intimidad, consecuentemente se deducirían las responsabilidades legales correspondientes.

En relación a la tutela judicial de los registros personales: Específicamente nos refiere al fundamento legal para la protección de esta información que es el Decreto 57-2008. Ley de Acceso a la Información Pública, puntualizando que el Amparo es la vía idónea para restablecer este derecho.

Han existido diferentes iniciativas que han surgido con el fin de regular lo relativo al tema de tutela a la privacidad e intimidad de las personas (Habeas Data) y lo concerniente al Derecho Informático, tal es el caso de la iniciativa 4054 "Ley contra el Cibercrimen" además de otras como la iniciativa 4055 y 4090, mismas que se desarrollaran más adelante.

C. La Protección de Datos en el Derecho Comparado.

En el tema de protección de datos es menester analizar que en el año 1980 se conformó La organización para la cooperación y desarrollo económico que fue la primera en adoptar el mecanismo para la protección de datos y en materia de privacidad de la información (OCDE). Esta organización es un modelo a seguir en diferentes países de globo terráqueo Como por ejemplo se incluye a Israel, Japón, Australia, Canadá, Chile, Estados Unidos y México. (GDPR Legal, 2018)

En diferentes países del mundo el tema de la protección de datos se regula de diversas formas, existiendo y funcionando el andamiaje jurídico que busca la tutela a este derecho, por ejemplo tenemos el caso de España en donde existe una ley que se llama "Ley de Protección de Datos" que se contextualiza o se acopla a los estándares de Europa, siendo España uno de los países que más ha avanzado en el tema de protección de datos a nivel mundial debido a que existen diferentes instituciones y

entes públicos y privados que se han encargado de ir mejorando las condiciones de seguridad de la información de este país. En Europa actualmente Funciona el reglamento general de protección de datos (RGPD) y que aplica para toda Europa.

Para regular la protección de datos también deben de considerarse aspectos, sociales, económicos, culturales, demográficos, jurídicos y políticos ya que existe diferencia entre la regulación de Europa y la de Estados Unidos de América. En Estados Unidos se cumplen diferentes protocolos y principios para la seguridad de la información mismos que son autoevaluables a través de diferentes certificaciones. En el plano internacional Europa ha tenido mayores avances en implementar mecanismos para la protección de datos y seguridad de la información ya que en el caso de Estados Unidos este tipo de seguridad se enfoca más a temas militares, armas químicas y tecnología utilizada para otros fines, sin embargo en el tema de protección de datos y seguridad de la información en Estados Unidos es común la vulneración de la seguridad y privacidad de la información, ejemplo de ello es la empresa Google, qué es uno de los mayores entes vulneradores de la privacidad de la información del mundo.

Como se apuntó anteriormente España que es parte de la Unión Europea es uno de los países que tiene una interesante estructura normativa jurídica qué se enfoca a diferentes elementos y aspectos del derecho informático en este caso nos referimos a la protección de datos, es por ello que existe desde el año 1999 una Ley Orgánica de protección de datos qué está enfocada especialmente a la protección del honor, intimidad y privacidad de las personas y de carácter familiar. Y es que raíz de ello surgieron diferentes instituciones encargadas de velar por la por el efectivo cumplimiento de esta normativa cómo lo es la agencia española de protección de datos (AEPD). Además, es necesario apuntar que dentro del objetivo fundamental de este ente es la protección en forma integral de los datos de las personas ya sea en el ámbito público como privado. Al referirnos a la protección de datos podemos estudiarlo desde el punto de vista de la intimidad o de carácter personal en cuanto a los registros públicos y privados, información que responde a datos sensibles de las personas

Existe en Guatemala una serie de empresas que comercializan con información y que prestan este tipo de servicios al sistema bancario para poder crear un perfil del

estatus económico financiero para poder otorgar créditos y para nadie es un secreto que el mismo sistema bancario a través de las diferentes entidades financieras se transmiten o comercializan la información a efecto de contactar al usuario final, todo esto con carácter lucrativo. También podemos estudiar la protección de datos desde el punto de vista de la circulación utilización y consulta de datos en la internet, la información que se almacena en los diferentes servidores de correo electrónico, servidores de mensajería instantánea y los ficheros que se almacenan en diferentes plataformas virtuales y que contienen información elemental de una persona individual o colectiva.

Al hacer la consulta en la enciclopedia virtual de Wikipedia es interesante leer lo referente a la Red Iberoamericana de protección de Datos (RIPD) en cuyo contenido en su parte conducente indica que “En América Latina se están desarrollando políticas para la protección de los datos personales. En 2012 se aprobaron dos nuevas leyes. En Nicaragua, la Ley Nº787 de Protección de Datos Personales, de 29 marzo de 2012 y la Ley Estatuaria Nº1581 del 17 de octubre de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales. En Chile, asimismo la Ley 19.628, de 28 de agosto de 1999, sobre Protección a la Vida Privada, se encuentra actualmente en un proceso de revisión de parte de su articulado. La Asamblea Nacional de Venezuela está tramitando el proyecto de ley de Protección de Datos Personales de Habeas Data. Y en Costa Rica ya existe una Agencia de Protección de datos de la República de Costa Rica, en cumplimiento de la ley aprobada en 2011”. (Wikipedia, s.f.)

D. La protección de datos y la libertad de expresión como garantía constitucional. La neutralidad de la red.

Este aspecto es muy interesante y tal como lo refiere la Organización de Estados Americanos en el texto “Estándares para una Internet libre, abierta e incluyente”, la neutralidad de la red ha sido reconocido por la Relatoría Especial para la libertad de expresión de la Corte Interamericana de Derechos Humanos como “una condición necesaria para ejercer la libertad de expresión en Internet en los términos del artículo 13 de la Convención Americana” Lo que persigue tal principio es que la libertad de

acceso y elección de los usuarios de utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal por medio de Internet no esté condicionada, direccionada o restringida, por medio de bloqueo, filtración, o interferencia. (Organización de Estados Americanos)

a. Protección de datos en Guatemala y la libertad de expresión como garantía constitucional.

Cuando nos referimos a la protección de datos automáticamente debemos analizar e interpretar toda la normativa jurídica qué se encarga de dar ese resguardo y protección de la información que existen en registros públicos y privados, en ese sentido la información de carácter público se encuentra en los diferentes entes estatales como por ejemplo la información que se almacena en el Registro Nacional de las Personas, Registro de la Propiedad, Registro de Información Catastral, Registro de Personas Jurídicas, entre otros; al referirnos a la información que existe en el ámbito privado nos trasladamos al escenario de las empresas privadas y es ahí cuando nos debemos de hacer la siguiente interrogante: ¿Existe en Guatemala la normativa jurídica adecuada qué se encarga de la protección de datos de las personas?. Es menester citar lo que para el efecto establece y señalan los considerandos de la Ley de Acceso a la Información Pública y para ello se debe contextualizar el primer considerando de ésta normativa indicando que la Constitución Política de la República de Guatemala garantiza la publicidad de los actos y la información que se encuentra en la Administración Pública y que puede accederse en forma libre a salvo lo establecido en algunas excepciones que también lo señala nuestra Carta Magna, además en el segundo considerando se refiere que la misma información puede ser de acceso público a excepción de la información que se considera como confidencial y reservada. El Decreto 57-2008 del Congreso de la República se refiere a esa información de carácter público que se puede encontrar en las diferentes oficinas o entidades del estado y que mediante las diferentes unidades de información públicas que existen cada una de ellas una persona que tiene interés puede acceder a ellas llenando los requisitos de ley y con las excepciones que la misma legislación regula, el artículo 19 de este cuerpo legal se refiere a estas unidades de información pública.

El artículo 21 de la citada normativa se refiere los límites de acceso a esta información y eso se rige de conformidad a lo que se establece en la Constitución Política de la República de Guatemala, además es menester recordar que existe información confidencial o que está clasificada como Reservada. Es imperativo analizar lo que refiere el artículo 30 del Decreto en mención, que enmarca en su epígrafe como el “Habeas Data”, en el entendido que la administración pública debe tener los procedimientos adecuados para poder dar la información pública requerida al interesado y que en este caso el sujeto activo de esta solicitud es decir el particular no puede usar la información para fines comerciales salvo que así sea autorizado por la entidad que haya aprobado la entrega de esta información. Es interesante analizar lo que establece el artículo 36 de esta ley que se refiere a la salvaguarda de los documentos específicamente que los archivos administrativos no se puedan destruir o modificar o crear algún tipo de perjuicio en contra de la administración pública.

Los entes encargados de resguardar esta información deben hacer cumplir esta normativa, no obstante, debemos ir más allá y preguntarnos lo siguiente: ¿qué pasa con esta información si se encuentra almacenada en servidores o en bases de datos y no se cuenta con los protocolos de seguridad necesarios para mantener resguardada la información? Y es que debemos entender qué en la Nueva Era digital toda la información de los entes públicos se encuentra en grandes servidores que almacenan toda esta información y esto responde a la llamada “Big Data” que no es más que el manejo de grandes volúmenes de información y que se encuentran almacenadas en diferentes lugares, que en muchas ocasiones son lugares poco convencionales. En virtud del volumen de la información, deben existir una serie de protocolos inteligentes para el almacenamiento y resguardo de la información para que exista plena certeza de privacidad y seguridad de la información. Todo esto también podemos integrarlo de conformidad a lo que establece el artículo 2 de la Constitución Política de la República de Guatemala referente a la Seguridad Jurídica y el artículo 29 de nuestra Carta Magna en cuanto al libre acceso a tribunales y dependencias del Estado; eso debemos de interpretarlo como la forma en la cual el estado tutela la protección de la información que se encuentra en diferentes registros para proveerles de una seguridad jurídica y esto se concatena con lo que establece el artículo 30 de la misma Constitución en

cuanto a la publicidad de los actos administrativos ya que los interesados o administrados pueden obtener la información y efectuar las consultas de los registros que se encuentran en los diferentes entes estatales sin olvidar lo que indica el artículo 31 de la Constitución, es interesante porque aquí nos refiere a que toda persona puede conocer toda aquella información que exista en cualquier registro estatal.

Analicemos y contextualicemos el artículo 31 de la Constitución Política de República de Guatemala cuyo contenido se refiere al "Acceso a archivos y registros estatales"; existió un caso en el cual una empresa privada se dedicó a recopilar la información de las personas y efectuó una perfilación individual de las personas junto a las deudas, embargos o cargas económicas que figurarán en el sistema bancario del país y ello le servía para formar una base de datos que posteriormente se la vendía a otros entes del sistema bancario que daban la pauta para poder otorgar o no créditos a las personas, es decir sin ningún tipo de consentimiento la empresa privada comercializó la información de carácter personal de diferentes ciudadanos y con ello se empezó a negar el derecho a un crédito o incluso a un trabajo, evidentemente colisionando derechos fundamentales consagrados en nuestra Carta Magna.

b. Neutralidad de la Red.

Así como lo refiere (Rodriguez, Legislación y Etica Profesional, 2013) "Se reconoce que la neutralidad de Internet bajo los siguientes aspectos:

1. No debe existir discriminación entre las aplicaciones que se transportan y se utilizan; 2. Todo actor de la red puede ofrecer contenidos desde cualquier punto de la red sin que esté sometido a control alguno; 3. Ningún usuario de Internet, tampoco los prestadores o intermediarios de la Internet que difunda datos puede ver alterados, en su contenido, los mismos.

El principio que se aplica según comentan los analistas de la evolución tecnológica y en especial de la Internet es el principio "end to end"[5] (e2e) es lo que

[5] Es un término que se utiliza para indicar que un proveedor de software, además de suministrar una solución, estará presente en todas las fases de interacción de un cliente con esa solución. El proveedor participará en su implementación, integración y configuración y hará un posterior seguimiento con el

permite que quien emite y quien recibe información por la red pudieran ser intercambiados sin ningún inconveniente por parte de los intermediarios que ayudan al envío de los datos. Opino que esta teoría es totalmente libre y no pone ninguna limitante se considera que en nuestra actualidad es nefasto en virtud que deben existir los protocolos necesarios para que una persona pueda navegar, transportar, transmitir, crear e intercambiar la información sin crear una limitante que obstaculice el libre desarrollo de la información a través del internet.

Sigue manifestando el autor Rodríguez que:

> entonces, las restricciones, limitaciones o prohibiciones universales al régimen de neutralidad constituyen una amenaza directa a la libertad de expresión, pues si alguien, regulación mediante, puede actuar sobre la red estableciendo que contenidos pueden almacenar y transportar la red caemos en la figura de la censura digital. La ley prevé que frente a la comisión de acciones delictivas se pueden aplicar las sanciones previstas para cada caso. (Rodriguez, Lecciones de Derecho y Etica Profesional)

Postura en la cual no estoy de acuerdo en virtud que incluso las limitantes también coadyuvan a que la libre emisión el pensamiento se dé con mayor objetividad y seguridad tanto para el receptor como para el emisor del mensaje. Al tratar el tema de la responsabilidad que se tiene en cuanto al manejo de la información en las redes debemos de situarnos en la postura de si es un control o una libertad, para entender puntualmente este tema es necesario reflexionar que la información que circula en las redes existen diferentes registros tanto públicos como privados, y que existen diferentes filtros y controles necesarios para salvaguardar la información a manera de que pueda existir esa certeza jurídica que nos reza el artículo dos de la Constitución Política de la República de Guatemala. Es evidente que en Guatemala el tema de protección de datos aún se ve limitada y tiene mucho que mejorar en virtud que el sistema es deficiente y son escasos los mecanismos legales necesarios que puedan atender a esta necesidad del imperioso avance de la tecnología.

---

cliente del funcionamiento de la solución. https://algoritmia8.com/2019/12/12/end-to-end-solutions-proveedores-aliados/

Después de abordar algunos puntos referentes a la protección de los datos e información debemos considerar la necesidad de la existencia de limitantes o control de la información que circula en redes, por ello debemos reflexionar sobre la gran influencia de las redes de información que coexisten a nivel mundial y es por eso qué debemos advertir qué a la fecha la era digital se hace presente de diversas formas en nuestras vidas ejemplo de ello está el uso de un teléfono o un dispositivo inteligente, las redes sociales, el correo electrónico, el uso de un dron, entre otros. Y es procedente preguntarnos: ¿cómo deben de ser los controles necesarios para el uso del internet? ¿O es acaso que existe una libertad plena para omitir sus controles? Citemos algunos ejemplos a través de los cuales se puede evidenciar la forma en que el abuso o el uso excesivo de manejo de información puede atentar o puede condicionar diferentes derechos. Primero, el caso que se dio ya hace unos años de una empresa proveedora de servicios cuyo nombre comercial y en redes era “Taringa” que tenía sus bases de datos con todo tipo de contenido tales como: música, videos, libros en pdf, entre otros y todo esto ocasionaba un grave perjuicio a los autores de este tipo de contenido. Cuestionémonos entonces ¿cuál es el nivel de responsabilidad de estos sitios intermediarios que proveen la información y que son entregados al usuario final?

Cómo lo apuntaba al inicio debe existir un control sobre el tipo de información que está en red y no entenderlo como una restricción a la libertad de expresión o de la información que circula sino más bien para proteger y tutelar otros derechos, incluyendo la propiedad intelectual. Un ejemplo interesante sobre este tema de propiedad intelectual y el debate sobre la neutralidad del internet es el caso de la página llamada “Megaupload” ya que este sitio también almacenaba diferente tipo de contenido para que fuera descargado por los diferentes usuarios y es de conocimiento público que este sitio fue cerrado porque también atentaba contra los derechos de autor y esto se conoce como un ejemplo sobre la mayor afectación en cuanto a la neutralidad del internet.

Entonces, las restricciones, limitaciones o prohibiciones universales al régimen de neutralidad constituyen una amenaza directa a la libertad de expresión, pues si alguien, regulación mediante, puede actuar sobre la red estableciendo que contenidos

pueden almacenar y transportar la red caemos en la figura de la censura digital. La ley prevé que frente a la comisión de acciones delictivas se pueden aplicar las sanciones previstas para cada caso. (Clarin, 2013, pág. 26).

2.2. Protección del Software.

A. Generalidades sobre programas de computación y derechos intelectuales.

Es necesario contextualizar algunos términos que serán de utilidad, como por ejemplo la llamada “computación en la nube” o el Cloud Computing que “permite ofertar y prestar servicios a través de Internet, se trata de un servicio al que se puede acceder sin necesidad de contar con conocimientos especiales de ninguna naturaleza, se trata según la literatura especializada de un prototipo en el cual la información se almacena en servidores de forma permanente y desde allí puede enviarse a archivos temporales de cliente” (Rodriguez, Legislación y Etica Profesional, 2013)

Sigue manifestando el autor en el texto citado que:

> sin mayor esfuerzo podemos inferir que desde el punto de vista económico una copia autorizada resulta de mayor precio que una “pirata” que al no contar con la debida autorización legal el precio de comercialización resulta muy inferior al precio real, constituyendo este “spreed”, este delta, una posibilidad de mayores “ganancias”. Aseguran autores de prestigio que “la facilidad y el bajo costo con que pueden copiarse los programas de computación, han brindado condiciones para el nacimiento a un mercado “paralelo” de copias ilegítimas…” (Rodriguez, Legislación y Etica Profesional, 2013)

El autor además manifiesta que existen motivaciones que originan esta vulneración a la venta de copias no autorizadas de programas de computación señalando que “muchas veces resultan exageradamente inferiores a los originales, aunque entre las desventajas que esta modalidad de adquisición de programas en el mercado “pirata” cabe mencionar el apoyo posventa, muy importante en la solución de

los problemas que el uso del programa puede ocasionar, y otra desventaja a citar es la imposibilidad de recibir nuevas versiones, aspecto este que si se adquiere el programa original, legal, puede recibirse y actualizarse el software sin mayores costos." (Rodriguez, Legislación y Etica Profesional, 2013)

a. Protección Jurídica del Software

En diferentes países se regula lo relativo a la protección de los programas que sirven para los ordenadores o computadoras, hoy en día en las diferentes legislaciones de los países existen leyes que regulan el derecho a la creación de la persona en una de las áreas de la tecnología, es decir la creación de programas de computación y es que esto corresponde a la creación en base al intelecto y a la destreza de una persona, siendo qué en muchos países los programas de computación se conozcan dentro de la regulación legal sobre los derechos de autor.

En la industria de la creación de programas de computación al inicio se tenía entendido que esto correspondía a una parte interna de los dispositivos o de las computadoras, no obstante, durante el avance de la tecnología se ha visto en la necesidad de crear mecanismos acordes tanto para la protección de los dispositivos electrónicos como también para la creación de estos programas de computación. Actualmente los mecanismos de protección son insuficientes debido a la particularidad de estos programas ya que éstos pueden ser desde una simple aplicación para un dispositivo móvil como también programas avanzados en donde se manejen diferentes bases de datos o incluso la forma en que se almacena la información en las diferentes nubes o Cloud y esas nubes responden al funcionamiento de un programa que hace funcionar dichos servidores de base de datos.

En Guatemala el tema de la propiedad intelectual se divide en dos ramas cómo es la Propiedad Industrial y los derechos de autor y derechos conexos. Surge entones la interrogante: ¿cuáles son los mecanismos adecuados y contextualizados para tutelar la creación, mantenimiento y respeto a los diferentes programas de computación?

b. Propiedad Intelectual y Propiedad Industrial

La propiedad intelectual recordemos que se refiere a las creaciones de la mente o el intelecto, además se refiere a la creatividad que tiene el ser humano para poder crear diferentes obras, símbolos, nombres, entre otros, para ello debemos observar en lo que para el efecto establece el artículo 15 de la Ley de Derechos de Autor y Derechos conexos en donde se refiere a que son todas aquellas producciones en el campo de la literatura, científico y artístico es decir cualquier forma de expresión y es aquí donde se incluyen los programas de ordenador o software, quedando limitado a esa esfera, es entonces que podemos inferir que la protección jurídica del software debemos de ubicarlo en los preceptos de la propiedad intelectual. Tal y como lo comentamos anteriormente si nos referimos a la protección jurídica del software obviamente debe existir un ente encargado de velar por su momento de sancionar las faltas o aquel perjuicio que se pueda ocasionar al creador de esa manifestación de expresión referente a software es por eso que aquí entra en juego el rol que desempeñan los diferentes órganos jurisdiccionales y específicamente en lo que desempeña el Ministerio Público.

El ente encargado de la persecución penal en Guatemala tiene una organización administrativa diversa y dentro de ella se encuentra la Fiscalía de Delitos contra la Propiedad Intelectual que dentro de sus funciones se encuentra la investigación y persecución de todos aquellos delitos o faltas en contra de los derechos de autor y derechos conexos y ellos lo podemos encontrar en lo que para el efecto establece el artículo 127 de la ley Derechos de autor y Derechos Conexos. Asimismo, el artículo 42 de la Constitución Política de la República de Guatemala regula lo relativo a los derechos de autor y derechos de inventores y que tiene una propiedad exclusiva de conformidad a la ley ya los tratados internacionales. Es complejo concebir y aceptar que esta fiscalía es la competente de conocer de ciberdelitos[6] y paralelamente conozca de los asuntos ya mencionados, es acá en donde debe promoverse una reforma

[6] Delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

integral en virtud de la diferencia y especialización con la que debe abordarse el fenómeno criminal.

En ese mismo orden de ideas es necesario acotar que existen actos reprochables objetos de una sanción cuyo bien jurídico tutelado es atentar en contra de la creación de la persona humana referente a la propiedad intelectual, citamos como ejemplo el artículo 274 “C” del Código Penal -Reproducción de instrucciones o programas de computación- en donde el supuesto es en contra del responsable de la copia o reproducción sin la debida autorización referente a programa o instrucciones de computación, acá el bien jurídico tutelado es el Derecho de Autor.

Es interesante analizar que este tipo penal no establece el momento de la efectiva consumación del hecho, es decir, cuando se está vulnerando el derecho del autor al momento de poder alterar o reproducir en forma ilícita un programa o software, en virtud que el aventurarnos a decir que la consumación se da por el simple hecho de copiar metadatos de un lugar a otro y qué eso se presume como una ilicitud, esto contraviene al principio de taxatividad de la norma jurídica en virtud que deben ser cerrados y no abiertos toda vez que si se aplican e interpretan de esta forma tienden a la ambigüedad y a la confusión atentando contra la protección del bien jurídico tutelado, seguridad jurídica, legalidad y debido proceso.

Al seguir analizando lo que regula o abarca los derechos de autor y derechos conexos podemos encontrar entonces que se encuentran todos aquellos derechos que están incorporados a la creación del autor de la obra o producción y es que la misma ley indica que hay derechos inherentes a la creación del ser humano como por ejemplo el Registro de Obras, Patentes y otras; en el marco internacional existen diferentes convenios suscritos por Guatemala en materia de propiedad intelectual, siendo los más relevantes: El Convenio de París, Convenio de Berna, entre otros. Es interesante analizar algunos artículos del Decreto 33-98 del Congreso de la República “Ley de Derechos de Autor y Derechos Conexos”, tales como:

ARTICULO 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. La documentación técnica y los manuales de uso de un programa gozan de la misma protección prevista para los programas de ordenador.

ARTICULO 31. El derecho de arrendamiento incluido en la literal e) del artículo 21 de la presente ley, no es aplicable a los arrendamientos cuyo objeto esencial no sea el del programa de ordenador en sí.

En el Derecho Comparado, por ejemplo, en Argentina existe la normativa que protege de una forma muy particular al software como por ejemplo en el artículo 1 de la Ley del Software que establece y refiere sobre el código fuente, haciendo referencia a un lenguaje de programación y que dentro de este lenguaje se encuentra un código objeto que resulta de la conversión de lenguaje de código fuente a lenguaje la máquina a través de signos binarios y que es ininteligible para el ser humano. Además, regula sobre las a compilaciones de datos que se refiere a todas la que el conjunto informaciones que están interrelacionadas entre sí y que se encuentran almacenadas mediante diferentes técnicas y mediante diferentes sistemas informáticos, técnicamente se llama la “Ley de la Propiedad Intelectual.

En Argentina se regula de manera específica lo referente al software, para ello cito el análisis y transcripción que hace Luis de Espanes y María del Pilar Hiruela, citando textualmente su postura consistente en:

> a partir de ello, cuadra señalar que nuestra legislación local ha provocado una injusta discriminación entre los programas de computación elaborados o publicados en el extranjero y los creados en el país, ya que la efectiva protección de aquéllos no se encuentra supeditada a ninguna condición suspensiva, mientras que los autores locales deben necesariamente registrar el software para que la tutela de la obra se haga efectiva… En aquella época los programas de computación se hallaban reproducidos sobre tarjetas perforadas o soportes magnéticos autónomos. En estas circunstancias, podía preverse la posibilidad de que una eventualidad accidental inutilizara los

ejemplares provistos por el autor o por el editor licenciado. Esto imponía al legislador la necesidad de introducir una excepción a la facultad autoral exclusiva de reproducción para permitir a los usuarios legítimos de programas de computación obtener una copia de salvaguarda (back up) útil para asegurar el funcionamiento del sistema en los supuestos en que el ejemplar recibido se tornaba inservible. En el contexto técnico contemporáneo esta excepción carece de significación, dado que los ejemplares originales, no tienen ahora otra función que el transporte de los archivos de los programas hasta el ordenador del usuario, donde los mismos se instalan. Es decir, en la actualidad, los softwares se copian en un medio de almacenamiento interno del ordenador desde donde luego se cargan en ocasión de su utilización…. Consideramos que el Derecho a Autor resulta ser el medio de protección jurídica que de un mejor modo tutela al software y a su autor. Por ello, entendemos adecuado y correcto el régimen jurídico instrumentado en nuestro país. Empero, no se puede desconocer la tendencia mundial que propugna al régimen de las patentes como marco jurídico adecuado para proteger al software, y en ciertos casos corresponde reconocer que la demanda resulta acertada. Esto exige en los operadores jurídicos un nuevo desafío, a fin de determinar con la mayor precisión posible las condiciones en las cuales a más de la protección por el Derecho de Autor corresponde o es conveniente otorgar a los programas de computación una patente de invención" (Espanes & Hiruela de Fernández, págs. 14-16)

Opino que la mejor forma para poder proteger un software es que se mantengan sobre la línea de la propiedad intelectual específicamente en los derechos de autor ya que crean los mecanismos y normativas jurídicas que puede hacerse valer frente otros ya que si bien es cierto las patentes de invención son más específicas estas pueden llegar a deslegitimar el derecho, toda vez que para crear una patente de invención se cumplen demasiado requisitos y se puede perder el objetivo fundamental que es la

protección del Software, aunado a ello se debe seguir propiciando el trámite de los diferentes procedimientos a través de servicios en línea y que incluya la firma electrónica y certificados digitales.

c. La Firma Electrónica, digital y digitalizada.

Cuando escuchamos el término de firma electrónica inmediatamente lo asociamos a cualquier dispositivo electrónico que está a nuestro alcance, además lo asociamos a una serie de números códigos o letras qué están plasmados en un documento. Sin embargo esos conceptos tienen una connotación diversa y para ello debemos de afirmar que el concepto de **firma electrónica** *stricto sensu*, se refiere a datos electrónicos o que tienen relación con algún tipo de documento que lleva implícita la creación de esta firma mediante el uso de un programa determinado, tal es el caso de los PDF que a final de un trabajo podemos crear una firma electrónica en base a las opciones que ofrece el software correspondiente, sin embargo esta carece de validez jurídica y legal; es entonces qué es necesario que sea utilizado un programa o aplicación que pueda certificar esta firma electrónica.

Y es ahí donde es necesario emplear diferentes protocolos para certificar un documento, la firma electrónica en forma aislada no tiene validez jurídica ante un juez competente o ante una empresa según sean las circunstancias y la forma correcta de darle validez es **usar un protocolo de firma electrónica avanzada** o también llamada **firma digital** la cual nos da las condiciones necesarias de autenticación e identificación para que sea válidos procedimiento o proceso o en su defecto presentado ante las autoridades correspondientes; por último la **firma digitalizada** se refiere a aquél estampado manuscrito que se hace sobre una hoja o documento y que después es escaneada utilizada para los fines correspondientes, es por eso entonces qué podemos concluir que de conformidad a la terminología técnica estos dos conceptos son diferentes. Tomando en consideración lo referido podemos hablar entonces que la firma digital actualmente es utilizada para darles seguridad a diferentes procedimientos internos dentro de las empresas como también darle seguridad y certeza jurídica a un proceso ante un juez competente.

Ahora bien de conformidad a las diferentes legislaciones de los diferentes Estados la terminología firma digital y firma electrónica se concibe como un sinónimo y es por eso qué en Guatemala se desarrolla lo concerniente a la firma electrónica, en el entendido que de conformidad a la técnica conceptual lo correcto sería referirnos a firma digital, cómo lo apuntaba, en Guatemala se maneja el término firma electrónica y esto lo podemos evidenciar en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Decreto número 47-2008, del Congreso de la República de Guatemala, la que analizaremos más adelante en otro contenido.

En otras legislaciones la firma electrónica es la equivalencia digital de la firma manuscrita y tiene la misma validez legal. Jaime Espinoza y Rómulo Verdezoto indican que:

la firma digital permite la transacción segura de documentos operaciones y aplicaciones computacionales garantizando los aspectos de: a) Integridad, ya que reconoce unívocamente a un emisor como autor del mensaje, el documento no puede ser alterado de forma alguna durante la transmisión. b) No repudio, ya que el emisor no puede negar en ningún caso que un documento no fue creado. c) Confidencialidad, solo las partes pueden leer el documento. Con la firma electrónica pueden realizarse diferentes tipos de transacciones a través del internet sin necesidad de desplazarse, ni hacer fila en los trámites públicos y además agilizan aumentando la transparencia, lo que se traduce en ahorro significativo de tiempo y dinero. Las aplicaciones de la firma digital son varias como, por ejemplo: compras públicas, gobierno electrónico, gestión documental, operaciones bancarias, pago dinero electrónico, balances electrónicos, trámites judiciales y notariales, comercio electrónico y factura electrónica" (Espinoza & Verdezoto, 2015)

La comisión de las Naciones Unidas para el derecho mercantil internacional que define por firma electrónica a los datos en forma electrónica consignados en un mensaje de datos o adjuntados o lógicamente asociados al mismo, que pueden ser

utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

Puedo definir a la firma electrónica como aquel documento que ha sido emitido por un emisor que mediante esa recopilación información y se puede tener la certeza que es legítimo y auténtico en virtud de la información plasmada en el documento y que se presume que es original y que no ha sido manipulado de ninguna forma y así es cómo llegará al receptor. En este proceso de transacción de información deben de existir varios elementos como lo es el emisor, receptor y el ente que certifica la información.

La tesista Andrea Lepe hace referencia al desarrollo de los sujetos que intervienen en el proceso interactivo de la firma electrónica y expone que:

"**Emisor o suscriptor…** la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa. Es decir que no es más que la persona o el usuario que crea la firma electrónica. Envía el mensaje de datos y lo firma electrónicamente con objeto de ser debidamente identificado.

Receptor o destinatario: "parte que confía", y lo define como la persona que pueda actuar sobre la base de un certificado o de una firma electrónica. La función del receptor o destinatario es recibir el mensaje de datos con la firma electrónica y necesita realizar el procedimiento de verificación para identificar al emisor y/o descifrar el contenido del mensaje.

Autoridad de certificación o proveedor de servicios de certificación: …la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas. Los proveedores de servicios de certificación (PSC), reciben en doctrina y otras legislaciones nombres distintos como gerenciadores de nodos o terceros de confianza (trusted third parties), esta última denominación por la actividad que realiza al ser la persona en quien confía tanto el emisor como el receptor, para que esta última identifique al titular de determinada clave. Sin embargo, su función principal es ser una entidad de confianza, responsable de emitir y revocar

los certificados digitales, utilizados en la firma electrónica, para lo cual se emplea la clave pública. Cuando hablamos de “terceros de confianza”, nos referimos directamente al significado de confianza que es “la actitud hacia alguien en quién se confía o se espera que haga cierta cosa necesaria para su tranquilidad”. La naturaleza de la firma digital mediante criptosistemas de clave pública en el que los usuarios manejan dos claves, una pública y una privada, la necesidad de obtener la clave pública auténtica de cualquier posible corresponsal, y la conveniencia de poder distribuir la clave pública propia a los demás agentes, lleva necesariamente.

Certificado digital: Los certificados digitales son documentos que atestiguan que cierta clave pública pertenece a un individuo o entidad. Evitan que cualquiera pueda generar una clave distinta y puede hacerse pasar por cualquier otra. Estos certificados los emiten las autoridades de certificación y son documentos en que se relaciona la identidad de su poseedor y la clave pública a la que se refiere, y los cuales han sido firmados digitalmente con la clave privada de dicha autoridad.

Un certificado digital contiene:

- ✓ El nombre identificador de la autoridad de certificación emisora
- ✓ Nombre del titular de ese certificado
- ✓ Un número de serie que identifica únicamente al certificado
- ✓ Las fechas de inicio y caducidad del certificado
- ✓ La clave pública y otros tipos de informaciones según sean las finalidades del certificado.

Lo más importante de un certificado es que la información va firmada de modo indisoluble con la clave privada emitida por la autoridad de certificación. Es decir que la función

fundamental de los certificados es permitir la comprobación de que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar su firma

Clases de certificados: De la misma forma el documento WP.71 de las Naciones Unidas (ONU) establece que las autoridades de certificación pueden emitir diferentes tipos de certificados. Los cuales básicamente son:

- ✓ Los certificados de identidad, que son los más utilizados actualmente dentro de los criptosistemas de clave pública y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.
- ✓ Los certificados de autorización o potestad, son aquellos que certifican otro tipo de atributos del usuario distintos a la identidad.
- ✓ Los certificados transaccionales son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero.
- ✓ Los certificados de tiempo o estampillado digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo. De la misma forma determinan el día y la hora en que el documento fue firmado. Aunque anteriormente mencionamos que las autoridades de certificación son equivalentes a los “terceros de confianza” y que simplemente son una variante en su denominación. El documento WP.71 de las Naciones Unidas establece que no es lo mismo, en el sentido que se refiere al término “tercera parte confiable” (TTP), e indican que son aquellas asociaciones que suministran un amplio margen de servicios, frecuentemente asociados con el acceso legal a claves criptográficas. El doctor Alfredo Alejandro Reyes Kraft en su tesis doctoral establece que no se descarta que las TTP actúen como autoridades de certificación (AC), debido a que las funciones de ambas se van considerando progresivamente diferentes. La expresión AC, autoridades de certificación se utiliza para las organizaciones que garantizan la asociación de una clave pública a una cierta o

> determinada entidad, lo que por motivos obvios debería excluir el conocimiento de dicha autoridad de la clave privada; que es justamente el ámbito de acción de una tercera parte confiable (TTP), que es asociar una clave pública y una privada a un ente particular y validar lo anterior. (Lepe, 2007)

Además, podemos concluir que la firma electrónica realiza funciones como la garantía de que los intervinientes son legítimos tanto emisor como receptor. Dentro de la doctrina se contemplan diferentes firmas electrónicas como lo es la simple, avanzada y la firma electrónica reconocida.

Para ello conceptualizaremos cada una de ellas. **a)** Firma electrónica simple: identifica un documento electrónico que tiene una serie de datos y se usa sólo unas cuantas claves para cifrar la información y esta consiste en un trazo físico de la firma y que se puede digitalizar mediante un escáner, sirve para automatizar diferentes procesos y tiene diferentes usos específicamente los entes gubernamentales o en las empresas, como por ejemplo para firmar la hora de entrada o salida de la hora el valor de esta firma es muy reducida. **b)** Firma electrónica avanzada qué sirve para identificar al emisor y los datos enviados y se verifica si la información ha sido alterada, por ejemplo, se utilizan los algoritmos Hash o más reconocidos en MD5 y SHA 256 y SHA512. **c**) Firma electrónica reconocida, se utiliza mediante un certificado reconocido y generada mediante un dispositivo electrónico seguro que pueda crear la firma en forma auténtica y la característica fundamental es que acá existe un certificado digital otorgado y respaldado por una empresa encargada de este tipo de funciones, pero la facultad de autenticidad y legitimidad de su certificado debe ser autorizado por la ley, consecuentemente ésta firma electrónica es la que tendría que tener los efectos jurídicos ante juez competente para que tenga valor probatorio tanto en los procedimientos administrativos, así como en el Derecho Procesal.

Para concluir refiero que la firma electrónica es una forma moderna y novedosa a la firma tradicional o manuscrita a la que estamos acostumbrados y cumple en el mismo objetivo que es el de dar certeza y legitimidad a lo que debe de comprobar un documento es decir se reconoce la autoría de la persona que emite el documento, la

autenticidad del documento y más interesante es que puede utilizarse como plena prueba ante una persona o ente correspondiente o ante un juez competente.

Se estima que en Guatemala debe utilizarse una firma electrónica avanzada en donde se certifique la evidencia digital mediante los algoritmos permitidos y validos según los protocolos internacionales y si bien es cierto que en Guatemala se utiliza la firma electrónica para utilizarlas en diferentes dependencias tales como Registro Mercantil, Superintendencia de Administración Tributaria, Instituto Guatemalteco de Seguridad Social y Ministerio de Trabajo se advierte que es suministrada y respaldada por empresas privadas, esto debe transformarse y trascender al plano judicial tal y como lo ha implementado ya la Corte de Constitucionalidad, además se debe tomar en consideración que la firma electrónica o digital también es necesaria que empiece a utilizase en los procesos, es decir propicias la llamada "justicia digital" además debemos acotar que en el plano pericial los expertos en pericias forenses digitales son las personas competentes para certificar electrónicamente y digitalmente una evidencia que posteriormente será utilizada en el proceso.

2.3. La política de seguridad de la información.

Como lo hemos referido en los otros temas expuestos, en los diferentes estados que han avanzado en la regulación jurídica de la tecnología de la información en sus diferentes manifestaciones han tenido grandes desafíos hasta llegar a un mejoramiento en la protección de la información, las personas y todo lo relacionado con las tecnologías de la información. Es de hacer notar que cuando se habla de información ésta existe tanto en el ámbito privado como en el ámbito público, entonces entiéndase ámbito privado referente a las empresas y ámbito público a los entes o instituciones del estado.

Hoy en día la Big Data o el manejo voluminoso de datos día a día crecen más y es necesario que existan los protocolos necesarios para el resguardo y protección de la información. Podemos entonces inferir que cuando se refiere a protección de la información podemos estudiarlo desde diferentes puntos de vista. Por ejemplo desde punto de vista jurídico se refiere a la normativa jurídica vigente y positiva que existe

entre un estado para dicha protección, pero también podemos hablar desde el punto de vista técnico e informático, que es por ejemplo referirnos al tema del cifrado, la encriptación y los protocolos de seguridad implementados y en funcionamiento en una base de datos, montados y en funcionamiento en un dispositivo electrónico o simplemente el protocolo qué se debe de agotar para el correcto manejo, acceso y protección de la información.

Es interesante saber que el tema de la encriptación es parte fundamental para que exista una legítima y auténtica confidencialidad e integridad de la información. Pero para el tema objeto de estudio debemos abordar todos aquellos aspectos jurídicos que se deben aplicar o que deben de coexistir en forma integral para la protección de la información y es aquí donde actúa tanto el andamiaje jurídico, las políticas de estado y los diferentes sujetos que intervienen en la administración de justicia y desempeñan diferentes roles para la aplicación del derecho.

Hoy en día en la práctica existen diferentes procedimientos o protocolos que los diferentes entes públicos o privados en diferentes países aplican para el resguardo y protección de la información creando para ello una serie de procedimientos que sirven para atender los diferentes incidentes que se puedan presentar, esto se sustenta y fortalece cuando existe un derecho vigente y positivo qué de una certeza jurídica a dichos procedimientos y no sea una forma empírica o simplemente reglamentaria, sino más bien, exista una bilateralidad jurídica que coadyuven a esa tutela judicial efectiva en el resguardo y protección de la información.

En relación a las normas internacionales en materia de seguridad de la información, es necesario citar lo que expone en su texto Arián Hernando Velasco Melo en su obra “El Derecho Informático y la Gestión de la Seguridad de la Información”, señalando que:

> el origen reciente de la seguridad la información, entendida como un proceso que se debe gestionar, nace en el Reino Unido donde el Departamento de Industria y Comercio y las empresas del sector privado trabajaron de manera conjunta en esta problemática, lo cual dio origen a la norma BS7799 en el primer lustro de la década pasada; norma

> que no pretendía ser más que un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. Al final de la década pasada esta norma fue actualizada y complementada, lo cual dio como resultado una norma que establecía las recomendaciones para que una empresa evaluará y certificará su sistema de gestión de seguridad de la información. Esta nueva versión de la norma se convirtió en la norma ISO 17 999 de diciembre de 2000, la cual estaba alineada con las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico) en materia de privacidad, seguridad de la información y Criptología, hecho de gran trascendencia, pues le otorgaba un carácter global a la norma. En el 2002, la norma adquiere la denominación de ISO 27001, luego de una nueva actualización. (Velasco Melo, 2008, pág. 338).

Más adelante entraremos a estudiar la Norma ISO 27001 la cual contiene aspectos interesantes en materia de políticas para la protección de la información.

Tratamiento legal de los incidentes informáticos.

El maestro Velasco Melo en su obra el derecho informático y la gestión de seguridad de la información cita que el concepto de seguridad informática es reciente y que en los últimos quince años ha existido el fenómeno del ataque a las redes de comunicaciones y esto se da gracias a la aparición de los ataques de piratas cibernéticos que han actuado en el espectro electrónico y eléctrico después de la aparición de las líneas de comunicaciones telegráficas. Sigue manifestando el autor Velasco Melo que actualmente una de las mayores preocupaciones de las organizaciones es crear aqueos protocolos informáticos que puedan responder ante aquellos atentados que vulneran o destruir información valiosa de las diferentes organizaciones, indicando además qué quedará la historia la reciente actuación de un cracker reconocido como Kevin Mitnick quién fue acusado por diversos crímenes tales como la creación de números telefónicos notificables robo de 20,000 de tarjetas de crédito fue quien promovió la falsificación de direcciones ip desconocida cómo IP

spoofing[7], además de robo de software de terminales telefónicas control de aire centro de comunicación en Estados Unidos acceso ilegal a múltiples sistemas de gobierno de Estados Unidos entre otros incidentes de seguridad, sin embargo hoy en día esta persona es un experto consultor en temas de Ciberseguridad. (Velasco Melo, 2008)

Y es que al referirnos a temas de cómo tratar los incidentes de seguridad informática también nos conduce al análisis de la norma ISO 27001 ya que está también regula lo referente al aseguramiento de procesos de información y las debilidades en la seguridad, es decir, su objeto es crear un protocolo correctivo para evitar que existan vulneración a estos sistemas. Es por ello que el incidente de seguridad podemos nosotros interpretarlo como una acción de una persona que va encaminada a afectar un sistema de información con objeto de carácter ilícito y eso pueden ser aprovechados por diferentes delincuentes cibernéticos tales como Ciberterrorismo, piratas informáticos entre otros. También debemos considerar que para el tratamiento de un incidente de seguridad es necesario tener un protocolo de recolección de evidencia es decir el procedimiento para obtener esa muestra de la vulneración a los sistemas de seguridad y es aquí donde entra en función la informática forense a través de los diferentes procedimientos y herramientas que se deben de utilizar para responder a un ataque Cibernético.

El maestro Velasco Melo también refiere que:

> frente a la presencia de un incidente informático corresponde al equipo de seguridad reaccionar frente al incidente siguiendo este esquema de 4 pasos: identificar los equipos que pueden contener evidencia del incidente acaecido; preservar la evidencia de los daños accidentales o intencionales, lo cual se logra efectuando una copia o imagen espejada exacta del medio analizado; examinar la imagen de la copia original, buscando evidencia o información sobre los hechos que suponen la existencia de un incidente de

[7] La **suplantación de identidad** en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación. https://es.wikipedia.org/wiki/Suplantaci%C3%B3n

seguridad; y por último, escribir un reporte, finalizada la investigación, en el cual debe hacerse referencia de los hallazgos a la persona indicada para tomar una decisión, bien sea a un juez o al presidente de la compañía. El problema de la recolección de incidentes informáticos radica en aplicar protocolos que permitan un tratamiento probatorio conforme a la ley, de manera que la prueba obtenida tenga la legalidad requerida para ser aceptada en una causa judicial, sea ésta de naturaleza penal, civil, administrativa o disciplinaria. En términos gráficos, el tratamiento que se debe realizar respecto de la comisión de un incidente informático demanda aplicar técnicas equivalentes a las practicadas para buscar la evidencia de un delito cometido en el mundo real. No obstante, existen diferencias sustanciales al recabar la evidencia de incidentes informáticos, pues la prueba de tales acciones muchas de las veces pueden desaparecer o ser eliminadas por su volatilidad; característica que exige que la intervención del equipo de seguridad se realice tan pronto como se tenga conocimiento o sospecha de la ocurrencia de un ataque a los activos de información de una organización. (Velasco Melo, 2008)

Además, puntualiza en lo siguiente:

corresponde precisar que no sólo se trata de encontrar la evidencia del delito, ataque o intrusión, de carácter informático, sino que además se precisa la limpieza en la práctica de la misma, pues en caso de alterarla o desaparecer ésta, será imposible demostrar la comisión del incidente, y por esta vía, aplicar las sanciones o penas a que haya lugar, así como el resarcimiento de los perjuicios que se causen. Ahora bien, un incidente informático puede o no tener carácter judicial, y una organización seguramente definirá por razones estratégicas hacer pública o no su condición de víctima de un ataque a sus activos de información. Así mismo, la definición de si un incidente informático tiene carácter judicial es determinada por la tipicidad legal de la conducta del infractor; para el

efecto habrá de contrastarse la misma contra los tipos penales consagrados en la legislación de cada país. Los sistemas acusatorios permiten que los particulares puedan participar en la recolección de la evidencia de la comisión de determinados hechos potencialmente punibles, previo cumplimiento de los requisitos que exige la ley procesal. Esta facultad es fundamental en materia de oportunidad y pericia a la hora de recabar la evidencia de un incidente de naturaleza informática. La recolección de la evidencia de un incidente informático, por las particularidades y características del mismo, implica la participación de un equipo interdisciplinario de profesionales capacitados en identificar, recolectar, documentar y proteger las evidencias del incidente, apoyándose en técnicas de criminalísticas forenses, que permitan iniciar las acciones penales y civiles derivadas de la ocurrencia de estos incidentes. Al respecto es importante conocer las medidas que en el marco del sistema acusatorio de cada país existan para que los mismos particulares, en este caso las organizaciones afectadas, puedan recabar las pruebas de los hechos punibles cometidos, teniendo en cuenta la cadena de custodia, entre otras herramientas, que asegure las características originales de los elementos físicos de la prueba del incidente, desde la protección de la escena, recolección, embalaje, transporte, análisis, almacenamiento, preservación, recuperación y disponibilidad final de éstos, identificando al responsable en cada una de sus etapas y los elementos que correspondan al caso investigado". (Velasco Melo, 2008)

En conclusión para ese tema podemos asegurar existe escasa información en Guatemala referente a cómo tratar los diferentes incidentes en materia de seguridad ya que no existe un protocolo uniforme que pueda dar una respuesta certera y efectiva para solucionar este tipo de asuntos, es decir se actúa en forma empírica ocasionando que el trabajo tenga muchas falencias atentando contra la seguridad jurídica y en el análisis resalta la importancia que de la actuación de un equipo multidisciplinario con

competencia especializada y el valor de la cadena de custodia, siendo este último un elemento vital en la criminalística digital.

2.4. Los contratos informáticos.

Dentro del objeto de los contratos informáticos debemos interpretar que esto irá encaminado a la contratación de bienes o servicios, como por ejemplo el Hardware qué se refiere a todos aquellos dispositivos electrónicos como también al Software que se refiere a todos los programas de cómputo. Más interesante resulta que en esta nueva era ya se efectúan contrataciones civiles y mercantiles a otro nivel es decir en el campo informático y telemático en donde se adquieren juegos en línea, licencias para uso de aplicaciones en dispositivos móviles, licencias para uso de programas de computación, sin embargo aunque ésta contratación sea similar a la civil o mercantil esto no significa que se omitan todas las formalidades toda vez que tiene ciertas particularidades al contratar diferentes bienes o servicios informáticos. Es importante que el lector pueda conocer que en la actualidad existen contratos un tanto complejos por el contenido o el objeto sobre el que recae, en virtud que dentro de los contratos de software podemos citar el arrendamiento o compra de dominios web, creación desarrollo y mantenimiento de página web, contratos de Hosting o alojamiento de páginas web, compraventa y transacciones financieras en línea y entre muchas más.

Existen diferentes tipos de contratos informáticos y tal y como se detalla en el sitio web llamado “tuabogadodefensor” nos señala una pequeña clasificación qué es muy interesante siendo el siguiente:

a. Contrato informático de hosting. Este tipo de contratos, de carácter mercantil, es aquel que se celebra entre la empresa de alojamiento de la página Web y al empresa o particular propietaria de dicha página Web. Con carácter general, no suele realizarse contrato escrito, aunque también con carácter general del contratante, en muchos casos, online, se tiene que adherir a las condiciones generales que figuran en la propia Web de alojamiento. Los derechos y obligaciones, en este tipo de contratos se encuentra difuminada y es compleja

su interpretación, sobre todo teniendo en cuenta que, en muchos casos, el contrato se realiza online, y el lugar del cumplimiento de la obligación es un país fuera de España o incluso fuera de Europa, con lo que los incumplimientos son difíciles, que prospere una demanda de carácter internacional o por lo menos muy costosa.

b. Contrato informático de outsourcing. Este contrato informático consiste en la cesión de la gestión de los sistemas de información de una entidad a un tercero que, especializado en esta área del derecho informático, se integra en la toma de decisiones y desarrollo de las aplicaciones y actividades propias de la referida gestión. Su finalidad es la optimizar los resultados de la misma, así como permitir a la entidad el acceso a nuevas tecnologías y la utilización de recursos especializados de los que no dispone.

c. Contratos informáticos sobre el software. Se puede definir el software como esos programas que cuando se conjugan con el sistema, son capaces de procesar información al objeto de ejecutar o alcanzar una determinada función o resultado. Los programas constituyen la parte blanda (software) o lógica del sistema, y comprende los procedimientos, reglas y cualquier documentación asociada a la operación de un sistema de proceso de datos.

d. Licencias de programas estándar. Los programas estándar son aquellos que se elaboran previamente para su posterior comercialización en masa. Estos contratos informáticos, se configuran contractualmente como bienes de naturaleza híbrida entre producto y obra. Por un lado, nos encontramos ante un producto estándar de disponibilidad inmediata y previamente testado, pero, por otro lado, la prestación de unos servicios impide considerar este tipo de programas como una simple mercancía o producto.

e. Contratos informáticos de desarrollo de programas. Un programa de ordenador puede ser una obra creada por encargo, donde el autor se compromete a entregar un software específico, para una determinada aplicación. Podemos decir que el programa nace de la colaboración entre el proveedor y el cliente ya que es una obra en la que participan tanto el usuario (en la fase de definición de las especificaciones externas) como empresas de servicios o trabajadores independientes.

f. Contrato de mantenimiento informático. Se trata de uno de los contratos informáticos que más se desarrolla en la práctica. La paralización de una empresa por un defectuoso funcionamiento de su sistema informático, produciría enormes pérdidas que, llegado el caso, podrían ser irreparables. De ahí que el empresario ha de contar con un servicio que prevenga este evento o lo corrija en caso que se produzca. La complejidad de todo un sistema exigirá que este mantenimiento se extienda tanto al hardware como al software; por lo que este contrato presenta múltiples facetas y posibilidades. Lo que se pacta es asegurar la perfecta utilización del bien adquirido, realizar las adaptaciones que sean precisas según las circunstancias e introducir cuantas mejores se estimen por oportunas.

g. Contrato de escrow. Surge como respuesta a los posibles conflictos que pudieran surgir entre el usuario de un programa y sus creadores o empresas de software, en relación con la posesión del código fuente (código fuente es el núcleo formal del programa y constituye la primera expresión independiente del proceso de creación que alcanza una protección directa del derecho de autor). La importancia de este concepto es enorme, de tal manera que quien posea el denominado código fuente, tiene la posibilidad de alterar de cualquier modo, interconectar y multiplicar el programa. Ésta es la razón por la que las empresas

de software siempre han sido reticentes a la entrega del código fuente al licenciatario de un programa de ordenador. El contrato de escrow se nos presenta como elemento imprescindible para asegurar la viabilidad de un sistema informático con su necesario mantenimiento, actualización y estabilidad, que deja de estar pendiente así de la actitud de la empresa de software. Podemos considerar a este contrato como complejo en cuanto a su naturaleza puesto que participa en cierto modo de la naturaleza jurídica del depósito y de la del de mantenimiento, con una intención de garantía de protección y aseguramiento de derechos previamente adquiridos. Este contrato de escrow se celebra entre la empresa de software, titular de los derechos de propiedad intelectual sobre el programa, y el usuario del mismo, pero a su vez se exige la presencia, por la propia esencia del contrato, de un tercero depositario por lo que este tercero, o bien interviene en el propio contrato o bien se vincula a él a través de un contrato conexo.

h. Contrato de auditoria informática. Consiste en la revisión de la propia informática y de su entorno. La auditoría informática investiga las instalaciones y los sistemas de tratamiento de la información del empresario o profesional analizando las posibilidades de mejora, detectando fallos en los sistemas, corrigiendo duplicidades, etc. La auditoría revisa la seguridad, calidad y eficiencia del sistema de información de la empresa. El contrato deberá definir las modalidades según las cuales la empresa consultora realiza, en la sede del cliente, la auditoría general de seguridad de los equipos informáticos en diferentes campos. Dicha auditoría general de seguridad informática exige una colaboración activa entre el auditor y el auditado; el intercambio constante de informaciones tiene por objeto evitar la generación de incidentes perjudiciales.

i. Contrato de consultoría y estudio informático. La consultoría informática, es un contrato de servicio informático, consistente en dar asesoramiento o consejo sobre lo que se ha de hacer o cómo llevar adecuadamente una determinada actividad para obtener los fines deseados. El objeto de este acuerdo es el conjunto de actividades necesarias para el estudio y evaluación de los sistemas de información que resulten más adecuados para una empresa determinada. Los contratos de consultoría de software informático se corresponden normalmente con contratos de servicios, siendo su finalidad la de realizar un estudio o prestar un consejo. (Tuabogadodefensor, s.f.)

Anteriormente ya se ha expuesto, la clasificación general de los contratos en materia informática o telemática en dónde podemos apreciar que hay muchos contratos que en Guatemala podrían encuadrarse como contratos mercantiles en virtud que son atípicos, sin embargo, como se ha aclarado ya, los contratos informáticos deben de ser vestirse con ciertas formalidades propias para que salga la vida jurídica con plena certeza sin ningún tipo de vulneración a los derechos de la otra parte. Como por ejemplo contrato de outsourcing es uno de los que se aplica en Guatemala por sus diferentes modalidades, recordando que este tipo de contratos es un tercero el que actúa obligándose a cumplir determinada acción o función. Los contratos informáticos sobre el software o programas de computación qué están regulados en la Ley de Derechos de Autor y Derechos Conexos Decreto 33-98 del Congreso de la República de Guatemala, en su parte conducente nos da la pauta de la creación de nuevas modalidades de contratación y tanto en el fondo como el aspecto formal.

Podemos indicar entonces que varios de los contratos detallados podrían ser concebidos como contratos mercantiles atípicos, sin embargo se advierte, nuevamente que los contratos informáticos deben de cumplir ciertos requisitos formalidades y particularidades para que pueda tener certeza jurídica, especialmente en nuestro derecho guatemalteco interno, tales como la privacidad de la información,

resguardo de contraseñas de acceso a redes sociales a través de medios de almacenamiento poco volátiles, entre otros.

- La contratación de bienes informáticos y servicios telemáticos.

En el derecho privado encontramos las diferentes manifestaciones de voluntad en la cual se adquieren derechos y se contraen obligaciones es decir vemos como la contratación se manifiesta mediante ese acto de voluntad en donde en forma bilateral dos o más personas pactan en adquirir un derecho y otra a cumplir una obligación, en Guatemala citamos como ejemplo la regulación de la materia civil y mercantil y eso lo podemos encontrar tanto en el Código Civil, Código de Comercio y en su parte procesal en el Código Procesal Civil y Mercantil. Sin embargo en los diferentes países existen legislaciones que adoptan las diferentes formas de contratación de bienes efectuados por las personas sin embargo en el tema de las tecnologías de la información, bienes informáticos o servicios telemáticos este tipo de contratación varía y no puede aplicarse por regla general los mismos criterios de contratación tradicional como por ejemplo en el área civil; esto es simple debido a que la mayoría de bienes que se contratan en el área civil o mercantil se refiere específicamente a bienes tangibles pero en el área informática o telemática en muchas ocasiones se manejan o regulan bienes intangibles, En pocas palabras los contratos civiles y mercantiles no podrían aplicarse como regla general a los contratos informáticos o telemáticos.

En su obra el derecho informático y la gestión de la seguridad de la información el maestro Velasco Melo explica qué:

> la regulación de estos contratos debe ser suplida por la voluntad de las partes, los principios generales de contratación, el derecho internacional y demás fuentes, de manera que cada uno de los aspectos de la relación jurídica a ejecutar entre las partes sea definido y consignado en el cuerpo del contrato y sus anexos respectivos, advirtiendo la importancia de regular de manera independiente las diferentes prestaciones jurídicas que puedan estar vinculadas al contrato principal. En la práctica se encuentra que los equipos de informática trabajan al margen de los equipos jurídicos

> dentro de las organizaciones en lo que tiene que ver con los procesos de contratación informática, situación que genera una ruptura en la tarea de gestionar de manera eficaz la seguridad de los activos de la información. No son extraños los casos en los cuales aspectos sencillos como la definición de la propiedad intelectual sobre los intangibles contratados no están formalizados, o existen reclamaciones sobre la propiedad de los mismos por quienes los han desarrollado. Ante esta realidad se aconseja que exista un proceso de comunicación clara entre las áreas involucradas en la contratación de intangibles digitales, en aras de que las inversiones en tecnología para la organización sean seguras. Los operadores jurídicos de la organización, responsables de la contratación de esta clase de bienes y servicios, han de tener en cuenta que la adquisición, desarrollo y mantenimiento de obras digitalizadas requieren de regulaciones apropiadas a la naturaleza incorpórea del objeto contratado, que exigen armonizar lo jurídico con lo técnico. (Velasco Melo, 2008, págs. 349-350)

Estimo que es importante que el profesional del derecho que intervenga en la autorización de este tipo de negociaciones debe conocer en forma básica el contenido de lo que se va a pactar para revestir de seguridad y certeza jurídica al instrumento público y si sobreviniere el incumplimiento de una obligación sea factible la ejecución de las cláusulas del documento público o el documento privado legalizado por el Notario toda vez que el profesional de derecho debe tener los conocimientos básicos para atender la el asunto que se presente. Como vemos en este apartado es muy importante la preparación integral del Notario para cumplir lo que preceptúa el artículo 2 de la Constitución Política de la República de Guatemala, relativo a la certeza jurídica en la formalización y validación de los contratos con contenido telemático o informático.

CAPITULO III

Delitos Informáticos.

Un tema que actualmente tiene mucho auge y que en diferentes países es tratado en forma recurrente es lo relativo a los delitos informáticos, tema de por si complejo y que es de agenda internacional y de suma importancia y es por ello que diferentes países del mundo como España, Argentina, Colombia, Brasil, Chile y Paraguay han encaminado sus esfuerzos para mejorar su legislación en relación a este tema. Este flagelo día a día se esparce en las redes de comunicación e información.

Muchas veces al escuchar el término delitos informáticos simplemente nos limitamos a pensar que se refiere al uso de computadoras o dispositivos electrónicos como un celular, una tableta electrónica o tal vez el uso de una memoria USB o pendrive, erróneamente se concibe esto simplemente en esa delimitación, sin embargo detrás de la configuración y significación de este tipo de delitos existe el funcionamiento y operatividad de la delincuencia organizada, narcotráfico, tráfico de armas, tráfico de órganos y una infinidad delitos que muchas veces. Es menester indicar que en nuestro contexto jurídico se deben implementar mecanismos que coadyuven al funcionamiento correcto de la justicia penal tomando en consideración ejes como la investigación criminal el manejo de la evidencia electrónica y digital y cualquier aspecto relacionado con la informática forense y útil en un proceso penal. Además, no debemos obviar el concepto de “volatilidad de la información” tema que desarrollaremos más adelante deben estar en consonancia con el derecho sustantivo y adjetivo para que se respete y cumpla el debido proceso y las garantías fundamentales dentro del proceso penal guatemalteco.

3.1. Definición de Delito Informático.

Previamente a abordar este tema es menester definir lo que es delito y decimos entonces indicar qué es el encuadramiento de aquella conducta u omisión típica, antijurídica, reprochable y posiblemente susceptible de la imposición de una pena y que esto de estar ajustado y conforme al principio de legalidad para que efectivamente exista un ilícito penal. Los principios de celeridad, concentración, debido proceso,

legalidad, tutela judicial efectiva, contradictorio, no declaración contra sí mismo o parientes, la analogía *in bonam partem* son solo algunos de los principios sobre los cuales debe enfatizar el jurista para adecuar y entender la dinámica de los Delitos Informáticos.

El doctor Claudio Líbano Manzur describe el delito informático como:

> todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas realizados en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados de la sana técnica informática, lo cual generalmente, producida de manera colateral lesiones a distintos valores jurídicos reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial actúe con o sin ánimo de lucro. (Libano Manzur)

El autor García-Pablos Molina, citando al profesor Davara, define al delito informático como "la realización de una acción, que reuniendo las características que delimitan el concepto de delito utilizando un elemento informático vulnerando los derechos del titular de un elemento informático ya sea Hardware o software, hackeo o sustracción de datos de las computadoras o incluso la forma ilegal en la que muchas veces se puede efectuar la interceptación de comunicaciones entre los usuarios" (Molina). En Guatemala no existe actualmente una ley que regule específicamente esta amplia gama de tipos penales referentes a la informática, mismos que más adelante podremos analizar detenidamente.

Según el texto denominado "Apuntes de Derecho Informático" de la Licenciada Edna Martínez en el apartado de delitos informáticos lo define como:

> la delincuencia informática se refiere a la forma delictiva del fraude informático que no sólo da origen a la acción civil sino además a sanciones penales y qué se caracteriza por ser una delincuencia de especialistas cuyo descubrimiento y seguimiento se dificulta por la capacidad de estos para ocultar o borrar las huellas del delito lo cual exige la

> tecnificación y capacitación de los investigadores factor es de que resulta mucho más importante que las previsiones legislativas. (Martinez, 2012, págs. 133-135). Sigue manifestando la autora que estas conductas están específicamente ligadas a la tecnología, piratería de software el repunte de la delincuencia tradicional con el uso de la tecnología y que muchas veces es usada para la comisión de delitos comunes (hurtos, estafas, interceptación de Comunicaciones, extorsión, aprovechamiento de error ajeno, pánico económico, entre otros) (Martinez, 2012)

En virtud de lo analizado puedo definir entonces al delito informático como aquel cúmulo de conductas que son típicas, antijurídicas, reprochables que afectan la seguridad de los diferentes sistemas telemáticos y que tiene como consecuencia el daño a hardware, software, datos y sistemas de información.

3.2. Características de los delitos informáticos.

Es interesante que dentro de esas características comunes que poseen, en este caso, las personas que cometen este tipo de acciones ilícitas es un tanto atípico en virtud qué en muchas ocasiones el sujeto activo son personas que están en constante contacto con las diferentes tecnologías o sistemas informáticos. Y es que ese tipo de personas tienen diferentes destrezas en virtud de la labor que desempeñan. Tal es el caso de una persona que navegando en la internet sin ningún tipo de intención ingresa a registros informáticos o a un sistema de una empresa o de una entidad estatal y simplemente actúa como observador y que de conformidad a la regulación normativa en el ámbito penal en algunos países esto se convierte ya en una consumación de un delito informático sin embargo es un tema a discutir en virtud que entran en función los elementos positivos y negativos del delito. Sin embargo, situación diferente es cuando una persona ingresa a un sistema informático y en forma dolosa modifica o altera los registros para obtener un beneficio como por ejemplo se encripta la información y solicita dinero al usuario atacado a cambio de darle la contraseña para recuperar su información.

Tal y como refiere el autor Julio Téllez en su texto Derecho Informático, explica que:

> el nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos no revela delincuencia informática, mientras otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudiera tener un empleado del sector de procesamiento de datos. A pesar de lo anterior, teniendo en cuenta las características mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Efectivamente, el conocido criminólogo señala un sinnúmero de conductas que considera "delitos de cuello blanco", aun cuando muchas de ellas no están tipificadas en los ordenamientos jurídicos como delitos, entre las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas y la corrupción de altos funcionarios, entre otras" -. Asimismo, este criminólogo dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no están de acuerdo con el interés protegido (como sucede en los delitos convencionales), sino según el sujeto activo que los comete. Algunas de las características comunes de ambos delitos son las siguientes: el sujeto activo del delito es una persona de cierto estatus socioeconómico y su comisión no puede explicarse por pobreza, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional (Téllez, 2008, pág. 189)

Más llamativo resulta la enunciación que hace Julio Téllez, referente a las características de los delitos informáticos, quien resalta lo siguiente:

1. Son conductas criminales de cuello blanco, White collar crimes[8], en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas. 2. Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando. 3. Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico. 4.· Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan. 5. Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física. 6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional. 7. Son muy sofisticados y relativamente frecuentes en el ámbito mi- litar. 8. Presentan grandes dificultades para su comprobación, por su carácter técnico. 9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales. 10. Ofrecen a los menores de edad facilidades para su comisión. 11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional. (Téllez, 2008)

3.3. Consideraciones doctrinarias de los delitos informáticos.

En Guatemala el concepto delito informático tiene poco auge en cuanto al estudio doctrinario, práctico y forense sin embargo es necesario qué realicemos una interpretación objetiva y para este aspecto el Derecho Penal nos explicará cómo debemos entender todo lo referente a los delitos informáticos. El concepto de delito informático tiene una definición diversa en los diferentes instrumentos normativos de carácter sustantivo y en otras legislaciones del mundo; en el caso de Guatemala no existe un catálogo definido sobre delitos informáticos que contemple los escenarios que se plasman en el Convenio de Budapest, no obstante, actualmente existe una

[8] Se refiere a crímenes no violentos cometidos por profesionales de negocios y gobierno con motivos financieros. https://es.wikipedia.org/wiki/Delito_de_guante_blanco

iniciativa de ley bajo el número 5601 “Ley de Prevención y Protección contra la Ciberdelincuencia” que está en fase de análisis en el Congreso de la República de Guatemala. Es interesante saber que una de las características principales de los delitos informáticos es que no se emplea violencia, sino que muchas veces son cometidos sin que la víctima se dé cuenta y el modus operandi de estos delitos en su consumación es que causan un grave perjuicio a la economía de los países del mundo. Estos delitos se pueden cometer desde cualquier estación informática, una computadora, teléfono, entre otros.

Existe una gran variedad de casos en los que las víctimas han sufrido las consecuencias de un delito informático, siendo una realidad que en Guatemala no se tiene la cultura de la denuncia y muchas veces tanto los órganos jurisdiccionales como el Ministerio Público abordan el conocimiento de la causa como un delito común, obviando que estos tipos penales son complejos y la estrategia para abordarlos requiere un conocimiento y preparación especializada; y es que en la práctica forense se ve a diario y comúnmente que los diferentes sujetos procesales utilizan evidencia digital y electrónica para acreditar y sustentar su hipótesis o tesis ya sea de defensa o acusatorio y el problema surge cuando se trata o intenta dar un valor probatorio o un acreditamiento suficiente e intelectual a este tipo de vivencias.

En Guatemala no existen protocolos estandarizados que ayuden a los diferentes sujetos procesales a interpretar y utilizar adecuadamente estas evidencias o medios probatorios, es decir las consecuencias en la consumación de un delito informático en Guatemala se tiene casi por perdido porque muchas veces el delito que se investiga se pretende acreditar con medios tecnológicos de una manera errónea, si se aplicarán correctamente los protocolos en materia de evidencia electrónica y digital se podría tener como válido un juicio de razón en una sentencia condenatoria o absolutoria, sin embargo en la actualidad se actúa en forma arbitraria y sin ningún tipo de sustento técnico y legal.

En interesante conocer las características del sujeto activo y pasivo en los delitos informáticos, para el efecto el sujeto activo casi siempre deberá tener ciertos conocimientos básicos en cuanto al manejo de la tecnología para poder consumar un

ilícito penal. Además, el sujeto activo en muchos casos actúa en la esfera internacional es decir que una persona puede estar cometiendo un hecho ilícito en un país utilizando un sistema tecnológico de un segundo país y consumándolo en un tercero, no obstante, esto, no debemos descartar la esfera de acción de un particular dentro de su país, que muchas veces por la fragilidad o vacíos legales tiene la apertura para perfeccionar sus actos ilícitos sin ningún tipo de consecuencia jurídica sancionable.

La pregunta es entonces, qué normativa legal se aplicará a una persona que esté encuadrando su conducta en un delito informático y más complejo resulta la forma de efectuar el rastreo para poder efectuar una persecución penal de carácter internacional si es que puede aplicar. Hasta el momento sólo nos hemos referido a la forma en que un particular puede encuadrar su conducta en un ilícito penal, sin embargo, en la actualidad vemos como el crimen organizado hace uso también de la tecnología para poder cometer diferentes hechos que a la luz de las diferentes legislaciones de los diferentes estados del mundo se consideran como el modus operandi del crimen organizado utilizando la tecnología como objeto para la comisión de un ilícito.

Tal y como lo menciona el Doctor Santiago Acurio en su obra Delitos Informáticos quien refiere un amplio inventario de las actividades principales de las organizaciones criminales citando como ejemplo que:

> la provisión de bienes y servicios ilegales, ya sea la producción y el tráfico de drogas, armas, niños, órganos, inmigrantes ilegales, materiales nucleares, el juego, la usura, la falsificación, el asesinato a sueldo o la prostitución; la comercialización de bienes lícitos obtenidos por medio del hurto, el robo o el fraude, en especial vehículos de lujo, animales u obras de arte, el robo de identidad, clonación de tarjetas de crédito; la ayuda a las empresas legítimas en materias ilegales, como la vulneración de las normativas medioambientales o laborales; o la utilización de redes legales para actividades ilícitas, como la gestión de empresas de transporte para el tráfico de drogas o las inversiones

inmobiliarias para el blanqueo de dinero" (Acurio del Pino, Delitos Informáticos: Generalidades, pág. 3).

Además, podemos afirmar que actualmente en el mundo Cibernético el sujeto activo predominante en la comisión de diferentes ilícitos penales son los llamados Crackers que son piratas informáticos y especialistas en tecnologías de la información muy avanzado que vulneran una infinidad de sistemas, bases de datos, entre otros, cuyo fin es obtener una ganancia ilícita o también la llamada extorsión cibernética. Y es que un ejemplo claro de esto es cuando un cracker logra encriptar determinada información en cualquier terminal o computadora y pide dinero a cambio para que se pueda dar la clave o descifrar la información encriptada, un caso real de ello fue un caso no registrado pero que aparece en los sistemas de fuentes de información abierta y se refiere a una encriptación de información del Ministerio Público con sede en la cabecera departamental de Huehuetenango cuyo resultado fue la pérdida total de la información de los fiscales del Ministerio Público.

El sujeto pasivo de delitos informáticos puede abarcar a particulares, empresas o incluso las mismas instituciones estatales y es muy común escuchar la vulneración de los sistemas de seguridad en empresas y entes gubernamentales y esto se comprueba cuando se dice en muchas ocasiones que el sistema no funciona o el sistema cayó. En la esfera informática existen una gran infinidad de programas y aplicaciones que proveen a los diferentes usuarios la práctica para la vulneración de sistemas, páginas de internet, dispositivos electrónicos, servidores, entre otros y que muchas veces se encuentran en forma gratuita, es decir, el sujeto pasivo puede ser cualquier persona que esté conectada a la red informática y que muchas veces sin estarlo simplemente haciendo uso de diferentes dispositivos periféricos como por ejemplo una memoria USB o pendrive puede ser susceptible como víctima de un delito informático.

Es necesario saber cómo el sujeto activo del delito informático actúa de conformidad a las habilidades y consecuencias que sus actos ocasionan. Dentro de los más conocidos están: 1) El Hacker: es aquella persona que haciendo uso de las diferentes tecnologías de la información ingresa a las diferentes bases de datos,

descifra claves y simplemente observa sin afectar la información que tiene la vista sin embargo no vulnera la información. 2) El Cracker, es diferente ya que esta persona altera modifica destruye o bloquea la información a cambio de una contraprestación o dinero. 3) El Phreaker es aquella persona que tiene conocimientos en telefonía móvil y que con diferentes tipos de herramientas tecnológicas se dedica a la interceptación ilegal de celulares o teléfonos, para ello debemos también reflexionar que internet existe una gran variedad de herramientas, manuales e instructivos que ayudan a que una persona pueda convertirse en este tipo delincuente. 4) Hay otra técnica llamada Carding qué se refiere a aquellas personas que clonan tarjetas electromagnéticas su óptica es decir son aquellos sujetos que se dedican al fraude de tarjetas de crédito mediante diferentes herramientas tecnológicas. 5) Los llamados Lamer qué son aquellas personas que simplemente son curiosas y que sin la preparación técnica ni habilidades necesarias se dedican a buscar programas de hacking para intentar la operación de sistemas sin lograr mayor resultado. 6) También está la persona llamada Pisher, qué es quien envía diferentes códigos a correos electrónicos para obtener información de cuentas bancarias o de carácter personal.

Debemos entonces recordar que dentro de la comisión de un delito informático existen dos modalidades:

1) Como instrumento u objeto: en el cual usan los dispositivos electrónicos para llegar a su cometido, como ejemplo podemos citar la falsificación de documentos, sustracción de información de bases de datos, vulneración de códigos de seguridad, transacciones financieras utilizando cuentas bancarias falsas, uso de redes informáticas sin autorización o el conocido hackeo, interceptaciones telefónicas ilegales; para cometer todos estos actos ilícitos es necesario el uso de un instrumento relacionado con la tecnología.

2) Como fin: es decir que existe un ataque a computadoras, programas accesorios, entre otros. Como ejemplo citamos cuando un Cracker ingresa a una base de datos para alterar modificar o destruir determinada información, daña la memoria de la computadora o del dispositivo electrónico y que en muchas ocasiones utilizan ciertos códigos o Script para que dejen de funcionar algunos otros dispositivos internos como

por ejemplo un disco duro o la misma tarjeta madre. En este tipo de modalidad cabe perfectamente el llamado “Sabotaje Electrónico” con fines terroristas o políticos o la sustracción de información para posteriormente realizar algún tipo de extorsión o chantaje a cambio de una determinada cantidad de dinero.

Analicemos lo que opina el autor Santiago Acudio citando al profesor español Romeo Casabona señalando que:

> en la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes...el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información “ (Acurio del Pino, Delitos Informáticos: Generalidades)

Tomando en consideración lo anterior, si hablamos de un delito informático nos referimos a un hecho aislado y comparto lo que indica el autor Casabona, en cuanto a que a la complejidad en la que se desarrolla el Delito Informático debería entonces conocerse como una Delincuencia Informática en virtud que para que se puede consumar un hecho ilícito ya sea como instrumento o fin mediante las tecnologías de la información es necesario que concurran elementos de la Delincuencia Organizada y asimismo por la gran variedad y pluralidad de supuestos y consecuencias jurídicas es decir contemporáneamente debe ir cambiando el concepto de delito informático a una criminalidad informática en virtud que es muy incierto que se pueda unificar un solo

concepto que puede cumplir esas premisas de: esa acción típica, antijurídica y culpable en donde estén involucrados los diferentes procedimientos informáticos.

Los delitos informáticos tienen una clasificación y para el efecto son reconocidos por las Naciones Unidas así: (Hall, s.f.)

a. Fraudes cometidos mediante manipulación de computadoras

i. **Manipulación de los datos de entrada:** Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

ii. **Manipulación de programas:** Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal

iii. **Manipulación de los datos de salida:** Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

iv. **Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo:** Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

b. Falsificaciones Informáticas.

i. **Como objeto:** Cuando se alteran datos de los documentos almacenados en forma computarizada.

ii. **Como instrumentos:** Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

c. Daños o modificaciones de programas o datos computarizados.

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: **I) Virus:** Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. **II) Gusanos.** Se fabrican de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita. **III) Bomba Lógica o Cronológica**. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus

o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

d. Acceso no autorizado a servicios y sistemas informáticos.

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

i. 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.

ii. 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.

iii. Ciberterrorismo: Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de

muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

iv. Ataques de denegación de servicio: Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a muchos usuarios. Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

Después de haber analizado la información casa detallado podemos concluir que el bien jurídico que se protege en el llamado delito informático o criminalidad informática contempla la protección del patrimonio, la reserva intimidad y confidencialidad de los datos e información, la seguridad del tráfico jurídico y probatorio y el derecho de propiedad. Sin embargo, tal y como lo apuntamos anteriormente por la complejidad de los supuestos y consecuencias jurídicas que podría tener un tipo penal de carácter informático se puede inferir que un hecho podría afectar a varios bienes jurídicos es decir puede ser de naturaleza jurídica múltiple.

3.4. Riesgo inminente ante la consumación del Delito Informático.

Actualmente es necesario que se adopten diferentes medidas de seguridad y sobre todo eficientes para contrarrestar el flagelo de las consecuencias del crimen informático. Reflexionemos, cada día hay más personas conectadas al internet y que se hace presente en todo lugar tales como instituciones educativas, sistema bancario, hospitales y principalmente en el sector público. Si una empresa o una institución del Estado invierten muy poco en establecer protocolos para mejorar su seguridad

informática podrá sufrir pérdidas irreparables y que puede equipararse a información o grandes pérdidas de dinero. A diario diferentes sistemas de información son atacados y recurrentemente son jóvenes y muchos menores a los quince años, siendo que su actividad la realizan sin saber las grandes consecuencias negativas que podrían ocasionar a un tercero. Los fraudes por internet se incrementan día a día y la clonación de tarjetas de crédito es otro problema que existe a nivel mundial y que causa grandes pérdidas para los particulares y personas jurídicas. Tomando en consideración lo anterior y podemos concluir que el riesgo se incrementa día con día y si no tenemos protocolos que puedan responder a los diferentes ataques a nuestros sistemas de información o dispositivos electrónicos estamos a la espera de ser víctimas de un Delito Informático.

3.5. Situación Internacional

Cómo es de conocimiento general, el uso de los dispositivos electrónicos y digitales es cada día más útil e imprescindible para la realización de diferentes procesos en las diferentes labores del ser humano y así mismo también podemos afirmar que comúnmente se usa una computadora para poder desempeñar una función ya sea en nuestro ámbito laboral, académico, social, deportivo, entre otros. Esto también se puede observar en la práctica forense que los diferentes actores que se desempeñan en su sistema es oficio también se auxilian del uso de la informática o de tecnología para poder realizar sus funciones como por ejemplo de una computadora, es decir se usa la tecnología para la consecución de los diferentes objetivos, metas y procesos del diario vivir. Consecuentemente si existe una práctica común y útil en el uso de estos dispositivos también conlleva qué existe un mal uso de estos dispositivos qué tiende a que varios internautas transgredan límite e incurra en la comisión de actos ilícitos. Es por eso que en el ámbito internacional existen diferentes programas, iniciativas, normativas jurídicas qué se dedican a la protección de la información y la seguridad informática.

Existen diferentes instrumentos internacionales en donde diferentes países son parte cuyo fin es crear una normativa jurídica y cada país miembro a efecto de proteger

de una forma jurídico penal la información, que para perseguir penalmente a los responsables de la comisión de delitos informáticos y el control de las acciones que tienden a vulnerar información sensible de las personas. Es acá dónde surgió la necesidad de crear una legislación penal que responda a la protección del bien jurídico tutelado, como ejemplo cito la recomendación del Consejo de Europa R (89) 9 informáticos en la que se "*recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales*"

Esto nos da la idea de que debe existir la normativa pertinente que sea útil para proteger la información, que sea suficientemente adecuado para que el uso de un dispositivo electrónico digital de la certeza en el resguardo de la información.

Debemos diferenciar la justificación de la normativa jurídica, por un lado debe de existir para crear esa regulación de las acciones que se considerarían como ilícito es decir reglamentar qué acciones pueden apreciar y cuando no, en segunda instancia la normativa jurídica debe existir para el resguardo y protección de la información, en tercera instancia normativa también servirá para crear los diferentes procedimientos o protocolos que se utilizarán para la investigación y en su momento del análisis de la información que servirá para incorporarse a un proceso judicial sino referimos al ámbito público y en el caso del ámbito privado la normativa y reglamentación debe existir para dar un soporte y auxilio a los diferentes procesos irregulares que se presentan en el funcionamiento de una empresa. .

Para entender de mejor forma lo indicado podemos mencionar algunos ejemplos de esos escenarios en donde es necesario que exista una normativa jurídica actual que responda al tema de la Big Data[9] (también conocidos como Macrodatos o Datos Masivos de información) seguridad de la información, protocolos y procedimientos

[9] Los **macrodatos**, también llamados **datos masivos**, **inteligencia de datos**, **datos a gran escala** o ***big data*** (terminología en idioma inglés utilizada comúnmente) es un término que hace referencia a conjuntos de datos tan grandes y complejos que precisan de aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente. https://es.wikipedia.org/wiki/Macrodatos

establecidos por parte de los órganos de investigación, tal es el caso del espionaje por sustracción de información en forma ilegal conocido también como Phishing, el acceso no autorizado a diferentes cuentas de un usuario creando diferentes estrategias de hacking, la sustracción de contraseñas, propagación de virus que tienden a alterar los diferentes dispositivos electrónicos, bases de datos, entre otros y todo ello conlleva a que debe ser necesaria la regulación legal a efecto de poder penalizar dichos actos o hechos.

En anteriores líneas comenté sobre los diferentes grupos delincuenciales que actúan a nivel de una delincuencia organizada a través de estructuras, es decir, utilizan la interconexión de redes de computadoras para cometer delitos informáticos ya sea cómo medio objetos es decir si existe un ataque dirigido a dispositivos electrónicos o bases de datos o utilizan los mismos dispositivos electrónicos para la comisión de otro tipo de bichos llamados comunes como por ejemplo estafas, amenazas, pornografía, delitos contra el honor, entre otros. Sí hacemos una comparación en el ámbito internacional sobre la forma en que diferentes estados se han organizado para regular lo referente a los derechos informáticos podremos hacer una comparación muy interesante, porque resala que existe regulación referente a temas tales como, datos, estafa informática, falsificación de datos probatorios, entre otros; además es interesante mencionar que en Alemania se tuvo necesidad de analizar detenidamente la forma en que se debía aplicar el derecho penal tradicional a los comportamientos y secuelas qué se relacionan con los procesos electrónicos de datos y encontrar el punto de partida donde existía la lesión al bien jurídico. De lo anterior se tuvo como resultado que en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión y más compleja, pero que en realidad solo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos y para ello es necesario la existencia de una mesa de trabajo interinstitucional con el equipo multidisciplinario correspondiente para aborda la temática en forma óptima e integral.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician, además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. Como lo indica Santiago Acurio en su obra de Delitos Informáticos: el tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición. (Acurio del Pino, Delitos Informáticos: Generalidades)

En Francia existe la regulación referente al acceso fraudulento a un sistema de elaboración de datos, es decir, si una persona accede a un sistema se le sanciona, también se regula el "sabotaje informático" que consiste en la destrucción de datos la falsificación de documentos informatizados y el uso de documentos informatizados falsos, en síntesis, se refiere a esa manipulación o modificación de datos o documentos relacionados con informática. En Estados Unidos actualmente existe sanción cuando en la transmisión de un programa que tenga un virus, un gusano, un Caballo de Troya, Ramsonware otro tipo de virus afecta a otros dispositivos o sistemas digitales; cuando una computadora se ve afectada por cualquier tipo de virus la ley lo sanciona y es interesante que dentro de la regulación referente a la transmisión de virus establece que el creador de un virus no puede excusarse o alegar ignorancia de que su actuar causaría daño a una persona o un tercero. Lo que he comentado se basa en el acta Federal de abuso computacional del año 1994 la cual modificó el acta de fraude y abuso computacional.

Es interesante hacer un breve comentario de la legislación sobre delitos informáticos que tiene Chile y es que de conformidad a una de sus leyes se contempla proteger al bien jurídico tutelado en la calidad, pureza e idoneidad de la información, existe un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtenga. Varios artículos de esta ley mencionan lo referente a la distribución modificación de un sistema, apoderamiento intercepción, interferencia de la información. Interesante es indicar que referente a la protección de datos se tutela de tal forma que también se regula lo referente al daño o destrucción de datos y la difusión de contenidos en un sistema de información.

Se destaca que en la legislación chilena se contempla la figura del hacking y fraude informático y las penas dependiendo de la comisión del ilícito informático van desde 3 a 5 años de prisión. Otro ejemplo de una legislación que ha abordado los Delitos Informáticos con gran esmero es España para el efecto se menciona su Ley Orgánica número 10/1995.

Así como lo menciona el autor Santiago Acurio en su obra Delitos Informáticos: España tiene una legislación jurídica armoniosa en cuanto al fenómeno informático y a continuación se presenta un cuadro del nuevo Código Penal español en relación a la penalización de la delincuencia informática (Acurio del Pino, Delitos Informáticos: Generalidades)

Legislación Jurídica sobre la penalización de la delincuencia informática. (Acurio del Pino, Manual de Manejo de Evidencias Digitales y Entornos Informátios. Version 2.0)

INTERCEPTACIÓN DEL CORREO ELECTRÓNICO	USURPACIÓN Y CESIÓN DE DATOS RESERVADOS DE CARÁCTER PERSONAL
En el apartado correspondiente a los delitos contra la intimidad se introduce la interceptación de correo electrónico, que queda asimilada a la violación de correspondencia. El artículo 197 extiende el ámbito de aplicación de este delito a las siguientes conductas: ▣ apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales. ▣ interceptación de las telecomunicaciones, en las mismas condiciones. ▣ utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos. Estas actividades deben producirse sin consentimiento del afectado y con la intención de descubrir sus secretos o vulnerar su intimidad. La pena que se establece es de prisión, de uno a cuatro años y multa de doce a	También quedan tipificados los actos consistentes en apoderarse, utilizar, modificar, revelar, difundir o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos. El art. 197.2 castiga con prisión de 1 a 4 años para el caso de acceso, utilización, etc. y de 2 a 5 años si los datos se difunden, revelan o ceden a terceros. Cuando dichos actos afectan a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior. Esta inclusión de los datos personales en el Código Penal (a partir de aquí CP) supone una importante innovación. Este apartado desarrolla el principio de la Protección a la Intimidad, contenido en el Art. 18.3 de la Constitución Española de 1978.

veinticuatro meses (Con el nuevo concepto de días-multa, un día equivale a un mínimo de 200 pesetas y un máximo de 50.000 pesetas)	
Fraude Informático	**Daños informáticos**
El nuevo CP introduce el concepto de fraude informático, consistente en la manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina. Los Arts. 248 y siguientes establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.	En el delito de daños se contemplan los supuestos de destrucción, alteración, inutilización, o cualquier otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes, o sistemas informáticos. El art. 264.2 establece una pena de prisión, de 1 a 3 años en el caso de daños informáticos. El valor que pueden alcanzar en la actualidad los datos o la información de una empresa o administración pública en formato digital, ha obligado a incluir la figura del delito de daños informáticos en el CP.
DIFUSIÓN DE MENSAJES INJURIOSOS O CALUMNIOSOS	**Falsedades documentales**
El artículo 211 establece que los delitos de calumnia e injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante. Puede incluirse perfectamente en este supuesto la difusión de mensajes injuriosos o calumniosos a través de Internet, en especial, en el entorno www que es el más similar a la prensa tradicional. Las penas establecidas pueden llegar a los 2 años de prisión en el caso de la calumnia, y multa de hasta 14 meses en el caso de la injuria.	Los artículos 390 y siguientes castigan con la pena de prisión de hasta seis años las alteraciones, simulaciones y demás falsedades cometidas en documentos públicos. Los artículos 395 y 396 se refieren a las falsedades cometidas en documentos privados, pudiendo alcanzar la pena de prisión hasta dos años. También se castiga la utilización de un documento falso para perjudicar a un tercero. El artículo 26 define como documento cualquier soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

El artículo 212 establece la responsabilidad solidaria del propietario del medio informativo a través del que se haya propagado la calumnia o injuria. En el caso de Internet, la responsabilidad civil solidaria alcanzaría al propietario del servidor en el que se publicó la información constitutiva de delito, aunque debería tenerse en cuenta, en este caso, si existió la posibilidad de conocer dicha situación, ya que el volumen de información contenida en un servidor no es comparable al de una revista, un periódico o un programa de TV o radio. En este sentido cabe recordar la tesis que asimila al propietario de un servidor al librero, en contraposición con los que lo asimilan a un editor. La primera teoría es partidaria de liberar de responsabilidad civil al propietario de un servidor, debido a la imposibilidad de controlar toda la información que es depositada en el mismo por los usuarios.	Entendemos que quedaría incluido en el concepto documento los mensajes estáticos, compuestos por información almacenada en un sistema informático después de haber sido remitida o recibida a través de la red, pero surgen dudas sobre la naturaleza documental del mensaje que está circulando. Finalmente, el artículo 400 introduce el delito consistente en la fabricación o tenencia de útiles, materiales, instrumentos, programas de ordenador o aparatos destinados específicamente a la comisión de estos delitos, se castigarán con las penas señaladas para los autores. Entrarían dentro de este tipo los programas copiadores, las utilidades empleadas por los hackers y cualquier otro dispositivo similar.
REVELACIÓN DE SECRETOS	**Robos**
El art. 278 establece una pena de 2 a 4 años para el que, con el fin de descubrir un secreto, se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo. Si los secretos descubiertos se revelasen, difundieren o cedieren a terceros, la pena llegará a los 5 años de prisión.	El artículo 239 – Considera llaves falsas las tarjetas magnéticas o perforadas así como los mandos o instrumentos de apertura a distancia, considerando por lo tanto delito de robo la utilización de estos elementos, el descubrimiento de claves y la inutilización de sistemas específicos de alarma o guarda con el fin de apoderarse de cosas muebles ajenas.

La posición de los estados miembros de la Organización de los Estados Americanos es que el internet ha proliferado a gran magnitud y se ve inmerso en diferentes ámbitos sociales, causando un riesgo inminente de seguridad y tal y como lo referido en anteriores párrafos para nadie es un secreto que a través de los años el uso, del internet y las nuevas tecnologías de la información ha propiciado que mejoren las relaciones comerciales en el mundo, planificar actividades y ha acercado a las

personas a través de las diferentes plataformas de comunicación tal es el caso de las redes sociales y es que en el año dos mil uno en la tercera cumbre de las Américas en la ciudad de Quebec, Canadá diferentes líderes se comprometieron a aumentar la conectividad en América. Es así que en el aumento del uso del internet también ha aparejado el sinnúmero de amenazas cibernéticas que ponen en riesgo la seguridad de la información de los usuarios.

Existe una estrategia Interamericana integral de seguridad cibernética cuyo objetivo es mejorar la cultura de seguridad cibernética en las Américas y que también contempla un marco regulatorio que pueda ser capaz de responder a incidentes y recuperarse de los mismos es decir un Forensic Readiness. Dentro de algunas medidas que se contemplan están la de informar a los usuarios sobre la forma de asegurar sus computadoras o dispositivos móviles, mejorar los sistemas de seguridad en redes públicas y privadas y algo importante como lo es una legislación acorde a cada Estado para que regule lo relativo a los delitos informáticos.

En Argentina en el año 2008 se sancionaron las nuevas reformas al Código Penal en donde se incluyó la "Ley de Delitos Informáticos" y es interesante conocer en forma muy somera algunos tipos penales que están vigentes y que se regulan en este país tales como: delitos contra la integridad sexual como por ejemplo el tipo penal de ciber pornografía infantil incorporado en el año dos mil trece qué se refiere al acoso informático contra menores de edad. En este país también se contemplan diferentes tipos penales en donde se relacionan con componentes informáticos en su consumación, así como por ejemplo la falsificación, incluyéndose entonces conceptos como la firma digital, la intimidación pública a través de internet amenazas a través de diferentes plataformas digitales o informáticas y la extorsión a través de su modelo complejo utilizando redes informáticas o la llamada **Sextorsión** que es una forma de explotación sexual en la cual una persona es chantajeada con una imagen o video de sí misma desnuda o realizando actos sexuales que generalmente han sido compartidos mediante **Sexting**[10] y es cuando la víctima es coaccionada para tener relaciones

[10] Es un término que se refiere al envío de mensajes sexuales, eróticos o pornográficos, por medio de teléfonos móviles. Inicialmente hacía referencia únicamente al envío de SMS de naturaleza

sexuales con otra persona o entregar imágenes más comprometedoras o en su defecto dinero bajo la mesa difundir las imágenes en las plataformas informáticas.

3.6. El Convenio de Cibercriminalidad de Budapest

Actualmente se encuentra en vigencia el convenio de Cibercriminalidad de Budapest elaborado por el Consejo de Europa en Hungría el veintitrés de noviembre de dos mil uno y es interesante que diferentes países se adhirieron a este instrumento internacional cuyo objeto era crear los cimientos necesarios en relación a las políticas internas para la persecución penal de los Ciberdelitos es decir la creación de una legislación para cada estado para la persecución penal de esas conductas típicas y antijurídicas para ser investigadas no sólo en el estado miembro sino también la creación de los mecanismos necesarios para la persecución en diferentes Estados a través de la cooperación internacional a efecto de proteger los intereses legítimos en relación a las tecnologías de la información. Se debe considerar que en este convenio se debían adoptar todas aquellas estrategias y medidas para que los procedimientos pudieran ser eficientes.

En primer lugar, se especificaron algunas cuestiones terminológicas vinculadas con las definiciones de sistema informático, datos informáticos, prestador de servicio y datos de tráfico. Según lo refiere Di Lorio y demás autores en la obra El Rastro Digital del Delito la clasificación de los delitos informáticos, se estableció la existencia de las siguientes categorías: 1) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; 2) Infracciones informáticas; 3) Delitos vinculados al contenido; 4) Delitos vinculados a violación de la propiedad intelectual y otros derechos afines. (Di lorio. et al.)

Para que el lector pueda tener un panorama amplio de la clasificación anteriormente descrita, se presenta a detalle de cada una de las categorías según el texto “El Rastro Digital del Delito”, siendo la siguiente: (Di lorio. et al.)

---

sexual, pero después comenzó a aludir también al envío de material pornográfico (fotos y vídeos) a través de móviles y ordenadores. https://es.wikipedia.org/wiki/Sexteo

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

1. Acceso ilícito: Es el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Puede cometerse infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

2. Interceptación ilícita: Constituye la interceptación deliberada e ilegítima -por medios técnicos- de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático, o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. El delito puede cometerse con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

3. Ataques a la integridad de los datos. Es todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, pudiendo legislarse sobre la gravedad de los daños que se ocasionen.

4. Ataques a la integridad del sistema. Consiste en la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

5. Abuso de los dispositivos: Se trata de la comisión deliberada e ilegítima de los siguientes actos: a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos antes descriptos; como también de una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos antes descriptos. b) la posesión de alguno de los elementos contemplados

precedentemente con la intención de que sean utilizados para cometer cualquiera de los delitos descriptos. (Di lorio. et al.)

Cómo podemos analizar esta apartado se refiere específicamente a esa protección de datos sensibles que existen en diferentes sistemas informáticos siendo qué el objetivo ideal de una Ley de Ciberdelitos es que pueda tutelar al usuario para la no intrusión de personas ajenas para conocimiento de información de las personas ya sea a través de un acceso no autorizado, una interceptación ilegal, una modificación de datos con el objeto de crear un perjuicio o aprovecharse de la situación y también se enfoca a la forma en que puedan ser utilizados los dispositivos para obtener esa información tal podría ser el caso de uso de una computadora para poder obtener una contraseña a través de un método de Fuerza Bruta para quebrantar las medidas seguridad y obtener el código de acceso. En Guatemala está vigente la Ley de Acceso a la Información Pública decreto 57-2008, cuya naturaleza jurídica es darle certeza jurídica a las normas y los procedimientos para garantizar a toda persona, natural o jurídica, el acceso a la información o actos de la administración pública que se encuentre en los archivos, fichas, registros, base, banco o cualquier otra forma de almacenamiento de datos que se encuentren en los organismos del Estado.

El Código Penal de Guatemala en su Título sexto y capítulo séptimo referente a los Delitos contra el Derecho de Autor, la Propiedad Industrial y Delitos Informáticos regula diferentes tipos penales que tienen una cierta similitud a lo que se pretende en el convenio de Budapest específicamente en esta categoría de protección de datos. Por ejemplo, el artículo 274 inciso “A”. Destrucción de Registros Informáticos, 274 inciso “D” Registros Prohibidos, 274 inciso “E”. Manipulación de información, 274 inciso “F” Uso de información, 274 inciso G. Programas Destructivos; es decir estos tipos penales tienen un contenido que podría ser regulado en una ley de ciberdelitos con características más amplias a fin de dar una certeza jurídica al bien jurídico tutelado que en cada uno de estos artículos se protege qué es la seguridad de datos, la Integridad de las personas y protección de sistemas informáticos

En la segunda categoría encontramos los siguientes tipos: (Di lorio. et al.)

b. Infracciones informáticas

1. Falsificación informática: Dirigida a sancionar la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Puede exigirse una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

2. Fraude informático. Penaliza los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: la introducción, alteración, borrado o supresión de datos informáticos; o por cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

En la tercera categoría encontramos los siguientes tipos: (Di lorio. et al.)

c. Delitos relacionados con el contenido

1**. Delitos relacionados con la pornografía infantil**. Orientada a penalizar la comisión deliberada e ilegítima de los siguientes actos: a) La producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b) La oferta o la puesta a disposición de pornografía infantil a través de un sistema informático; c) La difusión o la transmisión de pornografía infantil a través de un sistema informático; d) La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; e) la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos. También se regula lo que se entenderá por «pornografía infantil» como todo material pornográfico que contenga la representación visual de: un menor adoptando un comportamiento sexualmente explícito; una persona que parezca un menor adoptando un comportamiento sexualmente explícito; de imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito. De igual forma se hace mención de lo que debe entenderse por «menor» como toda persona que no tiene aún 18 años de edad, que los Estados al legislar pueden reducir al límite de los 16 años.

En la cuarta categoría encontramos los siguientes tipos: (Di lorio. et al.)

d. **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines**

1. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Se pretende legislar las infracciones de la propiedad intelectual que defina cada Estado conforme a las obligaciones que hayan contraído por aplicación del Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor -a excepción de cualquier derecho moral otorgado por dichos Convenios-, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. También se regulan las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas -a excepción de cualquier derecho moral conferido por dichos Convenios-, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. Finalmente, en cuanto a la legislación de fondo que se ha descripto, la Convención establece que la comisión de todos los tipos previstos por ésta, debe ser penada por los Estados miembros, no sólo con relación a su autor, sino que también se debe castigar su ayuda y su instigación. El castigo de dichos delitos se debe realizar mediante sanciones efectivas, proporcionadas y disuasivas, que pueden llegar a incluir la privación de la libertad.

Asimismo, se estipula la posible responsabilidad de las personas jurídicas para su beneficio y cuando es cometido por cualquier persona física que actúe individualmente o como parte de un órgano de la persona jurídica que tenga una posición importante en virtud de un poder de representación de ésta, o tenga facultades para tomar decisiones en su nombre o para ejercer controles dentro de ella. La

responsabilidad puede ser civil, administrativa o penal, sin perjuicio de la responsabilidad penal que corresponda a las personas físicas que cometieron el delito.

3.7. Problemática de Persecución Penal.

El autor José Cuervo Álvarez en su libro Delitos Informáticos menciona que, en todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, o a un tercero. (Cuervo)

En consecuencia, de lo anterior, la expresión delito informático se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

Es necesario conocer algunos términos que en la terminología aplicada a los Delitos Informáticos son comunes es necesario conocer, tales como[11]:

1. Hacker. Aplicada en la computación y se refiere a la persona que se dedica a un área de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los hackers tienen "un saludable sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos".

2. Cracker. Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está

[11] https://www.coursehero.com/file/p18uoj9c/La-palabra-hack-en-ingl%C3%A9s-tiene-varios-significados-en-espa%C3%B1ol-entre-ellos/

prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

3. Phreaker. Es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

4. Gurús. Son considerados los maestros y los encargados de "formar" a los futuros hackers. Generalmente no están activos, pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales sólo enseñan las técnicas básicas

5. Carding (Tarjeteo). las personas que se ven vinculados al Carding, se ven inmersos al estudio de las tarjetas inteligentes (Smart Card), tarjetas magnéticas u tarjetas ópticas, los cuales comprenden la lectura de estos y la duplicación de las mismas.: uso ilegal de tarjetas de crédito.

6. Lamer o Script-Kiddes. Es un término coloquial inglés aplicado a una persona falta de madurez, sociabilidad y habilidades técnicas o inteligencia, un incompetente, por lo general pretenden hacer hacking sin tener conocimientos de informática. Solo de dedican a buscar y descargar programas de hacking para luego ejecutarlos, como resultado de la ejecución de los programas descargados estos pueden terminar colapsando sus sistemas por lo general destrozando su plataforma en la que trabajan.

7. Phisher. Es la persona que crea sistemas para hacer Phishing. Son delincuentes informáticos que tratan de engañar a personas para obtener información bancaria o personal, con la que puedan hacer fraude de algún tipo.

8. La liberación de Caballos de Troya: Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones no autorizadas y que la persona que lo ejecuta

no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto por ejemplo formatear el disco duro, modificar un fichero, etc.

9. Superzapping. Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un PC serían las Pctools o el Norton Disk Editor.

10. Puertas falsas (backdoors). Es una práctica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc., con objeto de producir un atajo para ir corrigiendo los posibles errores.

11. Ataques Asincrónicos. Este es quizá el procedimiento más complicado y del que menos casos se han tenido conocimiento. Se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc., de una forma periódica, si alguien consiguiera hacer caer el sistema y modificar dichos ficheros en el momento en que se ponga de nuevo el funcionamiento del sistema este continuara con la información facilitada.

12. Pinchado de líneas de datos (Spoofing): Similar al pinchado de líneas telefónicas, el objetivo son los sistemas de transmisión de datos (Cable telefónico usado por módem, cableado de una red local, fibra óptica, TV por cable) con el fin de monitorizar la información que pasa por ese punto y obtener información del sistema.

CAPITULO IV

Informática Jurídica y la Investigación Criminal en la Era Digital.

En otro capítulo definimos a la informática jurídica definiéndola como una ciencia que pertenece a la informática pero que se puede aplicar a la ciencia del derecho y que está disciplina no pertenece al área jurídica toda vez que la informática jurídica estudia los recursos informáticos como por ejemplo el Software y el Hardware utilizados en diferentes procesos, análisis, investigaciones útiles en el escenario jurídico. Es menester aclarar que la informática jurídica se enfoca a la forma en que son utilizados los dispositivos electrónicos, los programas informáticos y los sistemas de información para el control y desarrollo de procedimientos informáticos con por ejemplo el control de clientes en una empresa, formularios electrónicos, facturación automática, entre otros.

En Guatemala podemos advertir que aquella clasificación de la informática jurídica podríamos encontrarlo en diferentes escenarios por ejemplo en el caso de gestión y control la informática jurídica se aplica a la realización de contratos electrónicos, certificación de documentos emitidos por entidades gubernamentales en línea, transacciones bancarias que llevan un registro determinado. Un ejemplo muy claro de cómo es funcional la informática jurídica es la forma en que el Registro Nacional de las Personas maneja toda la base de datos en donde existe información de las personas hay registradas, entonces aquí podríamos hablar de una informática registral, otro caso interesante de aplicación son las bibliotecas virtuales y aquellos registros gubernamentales.

En el caso del Organismo Judicial, Ministerio Público y otros actores del sistema de justicia también en donde también se aplica la informática jurídica en virtud que es necesario tener un control y registro de expedientes de los diferentes casos que se tramitan siendo entonces esto una informática de gestión y control de expedientes jurídicos, sin olvidar información qué actualmente por ejemplo en la Corte de Constitucionalidad los fallos y sentencias están almacenadas en forma cronológica,

por categoría o por año. Resulta interesante ahora conocer la forma en que la informática jurídica se convierte en una herramienta indispensable en la investigación penal o criminal en esta era de la tecnología y de la información.

4.1. La investigación criminal en la era de la información.

Deseo recordar aquella definición de Criminalística y Criminología que aprendimos en las aulas universitarias indicando que la Criminalística es la ciencia que se encarga de establecer la forma en que se llevó a cabo un delito usando las diferentes ciencias forenses para darle respuesta a la hipótesis criminal del qué, cómo, cuándo, dónde, porque, a quién, con quién; mientras que la Criminología se refiere estudiar las causas y formas de su manifestación utilizando otras ciencias sociales como la Psicología, la Antropología Social, entre otras, enfocándose en el flagelo social que motiva al delincuente a cometer actos antisociales.

Tomando en consideración estas dos ciencias que son importantes para la investigación criminal podemos hacer un pequeño análisis de cómo ha evolucionado el fenómeno criminal de ir creando mecanismos acordes para su correcta investigación. Anteriormente los investigadores ya sea criminalístico o policiales utilizaban papel y lápiz para tomar notas de lo que hallaban en un escenario criminal, actualmente derivado de la complejidad de dicho escenario es necesario el uso de diferentes dispositivos que puedan dejar un registro o pueden tomar una evidencia para ser posteriormente analizar y efectivamente ese es el caso de la función que cumplen ahora las cámaras fotográficas, las cámaras de vídeo, el uso de un teléfono celular, una tableta electrónica, una computadora, entre otros.

El desarrollo tecnológico en el mundo cómo lo he mencionado en otros capítulos avanza muy rápido y el campo criminalístico no es la excepción y es que a raíz de esa complejidad de asuntos que conlleva el uso de la tecnología para la investigación criminal en muchos países con casos complicados se ha observado qué se llega a un punto de ebullición en cuál se coloca la balanza lo que son los derechos fundamentales versus la tecnología. Para tener más claro este ejemplo debemos de reflexionar que anteriormente las legislaciones clásicas regulaba no concerniente a la protección e

inviolabilidad de la vivienda, resguardo de la correspondencia y privacidad de la información cuyo fin primordial es evitar el abuso de terceros para no ingresar a una morada pero actualmente ésta inviolabilidad a la vivienda queda escueta ya que lo que se pretendía era que los terceros no afectaran derechos de terceros dañando o poniendo en riesgo la intimidad de las personas; hoy en día eso ha cambiado ya que al momento que un dispositivo electrónico está conectado a la red es muy probable que los diferentes piratas informáticos tengan acceso a mucha información confidencial y según de la intimidad de una persona sustrayendo direcciones, números de cuenta bancaria, números de teléfonos y fotografías.

Otro ejemplo a citar se da al momento de que las cámaras de seguridad que se encuentran en calles, edificios y cualquier lugar público o privado realiza un escaneo de las personas que allí transitan y para todos es sabido que existen dispositivos electrónicos capaces de realizar reconocimiento facial, reconocimiento de huella dactilar y que esto sirve para crear bases de datos de todas las personas en el mundo y es acá donde nos preguntamos ¿hasta qué punto es permitido que la tecnología en sus diferentes manifestaciones tenga un límite? y es acá donde entra en contraposición tecnología versus protección de los derechos fundamentales. Existe una ley vigente pero no positiva qué se refiere a la utilización de dispositivos electrónicos para el control de una persona que ha sido ligada proceso penal, ésta es la Ley de implementación del control telemático, Decreto 49-2016 del Congreso de la República de Guatemala, cuyo fin es a asegurar la presencia del imputado y evitar la obstaculización de la averiguación de la verdad en las personas sujetas a proceso penal. Este es un ejemplo claro de una posible vulneración a la intimidad corporal no obstante que su objeto es asegurar la presencia del sindicado ante Juez competente sin embargo también entra en tema de debate sí existe colisión con los derechos fundamentales y en síntesis esta yuxtaposición es complementaria y válida en Guatemala.

Comparto la opinión del autor Juan Carlos Ortiz que en su obra “La investigación Criminal del Delito en la Era Criminal indica

> que cada vez que realizamos o recibimos una llamada telefónica, compramos unos billetes de viaje electrónicos, revelamos a través de Internet las fotos de las pasadas vacaciones, accedemos a un foro o una red social, nos inscribimos a un boletín informativo electrónico o nos descargamos algún archivo en nuestro ordenador, etc., estamos generando una abundante información digital. Basta con googlearse para comprobar la inimaginable información actualmente disponible en la Red sobre nosotros mismos, y si a dicha información fácilmente accesible a través de la Red le añadimos toda la información sobre nosotros que se encuentra almacenada en las bases de datos de entidades privadas, organismos públicos, etc., el resultado es ciertamente incalculable (Ortiz Pradillo, 2013, pág. 6)

Sigue manifestando el Autor Ortiz Pradillo que la principal ventaja del empleo de estas nuevas medidas tecnológicas de investigación reside en su operatividad (transversalidad) para la obtención de evidencias de cualquier clase de delito, sea o no de los denominados “delitos informáticos”, pues resultan una eficaz herramienta en la investigación de cualquier tipología delictiva en la que tales dispositivos electrónicos constituyan una valiosa fuente de prueba, debido a sus actuales capacidades de almacenamiento de información y a su empleo para todo tipo de comunicaciones. Por ejemplo, pensemos en las células terroristas que se comunican mediante mensajes en clave o encriptados y publicados en blogs; el sicario que porta en su agenda electrónica un listado de sus clientes o de sus futuras víctimas; o el cabecilla de un grupo criminal organizado que guarda en su ordenador portátil documentos electrónicos sobre la contabilidad de sus operaciones, fechas y lugares de recepción y entrega de la mercancía, y los datos de contacto con otras bandas criminales. (Ortiz Pradillo, 2013)

Ortiz Pradillo también opina que el ciberpatrullaje y la búsqueda en la Red, el rastreo de ficheros que contengan imágenes y videos de carácter pedófilo, el uso de programas informáticos para la lectura automática de matrículas, la video vigilancia mediante cámaras IP con activación remota, los sistemas de imágenes aéreas, térmicas, de visión nocturna o por satélite, los equipos de reconocimiento biométrico de

los rostros de las personas, iris o de bultos sospechosos, o los programas de reconocimiento forense de voces, la utilización de radiobalizas de seguimiento de vehículos, embarcaciones o aeronaves, la utilización de georadares para escrutar y sondear el subsuelo, el empleo de pulseras electrónicas de localización permanente, el uso de la tecnología GPS para conocer la ubicación geográfica exacta de un concreto dispositivo, los sistemas informáticos de detección de tiroteos gracias a la triangulación geográfica del sonido que recogen unos sensores acústicos o el control en tiempo real de los movimientos bancarios y el uso de las tarjetas de crédito, son sólo algunos ejemplos de lo que la tecnología puede facilitar las labores policiales de seguimiento e investigación. (Ortiz Pradillo, 2013)

Comparto lo que expresa el autor citado en virtud que en esta era digital los criminales en muchos casos dejan un rastro digital evidencia del ilícito y es que muchos influenciados por el consumo tecnológico, en entre otros fenómenos sociales relacionados con las redes sociales, tienden a publicar con fotos o vídeos los acontecimientos de su vida y más aún cuando realizan algo diferente no fuera lo común dejan evidencias y estás se convierten en fuente probatoria y todo este material es susceptible para extraer información y presentarlo como prueba juez competente para que se valorada, evidentemente ajustándose a los estándares y protocolos internacionales y la legislación guatemalteca.

El uso de las cámaras de seguridad, el monitoreo a través de la red, los programas son capaces de darle lectura a las placas de los vehículos son ejemplos muy claros de esos mecanismos innovadores para la investigación y persecución penal. En Guatemala existen en la ciudad capital el sistema LPR (Lectura de Placas Vehiculares) cuyo sistema consiste en una grabación de cámaras de seguridad que se encuentran en diferentes puntos de la ciudad y que derivado de su gran capacidad de alcance y toma fotográfica y video tiene la capacidad de identificar placas de vehículos y que muchos casos son útiles para la investigación criminal, consecuentemente para para el esclarecimiento de diferentes hechos delictivos.

4.1.1 Directrices de investigación criminal tecnológica y fronteras nacionales

Cuando nos referimos a la investigación criminal debemos situarnos en el escenario criminal y consecuentemente todo el procedimiento que se debe agotar para que ese indicio inicial pueda convertirse en un medio probatorio útil, legal y suficiente susceptible de presentarse ante un Tribunal o Juez Unipersonal de Sentencia. Esta evidencia electrónica y digital debe catalogarse como prueba científica que respalde otros medios de prueba y que además debe ser integra sin haberse quebrantado la cadena de custodia respectiva.

Como lo comenta Ortiz Pradillo en su obra “La investigación del delito en la era digital”, explica que el efecto CSI que fue una encuesta practicada a varios Jurados en los Estados Unidos estableció que los miembros del Jurado tienden a absolver a los acusados en aquellos casos en los que durante el juicio no se presentó una evidencia científica, salvo que se presentara el testimonio de la víctima. (Ortiz Pradillo, 2013). Este estudio nos da la pauta que en el escenario forense de otros Estados el uso de la tecnología aplicada al campo de la criminalística es necesaria especialmente en los llamados Ciberdelitos.

En esta era digital el tema de la criminalidad y la persecución penal y los diferentes estados o países del mundo y a día se vuelve más compleja toda vez que la consumación de los diferentes ilícitos penales se realiza la luna forma muy variable. Los medios de comunicación internacionales a diario no dan a conocer sobre los diferentes eventos de investigación que se realizan para poder ubicar a los criminales y específicamente aquellos que utilizan como medio objeto un objeto a la tecnología. También es bien sabido que dentro de las principales diligencias de investigación que se realizan actualmente están la clonación de unidades de almacenamiento o discos duros y el análisis de diferentes dispositivos electrónicos y normalmente en la realización de allanamientos en diferentes inmuebles y aquí es donde se tiene un contacto físico con las evidencias y vale la pena cuestionar de qué forma se preservan y garantizan los Derechos Constitucionales para no vulnerar derechos fundamentales sin embargo en el entorno digital, los parámetros de ubicación rastreo y obtención de evidencia varía significativamente. Un ejemplo claro de ello es cuando se realiza un

allanamiento y en el inmueble se encuentran diferentes equipos dispositivos electrónicos y a grandes rasgos se estima que como prueba *per se* es suficiente para poder encausar un proceso penal, sin embargo, el escenario criminal cambiaría al momento que el equipo informático incautado no sea el que se haya utilizado para crear, modificar, recopilar o transferir la información que se está investigando sino que simplemente sea un canal de comunicación a través del cual la información se envió a otro lugar, por ejemplo otro continente del globo terráqueo. Cabe entones preguntarse ¿Qué mecanismos son utilizados para poder acceder a una información que no está almacenada físicamente en el equipo sujeto de investigación, sino que se encuentra en otra parte del mundo? ¿Es legítimo y legal el acceso a través de este equipo?

Entendemos a la referida deslocalización de la información digital como el acceso a la información desde un punto determinado y que no obstante que dicha información no es originaria o se encuentra alojada se permite accesar desde ese punto de referencia, consecuentemente aquí surge el uso de las nubes de información o también llamados Cloud Computing cuya funcionalidad se refiere a que la información está almacenada de manera permanente en servidores que se encuentran en cualquier parte del mundo y son accesibles a través de la conectividad y acceso a internet, utilizando para el efecto diferente dispositivos electrónicos tales como computadoras, teléfonos inteligentes, entre otros.

Para darle seguimiento al tema de la deslocalización de la información digital es menester conocer lo que opina Juan Ortiz en su texto “La Investigación del delito en la era digital”, indicando que “La trascendencia jurídica de la ubicación física de las pruebas electrónicas, a los efectos de lograr su incautación cuando se encuentran en el extranjero, nos hace recordar que la expresión “Internet no conoce fronteras” favorece al delincuente, porque en el plano policial las fronteras nacionales se convierten en auténticos obstáculos para las legítimas labores de investigación y recogida de las evidencias de dichos delitos. Las fuerzas y cuerpos de seguridad deben respetar la soberanía de otros países y, como norma general, no pueden llevar a cabo actividades de investigación y obtención de pruebas fuera de su jurisdicción” (Ortiz Pradillo, 2013)

Se debe considerar que la colaboración internacional en materia de persecución penal no es siempre efectiva por temas de protocolos, convenios internacionales o burocracia, además no todos los países cuentan con la misma estructura y capacidad de responder a un apoyo en este tipo de áreas, consecuentemente si un país es ineficiente para prestar este auxilio se corre el riesgo que las evidencias se puedan alterar o perder. A causa de lo expuesto nos enseña que los diferentes entes de investigación deben prestar la cooperación necesaria a través de nuevos mecanismos a efecto de obtener las evidencias electrónicas y digitales. Un ejemplo de ello fue lo discutido en la reunión de fecha veintiocho de marzo de dos mil diecisiete referente a la Fuerza de área Trinacional de El Salvador, Guatemala y Honduras para el combate de la Criminalidad Organizada Transnacional que en sus estrategias de trabajo número tres se incluyó “utilizar los diferentes medios tecnológicos con que cuenta cada país de la región para garantizar el envío de información.” (2017)

Los delitos que se cometen a través del internet se convierten en un entorno complicado de investigar en virtud de la gran amplitud geográfica en la que pudiese ser cometido, detalle que se ve reflejado en la determinación del tiempo, modo y lugar de la comisión del acto ilícito. Es entonces que se deriva la complejidad de determinar cómo se debe aplicar la competencia territorial de las diferentes judicaturas u órganos con estas facultades a lo largo y ancho del globo terráqueo y si le agregamos la capacidad que debe tener el recurso humano, este es otro detalle que impide una adecuada y eficiente persecución penal.

A nivel mundial existen diferentes mecanismos legales y técnicos que facilitan la investigación y el rastreo de información con la consigna de cooperación judicial en la obtención de pruebas en procesos penales transfronterizos, como por ejemplo los siguientes: 1. Convenio relativo a la asistencia judicial en materia penal entre Estados miembros de la Unión Europea. 2. Convenio del Consejo de Europa sobre el Cibercrimen. 3. Propuesta de Directiva sobre el exhorto Europeo de Investigación Criminal.

Es necesario apuntar que estos instrumentos legales fueron creados para tener registros transfronterizos de equipos informáticos para que las autoridades extendieran

el alcance de conectarse a equipos que se encuentran conectados al equipo originariamente investigado y con ello obtener las evidencias almacenadas en aquellos no obstante se encontraran en un lugar diferente (en el extranjero). Ante este extremo cabe resaltar lo que para el efecto establece el artículo treinta y dos del Convenio sobre Ciberdelincuencia que refiere "…una parte podrá, sin autorización de otra: "(…) a. Tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos o tener acceso a datos informáticos almacenados en otro Estado o recibirlos a través de un sistema informático situado en su territorio, si dicha parte obtiene el consentimiento lícito y voluntario de la persona siguiente autorizada a revelárselos por medio de ese sistema informático". (Ciberdelincuencia).

El autor Juan Ortiz en su texto "La Investigación del delito en la era digital" cita algunos ejemplos de la funcionalidad de las Leyes relativas al Cibercrimen en diferentes países indicando que:

> en Australia permite extender el examen del equipo informático con motivo de un registro domiciliario, tanto a los datos contenidos en cualquier dispositivo de almacenamiento de datos extraíble, como a los datos almacenados en un dispositivo en una red informática de la que el equipo investigado forme parte, incluidos los datos no almacenados en el domicilio (*including data not held at the premises*) y si dicho registro se prevé que tenga efectos extraterritoriales, la Surveillance Devices Act de 2004 dispone que el juez comunique dicha medida de investigación a la autoridad competente de dicho país extranjero, entendiendo por dicha autoridad quien pudiera conceder, conforme a las leyes de dicho país, similares medidas de vigilancia. En los EE.UU., se ha admitido jurisprudencialmente la admisibilidad de los registros transfronterizos para la obtención de datos almacenados en un equipo, aunque éste se encuentre en un país extranjero, y su validez probatoria en el posterior proceso judicial en territorio norteamericano. En Holanda también cabe extender el registro de un equipo informático

conectado a la red a otros sistemas que se encuentren conectados al equipo originariamente investigado, siempre que dichos sistemas sean legalmente accesibles a la persona que habitualmente utiliza o trabaja con dicho equipo, aunque en la praxis se ha entendido tales registros no pueden exceder de las fronteras holandesas en coherencia con los principios del Derecho internacional… Y en Portugal, la Ley portuguesa sobre el Cibercrimen posibilita extender el registro de un equipo informático a aquellos otros sistemas que resulten accesibles a través del equipo inicialmente examinado, cuando existan motivos suficientes para creer que los datos solicitados se encuentren en aquéllos, con expresa mención a los correos electrónicos y demás comunicaciones electrónicas, requiriéndose siempre autorización judicial, y aplicándose en todo lo no previsto la normativa establecida para la intervención de la correspondencia…" (Ortiz Pradillo, 2013, págs. 15-16)

Como podemos observar es más que evidente la funcionalidad del acceso a la información entre Estados y que es necesario un instrumento legal que pueda normar lo relativo a la deslocalización de la información digital y vemos la necesidad que los jueces puedan conocer y aplicar estos instrumentos a efecto de darle una certeza jurídica a los elementos probatorios, en virtud que de no contar con ningún marco normativo crea una gran deficiencia en el sistema de justicia, específicamente en Guatemala.

4.2. Incidencia de la investigación criminal tecnológica en la vulneración a los derechos fundamentales.

Como hemos referido en otros capítulos la investigación criminal cada día se vuelve más compleja en virtud de los análisis de los diferentes elementos de convicción que podrían servir en un proceso penal. Es necesaria la utilización de diferentes herramientas o metodologías contemporáneas, en este caso las herramientas o mecanismos tecnológicos que aportan y coadyuvan en una investigación general.

Las Tecnologías de la Información y Comunicación se materializan en una infinidad de dispositivos o sistemas sin embargo hay que considerar qué paralelamente al desarrollo de estas tecnologías también existe el riesgo inminente de una afectación a los derechos fundamentales de una persona que está siendo investigada. La Constitución Política de Guatemala en su Artículo dos expresa lo referente a los deberes del Estado y uno de ellos es proveer seguridad a los habitantes de la república, además, el artículo cuarenta y cuatro de esta misma Carta Magna establece lo relativo a los derechos inherentes a la persona humana que en su parte conducente indica *que los derechos y garantías que otorga la constitución no excluyen otros que aunque no figuren expresamente ellos son inherentes a la persona humana* y es acá donde debemos analizar en qué momento el uso excesivo de las tecnologías de la información y comunicación para proteger o proteger un derecho es sobrepasado o se excede de sus límites y atenta contra los derechos fundamentales de una persona.

Existen una infinidad de ejemplos en donde podemos hacer una integración y razonamiento a efecto de comparar la forma en que las Tecnologías de la Información y Comunicación son utilizadas y están en el límite a la vulneración de los derechos fundamentales por ejemplo cuando se utilizan diferentes dispositivos electrónicos para la grabación de conversaciones entre personas, dispositivos técnicos para ver y escuchar entre muros lo que sucede en un domicilio, el uso de escáner corporal para descartar el uso de dispositivos explosivos y otros que pudieran afectar a terceros, el uso de algoritmos a través de programas informáticos para descifrar las conductas humanas, el uso de geolocalizadores como por ejemplo las ***Balizas Digitales*** que son utilizadas para darle seguimiento a personas o ubicar su geo posicionamiento. Otro ejemplo es el uso de dispositivos electrónicos adaptables a la muñeca con el objeto de poder controlar a una persona y verificar el cumplimiento de las diferentes medidas impuestas y ordenadas por un órgano judicial. En Guatemala está vigente la Ley de Implementación del Control Telemático en el Proceso Penal cuyo objeto, según uno de sus considerandos es el control telemático como herramienta estratégica para asegurar la presencia del imputado y evitar la obstaculización de la averiguación de la verdad en las personas sujetas a proceso penal, ubicar a las personas que se encuentran

cumpliendo una pena a través de su libertad anticipada, o bien para proteger la integridad de las víctimas de violencia contra la mujer.

De conformidad a la opinión vertida por el autor Juan Carlos Ortiz en su obra “La Investigación del Delito en la Era Digital” refiere que

“…un interesante ejemplo de ponderación judicial sobre la proporcionalidad de los nuevos instrumentos tecnológicos y su empleo en las labores de investigación criminal, a la hora de determinar si vulneran o no los derechos fundamentales de las personas, lo constituye la doctrina de la Corte Suprema estadounidense relativa a la Cuarta enmienda (protección de la intimidad frente a pesquisas y registros) y a la necesidad de que las autoridades policiales necesiten de una orden judicial previa para poder llevar a cabo determinadas actuaciones que puedan considerarse “búsquedas y registros” a efectos constitucionales”. (Ortiz Pradillo, 2013, pág. 18)

Al efecto de lo que indica el autor anteriormente se estima que de existir un equilibrio entre la necesidad de que se lleve a cabo una investigación haciendo uso de las diferentes tecnologías de la información y comunicación y la protección a los derechos fundamentales de una persona como por ejemplo el respeto a su privacidad y ella se logra con efectivamente se realiza una justificación de la utilidad y alcance de esa diligencia sin que exista otra que pudiera suplirla.

Para un análisis más detenido de lo indicado y nos referiremos a la opinión de Tribunales Constitucionales de otros países referente al tema del uso de estas tecnologías y la ponderación protección a los derechos fundamentales se citan algunos ejemplos concretos, siendo los siguientes. (Ortiz Pradillo, 2013, págs. 20-26)

a) **Estados Unidos de América**: Caso Olmstead (1928), en donde la Corte Suprema estimó que la grabación policial de las conversaciones telefónicas no vulneraba la protección constitucional de la Cuarta Enmienda porque no se había llevado a cabo una “invasión física de su domicilio”, mientras que en el caso Silverman (1961) declaró que la instalación

de un micrófono en la pared exterior adyacente a la vivienda —instrumento denominado comúnmente “spike mike”— sí constituía un registro ilegal a los efectos de la cuarta enmienda, porque constituía una entrada física en las propiedades de los acusados. El Caso Katz (1967) cuando la Corte Suprema estadounidense proyectó la protección constitucional sobre las comunicaciones telefónicas en atención a la “expectativa razonable de privacidad del individuo” en relación con la Cuarta Enmienda, superando la doctrina restrictiva basada en la afectación a la propiedad que había sido emitida anteriormente y declarando que la Constitución “protege personas, no lugares”, y advirtiendo que la aplicación de la Cuarta Enmienda depende de si la persona que invoca su protección puede reclamar dicha expectativa legítima en atención a dos criterios: de un lado, si la persona ha mostrado una real (subjetiva) expectativa de privacidad, y de otro lado, si los poderes públicos deben reconocer dicha expectativa como “razonable”. El caso Ciraolo (1986) se llegó a la conclusión de que la utilización de un helicóptero y una cámara fotográfica de 35 mm para fotografiar una plantación de marihuana en una finca no constituía una violación de la Cuarta Enmienda, ya que la droga podía ser apreciada a simple vista, que el uso de helicópteros y avionetas privadas se ha convertido en una práctica cotidiana a nivel comercial y que la protección de la Cuarta Enmienda de la casa nunca se ha ampliado para exigir a la policía cerrar sus ojos al caminar por la calle o, como en el caso examinado, al sobrevolar una casa, pues dicha vigilancia en helicóptero se llevó a cabo de forma visual sin el empleo de complejos instrumentos tecnológicos. Por el contrario, en el caso Dow Chemical (1986), la Corte Suprema declaró que la vigilancia de la propiedad privada mediante el uso de equipos de vigilancia por satélite, de carácter muy complejo y que no están generalmente disponibles al público, podría ser constitucionalmente proscrita en ausencia de una orden judicial. Y de igual modo, en Kyllo (2001), el debate giró en torno al grado de intromisión de los instrumentos y equipos de investigación utilizados, en un caso en donde se utilizaron dispositivos de visión térmica para percibir desde la vía pública las

emanaciones térmicas producidas dentro de un domicilio donde se sospechaba que se estaba cultivando marihuana con lámparas de rayos UVA. Otro caso es si la persona que instala en su ordenador un programa P2P[12] que habilita para compartir archivos, dando así a cualquier persona con acceso a Internet la posibilidad de acceder a su equipo para descargarse dichos archivos, no tiene ninguna expectativa razonable de privacidad en los contenidos compartidos de ese equipo, de modo que no vulnera la Cuarta Enmienda la posibilidad de que la policía pueda utilizar un determinado software para localizar y descargar de forma remota tales archivos compartidos, incluso aunque el equipo informático en el cual se almacenan los mismos se encuentre en el domicilio del sospechoso. En virtud de lo anterior este Tribunal de alto rango maneja tres interrogantes: 1. ¿Cuál es el objetivo de la vigilancia a través de instrumentos tecnológicos? 2. ¿Qué clase de información se revela con dicho tipo de vigilancia? 3. ¿Cuál es la naturaleza de los medios técnicos utilizados?

El criterio personal que integran la respuesta a las interrogantes planteadas es que para que no exista esta afectación a los derechos fundamentales es necesario que exista una justificación plena de la diligencia, tener clara la información que se obtendrá y saber si los medios a utilizar son comunes y no sobrepasa la esfera de conocimiento publica de la herramienta tecnológica a usar y por último que no exista ningún tipo de expectativa o elemento de que está alterando la privacidad.

b) **Alemania**: El debate constitucional en torno al dualismo intimidad-tecnología se produjo con la regulación de la medida de investigación denominada «vigilancia acústica del domicilio» (Grosser Lauschangriff), hasta el punto que motivó la modificación de la Constitución germana en virtud de lo declarado por el Tribunal Constitucional alemán en

[12] Una **red *peer-to-peer***, **red de pares**, **red entre iguales** o **red entre pares** (***P2P***, por sus siglas en inglés) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. https://es.wikipedia.org/wiki/Peer-to-peer

2004 y en dicha sentencia se aprecia como lo debatido no era tanto la posibilidad del legislador de permitir dicha medida de investigación con el fin constitucionalmente legítimo de perseguir la delincuencia, sino la forma y modo en que debía llevarse a cabo la vigilancia del domicilio particular, pues para el intérprete germano “existe un núcleo inviolable en el que el particular desarrolla su vida privada, el cual debe ser respetado por el Estado al llevar a cabo medidas de vigilancia”. Otra medida tecnológica de investigación analizada por el Tribunal Constitucional alemán fue la utilización de las balizas de seguimiento GPS por parte de la policía, legitimadas en el año 2005, en donde se volvió a advertir de los peligros que el desarrollo de la tecnología puede suponer para el derecho a la privacidad. En aquel caso, el tribunal estimó que el uso de la tecnología GPS para revelar la ubicación de una determinada persona o su permanencia en un lugar determinado, aunque significaba una injerencia sobre el derecho a la intimidad del sospechoso, su alcance e intensidad no llegaban a tal nivel que se entendiera vulnerada la dignidad humana o su núcleo de desarrollo de la vida privada, si bien el tribunal constitucional advirtió de la necesidad de estar atentos ante el rápido desarrollo de las tecnologías de la información y su uso como medidas de investigación que pudieran vulnerar el derecho constitucional a la autodeterminación informativa, en el sentido de posibilitar una vigilancia total sobre un sujeto (Rundumüberwachung) y construir un perfil integral de la personalidad de un individuo que sería constitucionalmente inadmisible. Y también debe indicarse que, en el año 2010, el intérprete constitucional germano vuelve a advertir el riesgo de que el uso de la tecnología, a través del acopio y cruce masivo de datos, pueda dar lugar a la creación de los referidos “perfiles de personalidad” de los ciudadanos hasta el punto de llegar a influir de manera determinante en el comportamiento de los individuos, lo cual entiende que no sólo va en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional

elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar.

c) **España:** Refiere el Tribunal Constitucional español la protección de los derechos fundamentales de la persona y el empleo de la tecnología se persigue un fin legítimo como es la investigación criminal por parte de las autoridades judiciales y policiales, lo representa la STC 173/2011, de 7 de noviembre, en donde expresamente se pronuncia sobre la necesidad de establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas -en particular, la intimidad personal- a causa del uso indebido de la información así como de las TIC durante la investigación criminal. De conformidad a la legislación española refiere que se ha admitido de forma excepcional que en determinados casos y con la suficiente y precisa habilitación legal sea posible que la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que respeten las exigencias dimanantes del principio de proporcionalidad, y existan razones de urgencia y necesidad que motiven la intervención policial inmediata. De igual modo, también ha legitimado reiteradamente uno de los avances tecnológicos más utilizado en la lucha contra el crimen: el sistema informático SITEL de interceptación de las telecomunicaciones en sustitución de las grabaciones en cintas magnetofónicas. En numerosas sentencias, el Tribunal ha analizado el rango jurídico de la regulación de los requisitos técnicos y operacionales para proceder a ejecutar los mandamientos judiciales de interceptación de las comunicaciones, el funcionamiento de los servidores centrales y los niveles de seguridad en cuanto al acceso a la información allí alojada y su grabación en un DVD sellado digitalmente para su posterior entrega a la autoridad judicial, el bloqueo de los datos contenidos en el servidor central una vez que concluye la investigación que motivó la interceptación y el régimen de su posterior borrado físico a instancias de la autoridad judicial , así como la autenticidad y ausencia de

manipulación de tales DVD con los datos volcados del servidor, hasta llegar a concluir que el SITEL cumple con todas las exigencias y garantías propias de esta clase de diligencias de investigación y probatorias que cuentan con una previa autorización judicial para su práctica.

Como pudimos analizar de la lectura de esos casos relevantes que originaron cambios significativos en la legislación en materia tecnológica e informática se observa que tienen similares líneas de acción siempre enfocándose a la protección de la información y la intimidad de las personas. Además, es necesario conocer algunas fuentes procedimentales que originan medios de prueba en esta rama objeto de estudio y análisis, se hace entonces necesario que nos enfoquemos a la parte procedimental de un proceso en este caso en materia penal y es por eso que haremos mención de esos detalles específicos y necesarios sobre esas medidas probatorias.

Es menester hacer un recorrido sobre los aspectos procesales que contempla el convenio de Budapest, siendo éstos los siguientes:

1) De la conservación rápida de datos almacenados en medios informáticos: que se refiere específicamente a la protección integral de los datos en determinado tiempo.

2) De la conservación y revelación parcial de datos sobre el tráfico de información: que se refiere específicamente a esa conservación de datos durante el tráfico de información de un proveedor de servicios a otro o al usuario final.

3) Del Registro y confiscación de datos informáticos almacenados: que se refiere al registro Ingresó a un sistema informático o a un medio de almacenamiento.

4) De La obtención en tiempo real de datos sobre el tráfico: qué se refiere específicamente a la obtención en tiempo real sobre las comunicaciones e información Qué se transmite en el instante utilizando para el efecto un sistema informático, Hay que tomar en cuenta que se refiere a la captación de tráfico más no el contenido.

5) De la interceptación de datos sobre el contenido: este se refiere a la obtención del contenido de las comunicaciones que se transmiten utilizando un sistema informático o proveedor de servicio. Más adelante en otro capítulo abordaremos este punto para su mayor análisis y comprensión

4.3. Desafíos de la investigación criminal en la era tecnológica y digital.

Como hemos hecho referencia en capítulos anteriores el reto de los entes policiales y autoridades encargadas de la persecución penal y la investigación del delito cada día se vuelve más compleja en virtud que la criminalidad posee herramientas más avanzadas y que tienen relación íntima con la tecnología y en virtud de ello ese tipo de investigación criminal se vuelve particular y con cierto protagonismo. Es menester vislumbrar un escenario dual en dónde los medios tecnológicos son el medio de investigación y el otro en donde serán objeto de análisis e investigación.

También podemos inferir que en el afán de encontrar esa información que nos servirá para sustentar nuestra investigación entraremos al límite entre la legalidad e ilegalidad en virtud que al referirnos a estos desafíos de la investigación criminal en la era digital nos sitúa en un escenario en donde se pueden afectar intereses de las personas es decir puede verse afectada la intimidad de las personas desde el momento en que se obtiene la información y esto lo afirmó toda vez que en muchas ocasiones es necesario la ejecución de medidas de carácter intrusivo es decir sin autorización alguna. No obstante, esto es necesario acotar que este tipo de acciones se desarrollan en una esfera enmarcado en el ámbito privado de la persona investigada y los procedimientos a desarrollar deben estar reglamentados o normados por ciertas formalidades legales tal es el caso de las interceptaciones telefónicas.

Para nadie es un secreto que mucha información qué ayuda a perfilar a una persona se encuentra en las redes sociales y por más que intentemos eliminarlas siempre habrá mecanismos en la red para poder recuperarla o tener el indicio de su existencia, es decir la vida privada de una persona está en la red y está expuesta y es accesible a ella desde cualquier dispositivo conectado a la misma. Existen varios ejemplos en donde se pueden apreciar las vulnerabilidades de seguridad y el nulo o

escaso conocimiento de los procedimientos adecuados para el manejo de una posible evidencia. Los correos electrónicos que en algunos lugares del mundo para poder obtener el contenido del mismo se secuestran servidores o equipos completos sin seguir ningún procedimiento preestablecido o también llamado protocolo.

Existen otros casos en donde el desarrollo de la persecución penal es necesario investigar la visita que se realizó a determinados sitios Web y el problema es que la política de persecución penal no contempla el marco normativo o reglamentario para obtener esa información personal ocasionando consecuentemente la vulneración a la intimidad de las personas. La Unión Europea declaró que la retención de datos es contraria a los Derechos Humanos si no se tiene un procedimiento o protocolo preestablecido toda vez que se estaría obteniendo la información para una investigación criminal mediante la recolección de metadatos ocasionando una restricción a la libertad, debido proceso y presunción de inocencia. Si deseamos efectuar una comparación a nuestro contexto social y jurídico puedo mencionar el accionar de las empresas de telefonía que funcionan en el país que retienen (almacenan) información para los usos que en su momento correspondan como por ejemplo tener un historial de todo el flujo intercomunicacional de un usuario durante un determinado tiempo.

Es interesante lo que menciona Marianne Díaz en su obra Retención de Datos y Registro de Teléfonos Móviles, indicando que:

“la seguridad nacional y la prevención y persecución del crimen son los argumentos más frecuentemente empleados para justificar la creciente vigilancia a las comunicaciones, incluyendo la acumulación de datos sobre esas comunicaciones (...) La ola de implementación de registros obligatorios de tarjetas SIM se inicia en 2003, con las normativas de Brasil, Alemania y Suiza (GSMA, 2013) y para 2016 alrededor de 90 países requerían registro obligatorio a los usuarios de tarjetas SIM (GSMA, 2016). En su mayoría, las autoridades que implementan estas medidas emplean como justificación la necesidad de utilizar la información como una herramienta en la lucha contra el terrorismo y el crimen organizado (Kapellmann y

Reyes, 2015). También, aunque en menor medida, son empleados como argumentos el combate al robo y hurto de dispositivos móviles, así como la necesidad de disminuir la pérdida de recursos en la movilización del personal de policía y servicios de emergencia en casos de llamados de broma (Eagle News, 2016) (…) La aplicación efectiva de estas medidas en diversos países del globo ha demostrado la inexistencia de un vínculo claro entre las medidas de registro obligatorio y la prevención del terrorismo o del crimen organizado (Privacy International, 2004). En el caso latinoamericano, México modificó en 2009 su legislación procesal penal nacional y de telecomunicaciones, con la finalidad de establecer la creación del Registro Nacional de Usuarios de Telefonía Móvil (RENAUT), el cual obligaba a que los proveedores de servicios de telecomunicaciones llevaran un registro en el cual cada teléfono celular estuviera asociado de manera clara a un ciudadano, siendo este registro accesible a petición del Ministerio Público, que tendría acceso a datos como la geolocalización del dispositivo o el contenido de las comunicaciones. Sin embargo, estas disposiciones se derogaron apenas tres años después, puesto que, en lugar de disminuir, el porcentaje de comisión de los delitos en cuestión aumentó dentro de la vigencia del régimen (GSMA, 2013)" (Diaz, 2017).

Esto nos da la pauta que todas aquellas normativas de retención de información son útiles para temas de investigación, pero no precisamente para reducir los índices de delincuencia sino simplemente para tener un elemento más de convicción o de consulta.

4.4. Técnicas de investigación criminal en el ámbito internacional.

Antes de referirnos a las diferentes técnicas empleadas por los cuerpos policiales a nivel internacional es necesario mencionar aspectos que deben ayudarnos a reflexionar sobre la forma en que dentro de la sociedad actual se percibe a la

delincuencia. Día a día a través de diferentes medios de comunicación se nos informa sobre diferentes eventos en donde ha ocurrido un hecho ilícito. Pareciera que los medios de comunicación nos proveen de una clase magistral de Derecho cuando diversas personas opinan, detallan y critican sobre lo ocurrido en un escenario criminal, se anticipan a tachar a las personas de delincuentes, la sobreexposición del sospechoso ante los medios y el desgaste que sufren sin siquiera habérseles escuchado en una primera declaración, tal como se refiere en diferentes textos la criminalidad y delincuencia son parte de una industria del delito a través del cual diferentes sectores sobreviven y coexisten aprovechándose de las circunstancias que acaecen en un escenario criminal.

Tal y como lo refiere el autor Julio Leal en su texto Técnicas Policiales y Judiciales en la investigación criminal es importante conocer estas técnicas y métodos especificando que: “es una necesidad imperiosa para no perderse en el mundo moderno en que nos encontramos dominado por el auge que tienen este tipo de disciplinas y materias en las culturas democráticas, donde la curiosidad por el mundo de lo prohibido y morboso, se ha disparado, pero el interés social por lo criminal, no actúa sólo, sino que cuenta con una serie de protagonistas alrededor del cual se mueve toda investigación penal. Dejando a un margen al agresor y su víctima” (Leal Medina, 2011).

En el contexto de una investigación tenemos la interacción de diferentes sujetos y específicamente en Guatemala tenemos al Ministerio Público y sus equipos especializados de investigación dentro de los cuales podemos mencionar a la Dirección de Análisis Criminal (DAC), la Unidad de Métodos Especiales de Investigación (UME), la Dirección de Investigaciones Criminalísticas (DICRI), entre otros, mismos que se encuentran regulados en la Ley Orgánica del Ministerio Público y Ley contra la Delincuencia Organizada. Otros actores en el ámbito de la investigación criminal está la intervención y trabajo de la Policía Nacional Civil y sus diferentes unidades y secciones especializadas. Dentro del presente texto de investigación debemos hacer mención de la Unidad contra el Cibercrimen de la Policía Nacional Civil, el cual es de reciente creación y funcionamiento en Guatemala.

Dentro de las técnicas comunes que podemos encontrar en el pleno de una investigación de carácter tradicional en donde existe una escena con aspectos básicos podemos mencionar: análisis o rastreo de la huella dactilar, análisis biológico como ejemplo el Acido Desoxirribonucleico (ADN), análisis de rasgos o características propias del sospechoso como ejemplo fotos robot, acústica forense, entrevistas e interrogatorios, peritajes lingüísticos, exámenes médicos forenses, álbum fotográficos, grafotecnia, inspección ocular del lugar en donde acaecieron los hechos, análisis de cámaras de seguridad, auditoria forense, análisis intercomunicacional, análisis criminal, análisis balístico, métodos especiales de investigación, entre otros. Sin embargo, en el plano de la investigación digital existen técnicas de investigación tales especificas tales como: Análisis de volcado de memoria RAM, análisis y extracción de información de dispositivos electrónicos, análisis de correo electrónico, búsquedas avanzadas en computadoras, análisis y ubicación de direcciones IP, investigación en redes sociales, técnicas avanzadas de búsqueda en la internet, análisis de malware[13], análisis de memoria principal, entre otros; todas éstas técnicas en su conjunto forman parte de esa labor que realiza el perito forense digital en su labor de investigación.

Más adelante veremos la forma en que se desarrolla la aplicación de estas técnicas de investigación cuyo objeto final es darle certeza y legalidad a la prueba digital y electrónica con la oportuna cadena de custodia.

[13] “software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

CAPITULO V

Cadena de Custodia Digital y Directrices para el Tratamiento de la Evidencia Electrónica y Evidencia Digital.

5.1. Cadena de Custodia Digital.

a. **Consideraciones Generales:** Inicialmente nos hemos enfocado a explicar sobre algunos aspectos teóricos en relación a la prueba electrónica y digital y en este apartado debemos desarrollar lo referente a la importancia de la cadena de custodia que no solamente es la física sino más bien es la electrónica y digital que interesa en la presente investigación, siendo una parte medular de este tema. En el Ministerio Público existe una Dirección de Investigaciones Criminalísticas cuyo trabajo es de investigación y recolección de evidencias y que de conformidad a la Instrucción General número 07-2006 de fecha treinta de octubre de dos mil dieciséis del Fiscal General de la República y Jefe del Ministerio Público y es ahí donde se contienen las Directrices Generales para la aplicación del Manual de Procedimientos para el Procesamiento de Escenas del Crimen en su contenido indica que “todos los fiscales y técnicos de la Dirección de Investigaciones Criminalísticas del Ministerio Público deben aplicar el Manual de Procedimientos para el Procesamiento de Escenas del Crimen, sin perjuicio que cada escena de crimen es única y presenta particularidades especiales” (Ministerio Público, 2006).

Es necesario remarcar que se debe aplicar el referido manual de forma obligatoria al personal del Ministerio Público, sin embargo, este a la fecha carece de la inclusión de protocolos en materia de evidencia digital y electrónica que se ajuste a los estándares internacionales. La instrucción que estamos analizando también refiere que quien inicia la cadena de custodia es el Fiscal a cargo del caso y este es quien debe marcar las directrices a los técnicos para que los indicios sean recolectados en el escenario criminal, es acá donde debemos preguntarnos ¿Qué conocimientos tiene el personal fiscal del Ministerio Publico para el inicio de la cadena de custodia digital? Además, dentro de las directrices finales de la instrucción objeto

de crítica, refiere que los casos no previstos deben ser puestos de conocimiento de la Dirección de Investigaciones Criminalísticas y la secretaria Política Criminal. Es necesario advertir que actualmente el Ministerio Público cuenta con la Unidad UFED que dentro de sus funciones tiene asignada extracción y análisis de información digital en diversos casos y dentro de ellos los relacionados a la Trata de Personas y relacionados a la libertad e indemnidad sexual de las personas, tipos penales regulados en el Título III del Decreto Número 17-73 del Congreso de la República.

b. **Definición de Cadena de Custodia**: Tal y como lo refiere el autor Ismael García Garduza en el Diccionario Jurídico de la tercera edición, debemos entender este concepto como:"…una secuencia de actos llevados a cabo por el Perito, el agente del Ministerio Público o el Juez, mediante la cual los instrumentos del delito, las cosas objeto o producto de él, así como cualquier otra evidencia relacionada con éste, son asegurados, trasladados, analizados y almacenados para evitar que se pierdan, destruyan o alteren y así, dar validez a los medios de prueba" (Garduza).

Indiscutiblemente la forma inicial en que se recolecta y resguarda un indicio es vital para una investigación que reflejará certeza jurídica en virtud que la cadena de custodia asegurara que la forma en que se ha trasladado el indicio ha sido de la forma correcta, integra e incorruptible, consecuentemente al momento que sea sometido a diferentes peritajes no perderá eficacia, es decir, ese control histórico de la persona que ha manipulado el indicio nos dará como resultado una eficacia probatoria siempre y cuando cada Perito Forense Digital o experto haya implementado correctamente los procedimientos atinentes a su materia o rama especializada. Por otro lado, debemos hacer la diferenciación entre el concepto de indicio y evidencia que tienen una íntima relación y es cuestión del momento procedimental que se son objeto de recolección o análisis sabiendo que el primero se refiere al primer acercamiento que se tiene sobre el objeto en el escenario criminal y el segundo es el objeto recolectado que tiene relación o se presume que puede establecer algún extremo de lo acaecido en el escenario criminal. En ese entendido si no se inicia correctamente la cadena de custodia esto pondría en riesgo el valor probatorio de la evidencia incautada o recolectada tomando en consideración que el objeto de la evidencia es que pueda ser utilizada y presentada

ante Juez competente con base a los principios de legalidad, debido proceso, libertad probatoria, entre otros.

Tal y como lo menciona el autor Arístides Arbulora en su obra “La cadena de custodia”, refiere que: “(…) El procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene como fin no viciar el manejo de que ellos se haga y así evitar alteraciones sustituciones, contaminaciones o destrucciones…” (Arbulora Valverde, 2000). Según el criterio de Ricardo Mora y María Dolores Sánchez la cadena de custodia la definen como “el sistema de aseguramiento de la evidencia física compuesto por personas como normas, procedimiento, información, contenedores y lugares, que, al avalar el cumplimiento del principio de mismidad, garantiza la autenticidad de la evidencia que se recolecta y analiza y que se exhibe en la audiencia pública del juicio oral (…)” (Mora Izquierdo & Sánchez Prada, 2007).

Efectivamente se comparte estos criterios sustentados por los autores citados, en el sentido que la cadena de custodia busca evitar que se pueda efectuar cualquier tipo de alteración que reste valor probatorio al objeto que se está analizando para que se preserve la autenticidad e integridad de la evidencia; también podríamos indicar que La cadena de custodia es el procedimiento de control utilizado por el Ministerio Publico para registrar la evidencia encontrada en la escena del crimen que posteriormente se convierten en indicios, estos son registrados en hojas con un formato preestablecido que en forma cronológica lleva el control de las personas que han manejado los indicios desde su localización hasta la valorización por las personas encargadas de su análisis que por lo regular son los peritos. La cadena de custodia tiene por objeto dar certeza jurídica y procedimental al análisis de las evidencias para que no sea viciado, manipulado, alterado, sustituido, contaminado o destruido.

c. **Registro de la cadena de custodia**: Al referirnos a este tema nos circunscribimos específicamente a la forma en que se desarrolla una de las áreas de la criminalística, enfocándonos a ese trabajo de campo que realizan los técnicos de la escena del crimen y es precisamente en este momento en donde es necesario utilizar los formatos respectivos que dentro de su contenido se registra el

correlativo del indicio, nombre y apellidos de las personas que intervendrán en la cadena de custodia, cargo del funcionario, dirección y teléfono y la firma y sello respectivo. Además de la información descrita es menester indicar que en la otra cara del formato se debe registrar la descripción de los objetos o indicios, para el efecto existen formatos prestablecidos y que es encuentran regulados en el Manual de Normas y Procedimientos para el Procesamiento de la Escena del Crimen del Ministerio Público de Guatemala; posteriormente a la recolección de los indicios se traslada a donde sea requerido para practicar los peritajes correspondientes paralelamente la evidencia debe estar embalada correctamente mediante la colocación de los precintos y sellos correspondientes.

d. **Cadena de custodia digital**: Después de abordar algunos puntos sobre la cadena de custodia física o en papel utilizada en la escena del crimen es necesario referirnos ahora a la cadena de custodia digital que tiene algunas similitudes sin embargo tiene características interesantes. Debemos ser conscientes que lo relativo a la Informática Forense es una opción necesaria que coadyuva a la detección y recuperación de la información digital que probablemente se ha encontrado en un escenario criminal. Si nosotros no tenemos claro la importancia que tiene la aplicación de la informática forense en los diferentes procesos judiciales Estamos perdiendo una gran oportunidad de comprobar científicamente los diferentes extremos que pueden esclarecer un caso ante un juez. Sin embargo para nadie es un secreto que los diferentes actores del sector justicia tienen poco o nulo conocimiento sobre esta rama y qué tal como se ha apuntado en otros capítulos el Instituto Nacional de Ciencias Forenses de Guatemala –INACIF- presta el servicio informática forense, sin embargo este queda reducido simplemente al análisis de extracción de información que es remitido por el ente investigador, sin embargo no se tiene a al personal capaz e idóneo para poder actuar en el campo es decir en una escena del crimen, podríamos entonces pensar qué el Ministerio Público es el ente encargado de dotar a sus diferentes unidades de las capacidades necesarias para atender este tipo de necesidades sin embargo debemos apuntar que la Dirección de Investigaciones Criminalísticas

del Ministerio Publico a través de la Unidad de Recolección de Evidencias no tiene la preparación necesaria para obtener y manipular la evidencia digital y electrónica y si hablamos de iniciar correctamente la cadena de custodia digital también veremos que existe una deficiencia gravísima y que si se desea extraer la información está prácticamente estaría viciada desde el inicio. Probablemente el juez sentenciador le da algún tipo de valor probatorio no obstante la evidente presencia de la Teoría del Fruto del Árbol Envenenado, es decir desde el momento que se inicia la cadena de custodia digital en virtud de no aplicarse los procedimientos correctos y apegados a los protocolos internacionales.

Es interesante darle lectura a lo que en su parte conducente refiere el texto “El Rastro Digital del Delito de la Universidad de Fasta” indicando que:

“La Informática Forense demanda de personal entrenado en la materia, que pueda actuar metódicamente, mantener la cadena de custodia y no contaminar la prueba, principios forenses básicos. En la actuación forense o pericia se deben obtener evidencias, a fin de reconstruir la real sucesión de los hechos estudiados. La tarea clave es la correcta recuperación de toda la información posible, tanto visible como oculta, relacionada con el hecho de estudio. A la hora de recuperar la información, el perito informático debe trabajar con diferentes tecnologías, diversos métodos de almacenamiento, tecnologías que naturalmente eliminan evidencias, mecanismos internos de protección de la información, ausencia de herramientas específicas, herramientas que cubren sólo una parte del proceso, diferentes sistemas de criptografía, y otros obstáculos, siempre garantizando un proceso reproducible de adquisición, examinación, análisis, preservación y presentación de la evidencia para que tenga valor probatorio. Dada esta complejidad se requiere de profesionales altamente calificados desde lo técnico y respetuosos de los procedimientos que fijan los códigos procesales para la actuación forense (…)” (Di lorio. et al., pág. 17).

e. **Las Ciencias Forenses en Guatemala y su relación con la cadena de custodia digital**: Dentro de los servicios que ofrece el Instituto Nacional de

Ciencias Forenses de Guatemala como institución auxiliar de la administración de justicia, además de prestar el servicio de investigación científica, que además emite dictámenes técnicos científicos que dotan a la función jurisdiccional, con medios de prueba válidos y fehacientes en los procesos judiciales correspondientes existe el catálogo referente a Informática Forense sin embargo es limitado ya que dentro de su campo de acción se limita a la obtención y análisis de datos que son extraídos de dispositivos electrónicos y medios de almacenamiento de información, esto a requerimiento del Ministerio Público, sin embargo aún no realizan análisis de información de todos los casos sometidos a su conocimiento, específicamente la información que es obtenida *in situ* es decir en el escenario criminal en virtud que es el Ministerio Publico a través de sus diferentes unidades es quien remite la información, situación que es susceptible de una variedad de críticas en virtud de la falta de expertiz, desconocimiento de procedimientos y carencia de calidades técnicas para efectuar este trabajo forense digital. Refiriéndonos nuevamente al Instituto Nacional de Ciencias Forenses –INACIF- es necesario apuntar que, no obstante, los grandes esfuerzos y avances que han tenido sus diferentes unidades de servicio, a la fecha carece de personal que pueda prestar el servicio de análisis de información proveniente de un ataque a un sistema informático, sustracción de evidencia digital y electrónica *in situ*, presentación de informes acorde a los estándares internacionales, gestión y acción de incidentes ante a ataques cibernéticos, entre muchos más. En la administración pública existe otro ente cuyas funciones se encuentra el de analizar la información digital o informática, este ente es la Dirección de Análisis Criminal (DAC) del Ministerio Publico quien realiza funciones de investigación sin embargo por la amplitud de competencia a nivel nacional se encuentra saturado de casos y esto impide una labor objetiva y que cumpla con los postulados de acceso a la justicia, del cual abordaremos ampliamente en otro momento. Hemos hecho mención de los entes que por la naturaleza jurídica de su función debería de proveer de diferentes servicios en materia de auditoria e informática forense digital que no obstante su vigencia y funcionamiento no cubren a la fecha las expectativas o cobertura. Se advierte además que el experto responsable de esto

es el Perito Forense Digital. Existe otro ente de investigación que es la Unidad de Cibercrimen de la Policía Nacional Civil, cuyas funciones se relacionan, entre otros, a casos relacionados a Trata de Personas, pornografía infantil, secuestros, lavado de dinero, etcétera, sin embargo, su competencia también es muy limitada para atender casos en general sobre análisis forense digital por la cantidad de integrantes.

5.2. El escenario criminal.

Cuando se inicia el abordaje de la investigación de campo, uno de los primeros momentos esenciales para cursar eficazmente es trabajar adecuadamente el escenario criminal o escena del crimen. Regularmente un escenario criminal puede ser catalogado como un escenario principal o secundario, abierto o cerrado y que está limitada y caracterizada por diferentes aspectos tales como espacio físico, suelo, ubicación de indicios. Además, es importante señalar que cuando se procesa una escena del crimen podemos encontrarnos con diferentes obstáculos que deben ser superados para decir que se está procesando una escena criminal utilizando los diferentes protocolos y técnicas en forma adecuada. Recordemos que el objeto del procesamiento del escenario criminal es dar la certeza y legalidad a los indicios que son encontrados a efecto de evitar cualquier tipo de manipulación, contaminación o perdida, es decir se busca que la evidencia produzca plenos efectos jurídicos y que se respaldara mediante el cotejo de la cadena de custodia.

Además del tipo de escenas descritas, se advierte que existen escenarios criminales complejos es decir son mixtas. Nos hemos referido a detallar algunos extremos de la evidencia física y esto lo debemos transcribir a la evidencia electrónica y digital. Visualicemos que en un escenario criminal podríamos encontrar diferentes dispositivos electrónicos que podrían tener información útil para la resolución de un caso como por ejemplo teléfonos celulares, computadoras, memorias de almacenamiento, discos compactos, etc. Es acá en donde deben prevalecer algunos principios básicos de la Criminalística y un aspecto interesante es el acordonamiento del escenario criminal.

Si se utilizan los procedimientos comunes a efecto de salvaguardar los indicios que se encuentran en el escenario criminal en donde existen dispositivos electrónicos corremos el riesgo de que la evidencia pierda toda fuerza probatoria y desde el inicio la cadena de custodia y el embalaje estén viciados por un mal procedimiento. Un ejemplo común es cuando en un allanamiento se encuentran computadoras o teléfonos celulares, el procedimiento de curso normal sería el de revisar cada dispositivo manipulándolo o simplemente apagarlo para su posterior embalaje, sin embargo, de conformidad a protocolos internacionales el ejecutar esta práctica ocasionaría que contaminemos la evidencia digital y perdamos información valiosa, aspectos que más adelante podremos analizar detenidamente.

5.3. La Evidencia

Debemos reflexionar sobre la creciente demanda tecnológica que día a día se refleja en el mundo globalizado y el área del Derecho no escapa a esa influencia e imperiosa necesidad de estar actualizados. El flujo de información se incrementa y los usuarios y administradores de base de datos son más cada día. Esta información que se manipula con diferentes fines siempre deja un rastro de inicio, direccionamiento y finalización de la información y consecuentemente puede poner en evidencia la comisión de un hecho delictivo siendo acá la brecha en donde el Derecho Penal se conecta con la informática forense siendo esto equivalente al conocimiento *sine qua non* sobre temas de almacenamiento de datos; obtención, recolección, análisis de información, tratamiento de la evidencia digital y electrónica, entre muchos temas más que nos da la Informática Forense y el Derecho Informático.

Como lo indicamos anteriormente, la evidencia debe ser procesada en forma adecuada con el fin de que su recolección este revestida de todos los principios lógicos del peritaje como es la intangibilidad, certeza y continuidad, sin embargo, cuando se ven inmersa la tecnología se debe considerar que para que una prueba electrónica y digital sea válida ante un juez (ámbito público) o sea reproducible ante el cuerpo directivo de una empresa (ámbito privado) que pueda evidenciar un fraude, independientemente del ámbito, es necesario definir lo que es la evidencia digital física

y para ello citaremos a Laura Casado quien indica que la evidencia debe ser “certeza clara, manifiesta y tan perceptible que nadie racionalmente puede dudar de ello” (Casado, 2008).

También tomaremos en cuenta lo que menciona el autor Carlos Guzmán refiriendo que cuando

“se exploran los objetivos principales de la investigación en el escenario del delito, las áreas de importancia pueden resumirse de la siguiente manera: colección o acopio de la evidencia física, reconstrucción del hecho, identificación y eslabonamiento del sujeto con el escenario del suceso y establecimiento de la causa probable de arresto. En la persecución de, tales objetivos, el área policial encargada de la colección, preservación y documentación de la evidencia, así como de la investigación en el lugar del hecho, ha descubierto en ello un arte. Con el propósito de desarrollar una comprensión del rol prominente que juega la evidencia física en el entorno legal contemporáneo, una evolución perspectiva es una necesidad. Básicamente hay tres caminos principales, disponibles para coadyuvar en la solución de un hecho: confesión del sujeto, manifestaciones de una víctima o testigos, y la información obtenida a través de la evidencia física” (Guzman, 2000).

Tomando en consideración las dos connotaciones de los autores citados podemos inferir que debemos llamarle evidencia física a todo elemento visible o que mediante ciertas técnicas o métodos podemos palpar y observar en un escenario criminal toda vez que resulta un elemento pasivo que puede demostrar algún extremo de lo acaecido en el lugar del hecho es decir el elemento puede formar parte de un todo para dar explicación y dar respuesta a una hipótesis y con ello coadyuvar a establecer la verdad histórica del hecho. Resulta importante el valor que se le provee a una evidencia en virtud que ella se puede reflejar la seguridad y certeza jurídica que aportar a un juicio y que se perfecciona al momento que se comprueba la hipótesis acusatoria o de defensa según corresponda es decir que la evidencia evoluciona en el desarrollo del proceso ya que el objeto es que materialmente se transforme en una

prueba legal, útil y necesaria. Después de conceptualizar lo referente a la evidencia física, es menester enfocarnos al conocimiento de la evidencia electrónica.

5.4. La Evidencia Electrónica y Digital.

A. Evidencia Electrónica y Digital: Como hemos apuntado en líneas anteriores el uso de la tecnología en los diferentes campos del conocimiento ha obligado a las diferentes ciencias a ampliar su campo de conocimiento y a la creación de nuevas metodologías y prácticas que puedan responder a diferentes necesidades. En el área forense es menester apuntar que la evidencia física, electrónica y digital tiene matices similares y que es necesario conocer cuáles son esas similitudes y las variaciones a efecto que los sujetos procesales puedan abordarlo y manejarlo en forma práctica y ajustada a Derecho, esto se transcribe en una nueva herramienta para conocer la verdad histórica de los hechos en el entendido que este campo es muy amplio y complejo tomando en consideración que se deben tener ciertos conocimientos técnicos para que en verdad se le pueda dar una valoración ajustada a la realidad y no crear apreciaciones subjetivas que lo único que ocasionaría es la desacreditación de tales evidencias.

Según lo refiere el autor Yuri López en su libro “Computación Forense” emite opinión, indicando que:

“…para la obtención de evidencia hay que estar relacionado con los diferentes medios de almacenamiento y su funcionamiento. Si se dio un delito o hay la sospecha del mismo, existen muchos medios por los cuales el delincuente pueda esconder o mover los datos y las pistas, desde un medio de almacenamiento como puede ser su computadora a un medio portátil de almacenamiento. La lista incluye memorias flash que son tan pequeñas que pueden ser llevadas en la bolsa de una prenda de vestir o la palma de la mano, también pueden ser disfrazadas como plumas, relojes digitales, cámaras digitales, chips de memoria para cámaras digitales y estos pueden ser escondidos en un sobre, PDA’s y teléfonos celulares, estos últimos pueden almacenar una variedad de información tal como

mensajes de voz, mensajes de texto, notas en archivos almacenados, números…" (López Manrique, 2007).

El autor refiere que existe una gran diversidad de medios a través de los cuales se puede almacenar y movilizar la información, sin embargo, se debe hacer la inferencia que hace alusión a la evidencia electrónica y digital y en ese orden ideas la primera es tangible y la segunda intangible.

Según lo refiere el autor Daniel Bechimol en su texto "La Hacking desde cero" la evidencia digital, específicamente, es un tipo de prueba física, menos tangible que otras formas de evidencia (ADN, huellas digitales, componentes de computadoras, papeles). Tiene algunas ventajas sobre su contraparte no digital porque, por ejemplo, puede ser duplicada de manera exacta, es posible detectar si ha sido alterada y, aun si es borrada, a veces recuperarla. Esto se resume en: repetible, recuperable, redundante e integra" (Bechimol, 2011).

Estoy de acuerdo en lo que explica el autor citado en virtud que existen ventajas para obtener el rastro digital no obstante ser poco tangible, sin embargo, existen técnicas y procedimientos para obtener la evidencia digital en forma íntegra, es decir, es susceptible de ser manipulable y examinada en forma adecuada. Un aspecto relevante es que la evidencia electrónica y digital si bien es cierto que puede examinarse de forma accesible también lo es que puede ser alterada y modificada sin intención en virtud que existen diferentes protocolos y buenas prácticas que deben implementarse para recolectar y obtener la información tomando en consideración que la información es volátil y puede perderse con facilidad o en su caso puede ser cambiada y sufrir cambios significativos que causen la contaminación de la evidencia. En ese orden de ideas debemos advertir que en este plano la función del Perito Forense Digital es de vital importancia en virtud que debe embalarse e iniciar la cadena de custodia digital de conformidad a los protocolos que más adelante explicaremos, sin olvidar que además debe ir acompañada de una cadena de custodia física, todo esto para resguardar la información en forma correcta.

Llama la atención la explicación que hace José Daniel Ruiz Alquijay en su texto -La utilización de la informática forense en los casos de alto impacto social en Guatemala- sobre la evidencia digital indicando que: “La evidencia digital es cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático. En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal” (Ruiz Alquijay, 2012).

En ese orden de ideas podemos extraer que compartimos su razonamiento y es que para que pueda llamarse evidencia digital esta debe extraerse de un medio de almacenamiento de información y que no siempre se efectuará de un equipo de cómputo, es necesario indicar que desde el análisis hasta la extracción de la información debe seguir un procedimiento determinados a efecto que pueda ser repetible en forma sistemática es decir sometida al principio del contradictorio.

Según la obra Evidencia Digital de Raisa Vides Álvarez quien cita a Brungs Jameison, las características de la evidencia digital son las siguientes:

a) Es volátil: Ya que por su estructura, programación y contenido es capaz de cambiar o variar con facilidad y de forma poco previsible; esto implica cambios en su denominación, descripción, detalles, autores y sobre todo en los datos que pudieron haber sido herramientas en la comisión de un delito.

b) Es anónima: Identificar al autor de un delito informático por ejemplo implica una compleja red de conocimientos especializados y utilización de la lógica informática ya que la evidencia digital en su forma originaria, es decir, datos o información digital puede sufrir denominaciones ilimitadas por lo que no necesariamente algunos detalles de su contenido refieren con plena certeza a autor de dicha información; por lo que al momento de su recolección debe considerarse anónima ya que resulta en términos sencillos imposible determinar la autoría a simple inspección de una evidencia digital. Esto se puede extender a la suplantación de

información o datos de forma remota, derivado de la capacidad de administrar un dispositivo de manera anónima y a una distancia considerable; por ejemplo: las instituciones tienen un departamento de mantenimiento de sistemas que tiene acceso remoto a los distintos computadores, lo cual permite la manipulación de software, datos, información y contenido media por parte de un tercero.

c) Es duplicable: Como refiere Brungs y Jameison la evidencia digital es susceptible de duplicarse de forma idéntica que el archivo original, lo que dificulta muchas veces individualizar de forma objetiva su origen; ya que, aunque esta permanezca almacenada por ejemplo un documento digital sujeto a evidencia en un dispositivo USB, necesito de un dispositivo con capacidad para procesar texto lo que implica que su origen es desconocido y su autor anónimo.

d) Es alterable y modificable: Esta característica se deriva de la fragilidad de la evidencia digital ya que por su naturaleza y ausencia de tangibilidad es susceptible a ser modificable en cualquier momento, inclusive como previamente se indicó durante la cadena de custodia y análisis de la evidencia digital existe un riesgo de que la evidencia digital se altere de forma sustancial; lo que genera un complejo campo de peritaje informático en el cual los conocimientos especializados desempeñan un rol importante para la preservación, resguardo y garantía de la cadena de custodia sobre la evidencia digital.

e) Es eliminable: Una de los obstáculos que se presentan respecto a la evidencia digital es la facilidad con la que esta puede ser suprimida, hay mecanismos informáticos y herramientas que con el conocimiento necesario permiten ataques de forma remota a servidores y redes informáticas que no cuentan con la seguridad necesaria para contrarrestarlos, lo que infiere directamente en la alteración o supresión de la evidencia digital en su momento, por lo que esta debe seguir rigurosos controles de seguridad para evitar su perdida durante la cadena de

custodia ya que esto implicaría un daño directo a una tesis acusatoria por parte del ente investigador. (Vides Alvarez, 2011).

No se debe dejar al margen otras particularidades de la evidencia digital que es el acceso objetivo a la transferencia de información es decir la huella o rastro digital que es una particularidad que atiende al principio de Locard que explica la veracidad de un intercambio de materiales físicos, por el que el criminal deja evidencias en la escena y toma elementos de esta misma y que lleva para sí.

B. Clasificación de la evidencia digital: Según lo refiere que Harley Kozushko citado por Almeida Romo, menciona que "la evidencia digital se puede clasificar, comparar, e individualizar, es decir es el proceso por el cual se buscan características generales de archivos y datos, características que diferencian evidencia similar y que deben ser utilizadas a criterio del investigador, por ejemplo:

a) Contenido: Un e-mail, por ejemplo, puede ser clasificado por su contenido como SPAM, y puede ser individualizado a partir del contenido de sus encabezados, información que por lo general no es visible para el usuario. Por ejemplo, por su dirección de origen.
b) Función: El investigador puede examinar cómo funciona un programa para clasificarlo y algunas veces individualizarlo. Por ejemplo, un programa que inesperadamente transfiere información valiosa desde un computador confiable a una locación remota podría ser clasificado como un caballo de Troya y puede ser individualizado por la localización remota a la que transfiere la información.
c) Características: los nombres de archivo, extensiones e inclusive los encabezados internos que identifican los diferentes formatos de archivo que existen pueden ser de utilidad en la clasificación de la evidencia digital" (Almeida Romo, 2011)

Asimismo, Gómez Manrique refiere que la evidencia digital es posible dividirla en tres categorías: a) "Registros almacenados en el equipo de tecnología informática

(correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.). b) Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.). c) Registros que parcialmente ha sido generados y almacenados en los equipos de tecnología informática. (Gómez Manrique, 2014)

Es necesario también apuntar que para poder clasificar la evidencia digital también se debe considerar que en un escenario criminal puede haber una gran cantidad de dispositivos electrónicos lo cual implica que la cantidad de reactivos será más extensa además la información que pudiera encontrarse debe advertirse que no corresponderán a un mismo formato por ejemplo podría encontrar información con extensiones de archivos de música, fotografías o imágenes, archivos comprimidos, archivo de texto, vídeo, etcétera. Que la información muchas veces no está en forma aislada sino que podría encontrarse en carpetas cuyo contenido podría estar cifrado es decir como un algoritmo que impida el acceso en forma directa teniendo que insertar alguna clave o contraseña para su apertura; otros ejemplo es cuando se efectúa un allanamiento por el ente investigador en oficinas contables o dependencias que manejan información amplia sobre registros financieros bancarios obviamente la cantidad de información será voluminosa.

La evidencia digital como se ha reiterado en varias ocasiones es muy importante para el esclarecimiento de los hechos que se están investigando y ahora resulta necesario que se incluya y maneje una forma correcta en una investigación criminal toda vez de que si se cumplen todos los protocolos internacionales en el correcto manejo de la evidencia digital y electrónica entonces sí podríamos hablar de una seguridad y certeza jurídica la cual tomará al juzgador para darle un valor probatorio. Puedo citar ejemplos referente a qué tipo de entidades de gobierno en Guatemala manejan evidencias digitales para realizar sus investigaciones, tal es el caso de la Superintendencia de Bancos a través de la Intendencia de Verificación Especial –IVE- que a diario determina el rastro digital sobre transacciones sospechosas en materia bancaria y para ello es necesario tener las herramientas adecuadas para que al momento de rendir su informe a través del Reporte de Transacción Sospechosa –RTS-

se pueda efectivamente concluir si existe o no alguna anomalía que sea susceptible de perseguir e investigar por parte del Ministerio Público. Debemos de considerar que la evidencia digital es fundamental para una investigación criminal toda vez que se hace imprescindible en investigaciones en donde es necesario analizar transacciones financieras, correos electrónicos, documentos digitales, análisis de mensajes de texto, flujo intercomunicacional, entre muchos más; todo esto se transcribe en evidencia digital.

De la lectura de este subtema podemos inferir que la clasificación es diversa y nos permite hacer una clasificación de conformidad a la naturaleza del dispositivo electrónico, uso, volatilidad, entre otros; además me permito hacer la siguiente clasificación que surge de la inferencia de la lectura hecha: 1) Evidencia digital de registros internos del sistema que opera el dispositivo electrónico. 2) Evidencia digital derivada de datos que almacena el usuario del dispositivo electrónico. 3) Registros mixtos causados por procesos internos del dispositivo electrónico y otros procesos originados de la intervención humana.

C. Definición de evidencia electrónica y digital. Al intentar definir la evidencia digital podemos mencionar que son datos digitales que se encuentran almacenados o han sido transmitidos mediante equipos informáticos. Los ordenadores registran toda la actividad que se realiza. Estos registros o logs son fundamentales en las investigaciones informáticas, siempre que se pueda comprobar que no han sido manipulados.

Según la consulta efectuada en fuentes abiertas se define también así: “Los e-logs o evidencias electrónicas pueden ser recolectadas por medio de técnicas especializadas por un perito en una investigación informática, por ejemplo. Es decir, tienen la función de servir como prueba física, ya que se encuentran dentro de un soporte, de carácter intangible (no modificable). (Evidencias electronicas, 2020)

Debemos apuntar que la *evidencia electrónica se refiere a los dispositivos electrónicos que podemos encontrar en un escenario criminal mientras la evidencia*

digital es la información encontrada en los dispositivos electrónicos tales como archivos, logs del sistema, entre otros.

Es necesario mencionar que en una escena del crimen digital podrían recolectarse diferentes evidencias electrónicas y digitales, para el efecto existen protocolos que deben de agotarse para obtener esta evidencia y es que dentro del ámbito forense digital se maneja el término de una firma digital, o Hash que no son más que algoritmos que crean una serie alfanumérica que impregna de certeza e integridad a un archivo determinado es decir crea una serie de números y letras que garantizan que un archivo no ha sido modificado dando esto el primer paso para referirnos a una certeza jurídica digital.

En fuentes abiertas se obtiene la siguiente contextualización sobre el término Hash:

"…una función hash es método para generar claves o llaves que representen de manera unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud, y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original. El contenido es ilegible… Es posible que existan huellas digitales iguales para objetos diferentes, porque una función hash tiene un número de bits definido. En el caso del SHA-1, tiene 160bits, y los posibles objetos a resumir no tienen un tamaño límite. A partir de un hash o huella digital, no podemos recuperar el conjunto de datos originales. Los más conocidos son el MD5 y el SHA-1…cifrar una huella digital se conoce como firma digital." (genbetadev, 2020).

Es necesario conocer un poco sobre la forma en que se utiliza el *Hash* en entornos digitales, por ello se efectuó una consulta en fuentes abiertas referente a un Hash MD5, estableciendo que:

MD5: Su abreviatura (Message-Digest Algoritmo 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. Uno de sus usos es el

de comprobar que algún archivo no haya sido modificado, nos dirá con certeza si el software que acabamos de descargar es el oficial o ha sufrido algún cambio con respecto a éste y puede resultar peligroso para nuestro sistema. Es un algoritmo que proporciona un código asociado a un archivo o un texto concretos…el código generado por el algoritmo, también llamado hash, viene "unido" al archivo…Para que nosotros podamos ver este código MD5, existe software que analiza el archivo descargado y obtiene dicho código de él. Con el hash de nuestra descarga, podemos acudir a la web del desarrollador del programa del que tenemos el instalador y buscar el código MD5 de su instalador original. Una vez tengamos disponibles los dos códigos MD5, el de nuestro archivo descargado y el del instalador o software de la web oficial del desarrollador, podremos comparar ambos y ver si coinciden y nuestro archivo es fiable o no. (genbetadev, 2020).

Como podemos darnos cuenta el hash prácticamente nos da la certeza de la integridad de un archivo consecuentemente también aplicable para la evidencia digital en virtud que existen herramientas de comparación que nos permiten verificar si hay coincidencia o no en la firma digital o mediante la lectura del hash. La utilidad que podemos darle al algoritmo MD5 es la de poder comprobar que un texto no haya sido modificado y haya podido llegar de forma distinta a como era de forma original. Los datos digitales que se han recopilado de un escenario criminal deben conservarse en original y de éstos obtener copias que no deben alterarse a efecto de no invalidar la evidencia, es por ello que se recomienda que los expertos en pericias forenses digitales revisen que sus copias sean idénticas a las de la evidencia original y para ello se utiliza la verificación mediante un checksum o verificación de datos, así también los MD5.

D. Diferencia entre MD5, Evidencia Digital y documentación de evidencia: Tenemos que indicar que la evidencia digital se refiere a todos los datos que se pueden ubicar en la escena del crimen y que nos puedan dan indicios que coadyuven a descubrir la verdad histórica del hecho y el vínculo causal que existió entre la víctima y autor del crimen y para ello se documenta la evidencia en cadenas de custodia en donde se hace constar que la misma ha sido embalada previamente

por el ente fiscal; seguidamente se utiliza un descriptor con EL ALGORITIMO MD5 para comprobar que la evidencia incautada no haya sido modificada después de su análisis, en síntesis el primero se refiere a la evidencia encontrada, la segunda es la forma de documentarla y la tercera es la herramienta tecnológica que provee de certeza jurídica que no ha sido modificada de su original.

La evidencia electrónica que se encuentra en el escenario criminal debe estar **resguardada** en embalaje acorde a las características propias de los objetos para ello es necesario mencionar las **Bolsas y cajas de Faraday** que son elaboradas para la recolección, preservación, traslado y análisis de dispositivos electrónicos que tiene la capacidad de aislar la energía electroestática, son como un blindaje para teléfonos celulares, GPS, laptops, entre otros que provoca el bloqueo de toda señal celular wifi o de radio, estando dentro de esta bolsa no se puede conectar a la red aunque se encuentre encendido lo cual da una certeza jurídica ya que dichos dispositivos no pueden ser controlados, localizados o bloqueados en forma remota.

Cuadro comparativo de evidencia física, electrónica y digital		
FISICA	**ELECTRONICA**	**DIGITAL**
Es visible o tangible	Es visible o tangible	Intangible
Es capaz de ser percibida mediante los sentidos	Es capaz de ser percibida mediante el tacto y vista	No es percibida a simple vista mediante los sentidos. Está conformada por pulsos electromagnéticos o binarios
La recolección toma como guía el Manual de Normas y Procedimientos para el Procesamiento de Escena del Crimen del Ministerio Publico	La recolección de evidencia debe basarse en la norma ISO/IEC 27037:2012	Inició con la Guía RFC 3227 y actualmente La recolección de evidencia debe basarse en norma ISO/IEC 27037:2012
Puede o no utilizarse medios tecnológicos.	Se deben utilizar herramientas de análisis forenses digital (Software y Hardware)	Se deben utilizar herramientas de análisis forenses digital (Software y Hardware)
El tratamiento de la evidencia debe remitirse a varios laboratorios criminalísticos para el análisis según corresponda corriendo el riesgo de su modificación, manipulación o perdida	Se deben seguir los protocolos internacionales según corresponda y se garantiza la identidad y seguridad de la evidencia, aunado a ello se maneja una cadena de custodia física y digital.	Se deben seguir los protocolos internacionales según corresponda y se garantiza la identidad y seguridad de la evidencia, aunado a ello se maneja una cadena de custodia física y digital
No se puede duplicar para su análisis, debe de realizarse sobre el objeto material	Se pueden realizar un análisis forense in situ y extraer la información necesaria según el caso en particular. Es necesario utilizar bolsas, envoltorios o cajas con la tecnología Faraday, lo cual evita ataques externos.	Se realiza una imagen forense digital para su análisis, el original se embala con su respectiva cadena de custodia y el análisis se basa en la imagen forense la cual es integra y fiel a su original
Fuente: Investigador / Autor de esta tesis.		

En la comparación que se presenta se puede inferir que la evidencia electrónica digital debe de dársele un tratamiento diferente a la evidencia física ya que la forma de diligenciar y ofrecerla también toma otro matiz en virtud que el Perito Forense Digital

juega un papel muy importante ya que él es el experto que podrá individualizar y explicar el contenido de la evidencia electrónica y digital, proceso que resultaría complejo para los sujetos que intervengan en el proceso ya que un Perito del Instituto Nacional de Ciencias Forenses con expertiz en otras áreas (sangre, tejido capilar, entre otros) no tendría la capacidad de sostener un informe técnico o ejecutivo que contenga datos del peritaje forense digital realizado.

El proceso de recolección y análisis forense de la evidencia digital según lo menciona Cano Martínez en su obra “El Peritaje informático y la evidencia digital en Colombia” refiere que:

> “está diseñado según las propias necesidades que presenta la investigación criminal, se plantea como ejemplo se plantea el procedimiento estandarizado diseñado en el Reino Unido con la finalidad de superar los diversos problemas que plantea la manipulación de la evidencia digital. Como primer paso se plantea el procedimiento de la búsqueda, reconocimiento, recolección y documentación de la evidencia electrónica esto con el fin de identificar que medios se utilizaron para la materialización de un hecho delictivo y establecer la primera línea de investigación, es importante mencionar que en los casos de delitos informáticos se le puede denominar herramientas primarias ya que sin estas es imposible la comisión del delito, mientras que en otras manifestaciones del delito hay herramientas de tecnología que son auxiliares y por ello se les podría denominar secundarias ya que el resultado del delito no depende en mayor medida de la implementación de la misma y solamente generan una proximidad para la consecución del hecho delictivo. Plantea, como segundo paso o etapa el examen de la evidencia el cual contribuye a explicar el origen y a individualizar la evidencia trazando una línea criminal respecto al alcance de la misma. Esto implica la documentación del contenido y el estado de la evidencia digital en su conjunto con la finalidad de separar la evidencia útil de la demás que coexiste en la misma unidad de almacenamiento. Seguidamente se

debe concurrir a la fase de análisis y consiste básicamente en inspeccionar con las herramientas informáticas la utilidad de la evidencia digital obtenida, en este punto se indaga sobre el valor probatorio de la evidencia recabada y sobre todo la pertinencia de la misma al momento de introducirla al proceso penal. Por último, en el Reino Unido se requiere el reporte o declaración del perito el cual debe contener la información relativa al proceso que se implementó para analizar la evidencia digital y el resultado del análisis, haciendo énfasis en que las notas del forense en informática deben ser preservadas para efectos testimoniales. En este sentido, esta aproximación al procedimiento de recolección y aseguramiento de la evidencia digital en el Reino Unido sigue un procedimiento estandarizado con el fin de superar los problemas que presenta, circunstancia que se asocia de forma breve con otros países." (Cano J. J., 2010)

E. Aspectos básicos para la adquisición de la evidencia electrónica y digital. El Ministerio público es el ente encargado de recolectar y obtener la evidencia en el escenario criminal y debemos de advertir que desde acá reviste de vital importancia la correcta aplicación de los procedimientos y protocolos para la recolección y preservación de la evidencia digital y electrónica. Encontramos entonces qué cuándo se investiga la comisión de un hecho ilícito las diligencias de investigación de campo son fundamentales. En el artículo 187 del Código Procesal Penal se establece lo referente a la inspección y registro de lugares, cosas y personas cuyo objetivo es encontrar rastros y otros efectos materiales que pueden útiles para la averiguación del hecho y para encontrar a los responsables de la comisión del ilícito. El Ministerio Público realiza diferentes diligencias de investigación una de ellas es el allanamiento y por lo regular lleva implícita la inspección, registro y secuestro de indicios y es acá la importancia de aplicar procedimientos correctos para la recolección de la evidencia electrónica y digital, se advierte que estas diligencias no son un medio de investigación y prueba sino que son medios auxiliares para que el Ministerio Público obtenga medios de investigación y convicción que más adelante serán

medios probatorios. Específicamente en este apartado nos referiremos a la importancia de la diligencia de secuestro que de conformidad al decreto número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal, se encuentra regulado a partir de los artículos 198 al 203, la cual se realiza con previa autorización judicial. Se sobreentiende entonces qué el manejo de la evidencia digital en un escenario criminal previamente debe estar autorizado por un juez competente de lo contrario sería ilegal e ilegítima la evidencia obtenida.

Para efectos de nuestro estudio debemos puntualizar entonces que la **evidencia electrónica y digital es el punto central de la informática forense** toda vez que se centra en la búsqueda de la información o datos necesarios para detallar y encontrar la huella o rastro digital del delito además que nos dará diferentes elementos que nos ayudarán a encontrar información ya sea para dirigir o encaminar la investigación para esclarecer el hecho investigado o por sí mismo tendrá la información necesaria para conocer la verdad histórica del hecho.

En la práctica actual en Ministerio Público cuando tiene la necesidad de secuestrar dispositivos electrónicos para su posterior investigación se estima que no aplican los procedimientos correctos toda vez que manipulan el escenario criminal es una forma mixta, es decir, aplicar los mismos procedimientos para recolectar e incautar la evidencia física de cosas u objetos y así mismo para la evidencia electrónica y digital. Actualmente existe una Unidad de Asistencia Técnica -UAT- que pertenece a la Dirección de Investigaciones Criminalísticas del Ministerio Público cuya función es brindar un servicio de extracción de dispositivos electrónicos es decir teléfonos celulares, con computadoras, discos duros externos, análisis de videos, entre otras y que a lo interno está organizado en diferentes unidades qué tratan de brindar este servicio para apoyar la labor investigativa del Ministerio Público sin embargo a la fecha no tienen un procedimiento establecido y de aplicación para el manejo de la evidencia digital y electrónica.

Un criminalista que trabaja con evidencia digital y electrónica debe tener la expertiz necesaria, más adelante hablaremos sobre el profesional idóneo. A

continuación, sugiero algunos elementos para elaborar un protocolo de manejo de evidencia electrónica y digital siendo estos:

a) Creación de un hallazgo o cadena de custodia. Que sirve para llevar un control de quienes han manejado la evidencia digital y electrónica a lo largo del tiempo o en forma histórica.

b) Discriminación entre evidencia digital y evidencia electrónica. Se debe diferenciar a efecto de aplicar un procedimiento determinado. Por ejemplo, si fuera una computadora portátil se debe observar si es un equipo encendido o apagado y en su caso saber si se debe crear una imagen forense de información. Otro caso es obtener la información volátil del computador para ello se debe conocer la herramienta forense a efecto de obtenerla para no correr el riesgo de perderla.

c) Determinación del sistema operativo de los equipos. Se enfoca específicamente a dispositivos móviles y computadoras en donde se debe emplear la herramienta forense útil que ayude a extraer la información del sistema operativo en cuestión. Por ejemplo, Linux, Windows, Ubuntu, Unix, Fedora, Solaris, Mac, entre otros. En el caso de los teléfonos celulares o tabletas electrónicas el sistema operativo que utilizan es diverso y por ende se debe emplear el software que nos aporte los elementos necesarios para la investigación; existen sistemas tales como Android, Windows 10 mobile, BlackBerry OS, Ubuntu Touch, IOS, HarmonyOS, YunOS, entre otros.

d) Recuperación de archivos. Un reto que se tiene es aplicar procedimientos correctos para recuperar archivos que han sido borrados en forma maliciosa o sin intención. Recuperar archivos es una tarea ardua en virtud que en algunas ocasiones no se podrá recuperar la totalidad de información.

5.5. Principios del Peritaje Informático.

Existen principios universales que nos orientan para conocer los bases sobre las cuales debe encausarse un análisis científico. En este apuntaremos los principios que se deben considerar en la práctica del peritaje informático, siendo los siguientes:

a) Objetividad: Este se encuentra plasmado en el artículo 108 del Código Procesal Penal debiendo ser observaron en la función del Ministerio Público como ente encargado de la persecución penal en ese sentido la recolección de evidencia digital y la conformación de una cadena de custodia digital debe estar revestida de imparcialidad por parte del Perito Forense Digital de conformidad a los postulados de la ética, evitando así la alteración culposa y dolosa de la información digital lo que influiría significativamente en el resultado del proceso penal.

b) Autenticidad: este principio persigue determinar la autenticidad de la información digital, en virtud de que la evidencia digital es fácilmente duplicable y es necesario aplicar el procedimiento o protocolo útil para determinar si es el archivo original o es un duplicado. Advertimos que la hora y fecha son trascendentales para identificar cualquier alteración o modificación de la información.

c) Legalidad: está íntimamente ligado con el desarrollo de la investigación criminal, en este caso el perito forense digital debe cumplir postulados exigidos por la ley para obtener información, datos, archivos, registros y software para su investigación, esto en un escenario ideal en virtud que como se dijo ya con anterioridad el personal de la Dirección de Investigaciones Criminalísticas del Ministerio Público–DICRI- es quien recolecta la evidencia en general en un escenario criminal, se debe considerar que atender este último podría ser por una diligencia de allanamiento, inspección, registro y secuestro de evidencia o en su defecto por atención de un caso en donde es llamado el Ministerio Público para iniciar la investigación penal a raíz de una querella, denuncia o flagrancia manifiesta.

d) Idoneidad: se refiere a que la investigación criminal se lleve a cabo con las condiciones necesarias para demostrar la forma de la comisión de un ilícito, a efecto que pueda tener como resultado la observancia de los aspectos relevantes y suficientes para el caso.

e) Autenticidad, conservación e integridad. Desde el inicio de la cadena de custodia digital hasta la presentación de los medios de prueba digital ante juez competente debe de darse estricto cumplimiento a la integridad de los medios probatorios aplicando los protocolos y procedimientos prestablecidos, es decir se debe garantizar la inalterabilidad e incorruptibilidad de la evidencia recolectada.

f) Documentación: Tal como lo refiere Luis Escobar en su texto Manejo de la cadena de custodia en la recolección de la evidencia digital,

> "los indicios digitales y la evidencia que sea originada en dispositivos de tecnología que va ser sometida a investigación criminal debe ser documentada y debe ser descrita de forma íntegra especialmente reuniendo la información de fecha y hora de creación, ya que esta información en su momento puede indicar si esta fue alterada o no lo que implicaría un giro totalmente distinto en el ejercicio de la actividad punitiva y la investigación criminal, esto conlleva la descripción integra de los pasos que se han desarrollado para la recolección y manejo de la cadena de custodia incluyendo los sujetos que han intervenido en la misma". (Escobar, 2017)

Derivado de la lectura de este subtema defino "El Análisis Forense Digital" como el conjunto de técnicas y métodos científicos tecnológicos y criminalísticas que permiten la extracción de información de diferentes dispositivos y equipos tecnológicos con el objeto de identificar, preservar, analizar y presentar la información encontrada para que se utilizada en un proceso judicial o procedimiento administrativo en el sector privado. Cuando se realiza un análisis forense sobre diferentes dispositivos electrónicos o se analizan los datos que en ellos se encuentran se podrá encontrar información diversa sobre los incidentes de seguridad, ilícitos o cualquier rastro que del acto criminal que sea objeto de investigación.

CAPITULO VI

Metodología y Protocolos utilizados en Informática Forense.

6.1 Protocolos para el tratamiento de la evidencia electrónica y digital.

Con el avance de la tecnología también lleva en forma paralela la generación de contenido e información y si ésta se analiza como evidencia electrónica y digital también nos encontraremos con que se los protocolos para manejar la referida evidencia se vuelve más estructural e íntegra, consecuentemente no cualquier persona es apta para abordarla, y por eso que los expertos o también llamados Peritos Forenses Digitales, Peritos Informáticos o Peritos Digitales deben conocer a profundidad los protocolos específicos para el manejo de la evidencia electrónica y digital.

Surge entonces la necesidad de elaborar guías de recomendaciones y buenas prácticas que orientaran a los profesionales en las tareas a realizar, con el fin de evitar la contaminación de la evidencia electrónica y digital, es decir, la alteración del original y preservar esta información como prueba. Diversas instituciones a nivel internacional han propuesto a través de los años guías de recomendaciones y buenas prácticas, e incluso, protocolos de actuación específicos para ciertos casos, recordando que la evidencia digital tiene características diferentes y responde a un paradigma distinto que la evidencia física

A continuación, presentaremos los protocolos pertinentes y específicos que se utilizan en el “Análisis Forense Digital” correspondientes a la Informática Forense y más adelante haremos la propuesta concreta de la forma en que puede implementarse en Guatemala tomando en cuenta la legislación actual y sin que se vulneren derechos fundamentales de las personas. Siendo las siguientes directrices:

A. **RFC "Request For Comments" 3227, denominado "Guía para recolectar y archivar evidencia" (IETF-ISOC, 2002).** Tal y como lo podemos encontrar en el sitio web: "http://www.ietf.org/rfc/rfc3227.txt" este documento refiere que fue escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir qué recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal. Su estructura es la siguiente:

a) Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.
b) El proceso de recolección: transparencia y pasos de recolección
c) El proceso de archivo: la cadena de custodia y donde y como archivar que es uno de los primeros en ser adoptados por la comunidad de informática forense, es una guía general para recolectar y almacenar información relacionada con incidentes. (Killalea)

Propone una serie de buenas prácticas para determinar la volatilidad de los datos, considerando muy pocos aspectos legales, que naturalmente, son particulares del ordenamiento legal de cada país. La guía detalla las características esenciales de la evidencia digital referidas a la admisibilidad, autenticidad, completitud, confiabilidad y credibilidad, siendo todas ellas de suma importancia para que la prueba digital pueda ser incorporada a un proceso legal, la guía detalla las características esenciales de la evidencia digital referidas a la admisibilidad, autenticidad, completitud, confiabilidad y credibilidad, siendo todas ellas de suma importancia para que la prueba digital pueda ser incorporada a un proceso legal.

Tal y como lo refiere el autor Leopoldo Sebastián Gómez en su obra "La Evidencia Digital en la Investigación Penal":

La seguridad de la información digital requiere el establecimiento de un perímetro global, lo que usualmente se logra mediante técnicas de cifrado. Las copias de la evidencia basada en papel se hacen en forma deliberada, resultan iguales al original y no contienen metadatos, siendo este último término muy utilizado en informática forense para referir a toda información adicional incorporada en un documento, y que en muchas ocasiones puede resultar de suma utilidad para la investigación. Por el contrario, la evidencia digital puede repetirse en copias con diferentes versiones, realizadas posiblemente en forma inadvertida como método de resguardo automático, y alberga metadatos. La transmisión de evidencia basada en papel se realiza en forma tradicional, garantizando la integridad de la información y con alcance limitado en su distribución. En sentido opuesto, la evidencia digital se transmite en forma electrónica, es alterable y su difusión tiene alcance prácticamente ilimitado por sus facilidades en el envío de copias a múltiples destinatarios. (Sebastián Gómez, Evidencia Digital en la Investigación Penal, 2018)

B. **ISO 27037: Directrices para la identificación, recopilación, consolidación y preservación de la evidencia digital.**

Es importante mencionar que esta normativa busca crear una línea base para la normalización internacional de prácticas digitales forenses, su objetivo es facilitar la usabilidad de la evidencia en distintas jurisdicciones, por procesos legales. Esta norma solo cubre el proceso inicial del trabajo forense digital: identificación, obtención y preservación de la evidencia digital potencial.

Es necesario describir las diferentes fases del análisis forense de evidencias digitales y para ello citaremos al autor Carlos García que en su libro “Cadena de Custodia Digital de las Evidencias para la realización de un peritaje” nos detalla cada uno de estos estadios, siendo así:

a. Identificar: El proceso de análisis forense comienza con la identificación de los elementos que pueden ser o contener evidencia digital potencial. Formalmente, la identificación es el proceso que implica la búsqueda, el reconocimiento y la documentación de potencial evidencia digital. Aunque la identificación de potencial evidencia digital suena simple en principio, existen complejidades sutiles. Por ejemplo, la evidencia digital tiene tanto una representación física y una virtual. Un disco duro con potencial de almacenar evidencia digital, la ubicación física de los datos es el disco duro, pero la propia evidencia viene de los datos contenidos en la unidad. Por otra parte, también puede no ser en absoluto obvia donde se aloja la potencial evidencia digital. Un servidor puede tener muy pocos discos conectados directamente y tienen una parte significativa de su almacenamiento dentro de un SAN o NAS (Storage Area Network o Network Attached Storage)

b. Recolectar y adquirir. Una vez identificada la potencial evidencia digital, debe ser o bien recogida u adquirida para su procesamiento, para el efecto hay que tener en cuenta las diferencias entre los conceptos: Colección: proceso de recopilación de artículos, que contengan potencial evidencia digital. Adquisición: proceso de creación de una copia de los datos en un conjunto definido. Colección es más o menos equivalente a la práctica de aplicación de la ley estándar de aprovechar los elementos que contengan potencial evidencia digital bajo la autoridad de un orden jurídico (es decir, una orden de registro) y el envío de ellos a un laboratorio forense u otro centro para el procesamiento y análisis. La adquisición es más común en el sector privado debido a la necesidad de minimizar el impacto, de una investigación en curso, en el negocio. Cabe señalar que la copia creada durante la adquisición puede variar desde la creación de una imagen forense de una unidad de disco duro, a una copia de los contenidos de la memoria de un servidor, hasta los contenidos lógicos de casilla de correo electrónico de un usuario individual, dependiendo del propósito y alcance de la investigación.

c. Preservar. Una vez que la potencial evidencia digital ha sido recolectada o adquirida, que debe ser preservada. La Normativa ISO 27037 define la conservación como el proceso de mantener y salvaguardar la integridad y / o el estado original del potencial de la evidencia digital. La preservación del potencial de evidencia digital es un proceso complejo e importante. Ayuda a asegurar la preservación de pruebas admisibles ante un tribunal de justicia. Sin embargo, la evidencia digital es notoriamente frágil y se cambia o se destruye fácilmente. Teniendo en cuenta que el trabajo del laboratorio forense digital oscila entre seis meses a un año (y que los retrasos en el sistema legal podrían crear nuevos retrasos), el potencial de la evidencia digital puede pasar un período de tiempo significativo en almacenamiento antes de que se analice o se utilice de forma legal. Este almacenamiento requiere estrictos controles de acceso para proteger los artículos de la modificación accidental o deliberada, así como los controles de entorno apropiados.

d. Requerimientos generales. Los requerimientos generales para la Normativa ISO 27037, se llenan al cumplir con los principios de auditabilidad, repetibilidad, reproducibilidad y justificabilidad definidos por la misma.
    - Auditable. Debería ser posible que un evaluador independiente o de otras partes interesadas acreditadas para evaluar las actividades realizadas por un DEFR y DES 2. Esto requiere la documentación apropiada en relación con las medidas adoptadas, por qué y cómo.
    - Repetible. La repetibilidad se establece cuando los mismos resultados de la prueba, se reproducen bajo las siguientes condiciones definidas por la Normativa ISO 27037: Usando el mismo procedimiento de medición y método. Utilizando los mismos instrumentos y en las mismas condiciones. Se puede repetir en cualquier momento después de la prueba inicial.

- Reproducible. La reproducibilidad se establece cuando los mismos resultados de la prueba se producen bajo las siguientes condiciones definidas por la Normativa ISO 27037: Utilizando el mismo método de medición. El uso de diferentes instrumentos y bajo diferentes condiciones. Puede ser reproducido en cualquier momento después de la prueba inicial.
- Justificable. El DEFR debe ser capaz de justificar todas las acciones y los métodos utilizados, por lo cual la Normativa ISO 27037 provee las herramientas necesarias para el efecto (García Dahinten, 2014)

I) ISO/IEC 27037:2012 "Guía para la identificación, recolección, adquisición y preservación de evidencias digitales.

La Organización Internacional para la Estandarización (ISO, 2012) publicó la ISO/IEC 27037:2012 que describe los lineamientos de trabajo sugeridos durante la identificación, recolección, adquisición y preservación de potencial evidencia digital.

Como lo refiere el autor Sebastián Gómez en su obra "Evidencia Digital en la Investigación Penal",

> la norma define claramente dos roles principales en la actuación pericial informática: el DEFR (Digital Evidence First Responder) y el DES (Digital Evidence Specialist). Las personas que actúan como DEFR son quienes se encargan de tareas de campo en procedimientos judiciales vinculadas con la identificación y preservación de evidencia digital. Teniendo presente la escasez de especialistas en informática forense, se estima que el rol del DEFR debe y puede ser perfectamente llevado a cabo por personal policial o personas que realicen actividades de investigación debidamente capacitados. Sin embargo, las etapas metodológicas de análisis y presentación de evidencia digital, que usualmente se realizan en laboratorio, deben quedar exclusivamente reservadas para aquellos profesionales informáticos especializados que tengan el rol de DES y que son

> los responsables de la realización de la pericia informática. El DEFR es el encargado de seguir los principios y lineamientos establecidos en informática forense durante el trabajo de campo para garantizar la autenticidad y confiabilidad de la evidencia digital. Conforme prescribe el estándar, estos procedimientos procuran: a) minimizar la manipulación de los dispositivos electrónicos o datos digitales, b) documentar todas las acciones y cambios que se hagan a la evidencia digital, de forma tal que un experto independiente pueda validar y emitir opinión respecto de la confiabilidad de la evidencia recolectada; c) proceder conforme el marco legal aplicable del cada país; d) el DEFR no debe actual más allá de su área de competencia (…) Sin perjuicio de lo expuesto, esta norma internacional contribuye a una mejora gradual del trabajo de aquellos que tengan un primer contacto con evidencia digital, como personal policial, abogados, investigadores, fiscales y magistrados, profesionales de seguridad informática y de respuesta a incidentes. (Sebastián Gómez, 2018)

Como lo refiere el autor Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos”:

> En cuanto a los roles definidos por la norma ISO 27037:2012, gran parte de las instituciones judiciales y policiales de Argentina carecen de personal capacitado para actuar como DEFR. Las tareas de campo son realizadas por personal policial cuya experticia es limitada ya que sólo tiene experiencia en recolección de evidencia física y actúa en el mejor de los casos bajo los lineamientos de guías operativas para recolección de prueba digital. El estándar apunta a la idea de separar las actividades de campo de las actividades periciales en laboratorio sobre evidencia digital. Como ya ha sido anticipado, con una adecuada capacitación el rol del DEFR puede y debe ser realizado por personal policial, técnico o de respuesta a incidentes y que tiene un perfil diferente de quien actúe como DES, siendo este último bien conocido en Argentina bajo

> la denominación de perito informático. Atendiendo a la escasez de recursos humanos calificados, esta modalidad de actuación sobre evidencia digital con división de roles desde el punto de vista metodológico contribuye y facilita el trabajo del especialista en informática forense, quien debe concentrar su esfuerzo en el laboratorio sobre aquellas labores periciales que requieren un mayor nivel de experticia y profesionalismo (Navarro Clérigues, 2015-2016)

Este protocolo es uno de los llamados para aplicar en Guatemala en cuanto a la identificación, recolección, adquisición y preservación de evidencia digital. Al ser presentado en forma accesible para una audiencia amplia puede facilitar actividades que requieran de la transferencia de evidencia digital entre jurisdicciones de diferentes países y contribuir a la cooperación internacional en materia de investigación penal con evidencia digital. Se advierte que este protocolo es completo, integral y objetivo, no obstante ello, en nuestro país no se ha profundizado para su manejo, adecuación y aplicación en el sector justicia, es menester indicar que ofrece cimientos básicos que pueden coadyuvar de sobremanera a los sujetos procesales en un proceso penal derivado de las bondades y amplitud que ofrece, además las normas y protocolos internacionales, no se han desarrollado a plenitud o en algunos casos siquiera se conocen en nuestros países latinoamericanos en virtud que de las autoridades encargadas de la investigación criminal no han tenido la capacitación adecuada por parte de los expertos adecuados.

Es interesante el punto de vista del autor Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos en cuanto a los roles de los expertos refiriendo que:

> Particularmente y en cuanto a los roles de DEFR y DES establecidos en la ISO/IEC 27037:2012, el protocolo deja claro que la actuación de campo deberá ser ejecutada por personal policial en el rol de DEFR, mientras que la actividad pericial informática en laboratorio estará a cargo de especialistas en informática forense que actúen como peritos informáticos en el rol de DES. A fin de ilustrar los lineamientos principales en

materia de identificación y preservación de evidencia digital, resulta oportuno citar contenidos del protocolo de actuación para pericias informáticas. (Navarro Clérigues, 2015-2016)

Es menester recordar que en capítulos anteriores mencionamos lo importante y relevante de la cadena de custodia digital y sus respectivos sellos o precintos de seguridad que nos garanticen que la evidencia no ha sido manipulada de alguna forma y que en el caso de evidencia electrónica y digital por regla deberá preferirse el secuestro del material tecnológico a cualquier otra alternativa para la preservación de información digital.

Un claro ejemplo sobre la forma en que se aplica el protocolo objeto de estudio es en el sentido que las pericias sobre telefonía celular deben ser practicada por un profesional de grado en Ciencias Informáticas y que ejerzan como peritos informáticos o su equivalente con el rol de DES que define el estándar internacional.

II) ISO/IEC 27037:15 - Guía para la identificación, recolección, adquisición y preservación de evidencias digitales

Como lo refiere el autor Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos:

Esta guía fue publicada el 15 de octubre de 2012 y proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos, para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones. Esta norma proporciona orientación para los siguientes dispositivos y circunstancias: 1. Medios de almacenamiento digital, como discos duros, discos ópticos, cintas, etc, que

se suelen emplear en ordenadores y sistemas informáticos. 2. Teléfonos móviles, PDAs, dispositivos personales electrónicos, tarjetas de memoria 3. Sistemas de navegación móviles (GPS). 4. Cámaras digitales y de vídeo. 5. Equipos con conexión de red. 6. Redes TCP/IP y otros protocolos digitales. 7. y todos aquellos dispositivos con funciones similares a los anteriores. A diferencia de la RFC 3227, la norma ISO/IEC 27037 hace referencia a componentes tecnológicos más avanzados y tiene esta característica en cuenta en el desarrollo de la misma. Por ejemplo, para el análisis de teléfonos móviles es más adecuada esta norma. (Navarro Clérigues, 2015-2016)

III) ISO/IEC 27041:2015 "Técnicas de seguridad. Orientación para garantizar la idoneidad y adecuación del método de investigación de incidentes".

Como lo refiere el autor Jorge Navarro en su obra "Guía actualizada para futuros peritos informáticos":

Esta norma internacional publicada en junio de 2015, ofrece orientación sobre los mecanismos para garantizar que los métodos y procesos utilizados en la investigación de incidentes de seguridad informática son los adecuados. Incluye la consideración de cómo los proveedores y pruebas de terceros se pueden utilizar para ayudar a este proceso de garantía. Sus objetivos son: a) proporcionar pautas sobre la captura y el posterior análisis de los requisitos tanto funcionales como no funcionales relacionados con la seguridad en la investigación de incidentes, b) utilizar la validación como medio de garantías de la idoneidad de los procesos involucrados en la investigación, c) a partir de un ejercicio de validación determinar nuevos niveles de validación que se requieran y las pruebas requeridas, d) determinar pruebas externas y la documentación a incorporar en el proceso de validación. (Navarro Clérigues, 2015-2016). Esta norma puede resultar útil para garantizar la validez de las evidencias digitales ante un proceso judicial

IV) ISO/IEC 27042:2015 “Técnicas de seguridad. Directrices para el análisis y la interpretación de la evidencia digital”.

Como lo refiere el autor Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos”:

> Esta norma internacional publicada en junio de 2015 proporciona una guía para el Resultado de la evidencia digital. Provee información sobre como adelantar un Resultado de la evidencia digital potencial en un incidente con el objeto de identificar y evaluar aquella que se puede utilizar para ayudar a su comprensión. Ofrece un marco común para el Resultado de la gestión de incidentes de seguridad, que pueda utilizarse para implementar nuevos métodos. También introduce una serie de definiciones relevantes para la práctica del análisis forense digital. Trata los modelos analíticos que pueden ser usados por los peritos informáticos forenses en sistemas estáticos o activos y las consideraciones, a tener en cuenta en cada caso, en especial atención a incidentes en sistemas vivos o activos como: dispositivos móviles, sistemas cifrados, redes, etc.
>
> Se definen dos formas de adelantar el análisis en vivo:
>
> a) En sistemas que no pueden ser copiados o no se puede crear una imagen. Existe el riesgo de perder la evidencia digital cuando se está copiando. Importante tener cuidado para minimizar el riego de daño de la evidencia y asegurar que se tiene un registro completo de los procesos.
> b) En sistemas que si se puede copiar o realizar la imagen. Examinar el sistema interactuando u observándolo en su operación. Ser cuidadoso para emular el hardware o software del entorno original, usando máquinas virtuales verificadas, copias del hardware original con el fin de permitir un análisis lo más cercano posible al real. (Navarro Clérigues, 2015-2016)

Por otro lado, se detalla el contenido de los resultados del análisis en el informe pericial y sus consideraciones legales. Finalmente, recoge las competencias de los peritos forenses: formación, aprendizaje, habilidades, objetividad y ética profesional.

V) ISO/IEC 27043:2015 "Técnicas de seguridad. Principios y procesos de investigación de incidentes."

Como lo refiere el autor Jorge Navarro en su obra "Guía actualizada para futuros peritos informáticos":

> Esta norma internacional publicada en marzo de 2015 proporciona una guía de principios para los procesos de investigación de incidentes que involucran evidencias digitales. Incluye los procesos de preparación previa al incidente a través del cierre de la investigación, así como advertencias al respecto. Las directrices describen los procesos y principios aplicables a los distintos tipos de investigaciones delictivas, como, por ejemplo, violaciones de seguridad, fallos del sistema, accesos no autorizados, entre muchos otros. No ofrece detalles particulares para cada tipo de investigación, pero si una visión general de los principios y procesos de investigación aplicables. (Navarro Clérigues, 2015-2016).

VI) ISO/IEC WD 27044 "Técnicas de seguridad. Directrices para la información de seguridad y la gestión de eventos (SIEM)

En su obra "Guía actualizada para futuros peritos informáticos" el autor Jorge Navarro refiere que:

> Esta norma internacional todavía en desarrollo. Describe un sistema para la gestión de eventos y de la seguridad de la información (SIEM). Con esta norma se pretende dar solución a los actuales problemas que existe a la hora de recoger evidencias en sistemas activos, complejos o con falta de recursos. Estas herramientas permiten monitorizar en tiempo real los eventos, proporciona la visibilidad de toda la estructura de

información, captura y análisis de redes y dispositivos móviles, control de aplicaciones y eventos que generan. Análisis de sistemas objeto de ataque, antes, durante y después del mismo. Administrador de riegos de la organización o entorno. Gestión de logs de los elementos y dispositivos del sistema global. Capacidad de resiliencia en las organizaciones objeto de ataque. En resumen, proporciona a las organizaciones una plataforma de inteligencia de la seguridad.

De conformidad a la información que se encuentra en el sitio web "https://www.une.org" hay diferentes normas que son utilizadas en informática forense, a continuación, se presentan los protocolos que son preferentemente utilizados en Europa, siendo los siguientes:

VII) UNE 71505-2:2013 "Buenas prácticas en la gestión de evidencias electrónicas.

Norma española que establece los controles y procesos para la gestión de seguridad de las evidencias electrónicas. Se aplica a entornos propios de las organizaciones con independencia de su actividad o tamaño. Puede ser aplicada por empresas que desempeñen servicios de los que se describen en relación con el ciclo de vida y/o controles descritos en la norma. Determina los datos que debe incluirla evidencia electrónica, además de su propio contenido, con el fin de documentar una determinada operación. Su estructura –formato y relaciones entre elementos que la integran- debería permaneces intacta. La fecha que fue creada, recibida y manipulada, así como, los participantes a lo largo del proceso en caso de existir, identificar el vínculo entre evidencias. (UNE Normalización Española, 2020)

Un aspecto interesante de esta norma es que dentro de su contenido desarrolla lo relativo a la confiabilidad de los procedimientos reducir significativamente las dudas que pudieren surgir en la veracidad de la evidencia digital que se haya custodiado,

gestionado o almacenado, además indica una serie de elementos que ayudan a conocer las fases en que se desarrolla la evidencia electrónica (adquisición, almacenamiento, recuperación, transmisión y presentación)

VIII) UNE 71506:2013 "Metodología para el análisis forense de evidencias electrónicas"

Norma española publicada en julio de 2013 y establece una metodología para la preservación, adquisición, documentación y presentación de las evidencias electrónicas. Esta norma es de aplicación a cualquier organización, así como profesional competente en este ámbito, como por ejemplo el perito informático forense. Va dirigida especialmente a los equipos de respuesta a incidentes y seguridad, así como al personal técnico de laboratorios o entornos de análisis forense de evidencias digitales (…) El capítulo 5 está dedicado a la preservación de las evidencias originales garantizando su inalterabilidad y validez legal, lo que permite la reproducibilidad de estudios sobre ellas. Almacenamiento en lugares y soportes estancos y aislados de interferencias o posibles agentes externos. El siguiente capítulo trata la adquisición de las evidencias, distinguiendo el trato a seguir si el sistema está apagado o encendido. También se valora que el análisis forense puede ser sobre datos de origen estático, datos en tránsito de sistemas en funcionamiento, datos volátiles, sistemas embebidos, datos de móviles y redes, así como grandes sistemas almacenamiento con información repartida en varios repositorios. El capítulo 7 se refiere a la documentación, garantizar la cadena de custodia y la trazabilidad de las evidencias, a través de la implantación de un sistema de gestión documental que registre las actuaciones sobre dichas evidencias, bien sean originales o clonadas. En su capítulo 8 se dedica al análisis de las evidencias digitales objeto de investigación. Y, por último, su capítulo 9 trata la presentación de los resultados obtenidos a la autoridad judicial o entidad que solicita el informe pericial. (UNE Normalización Española, 2020)

Es importante destacar que uno de los aportes de esta norma es presentar un modelo de informe pericial en relación a las evidencias electrónicas y digitales que se presentan ante un órgano jurisdiccional, se destaca además los elementos necesarios que se deben poseer para analizar las referidas evidencias, ésta es una de las normas utilizadas por las fuerzas y cuerpos de seguridad de muchos países europeos.

IX) UNE 197010:2015 "Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones"

Norma española publicada en marzo de 2011. La norma enumera los apartados mínimos necesarios a incluir en la elaboración de un informe, sin ser esta una enumeración excluyente, limitativa ni exhaustiva. También se describen los requisitos formales que deben tener los informes, sin especificar los métodos y procesos de elaboración. Es la norma más empleada en España en el ámbito del peritaje y la recomendada por la mayoría de colegios, expertos y organizaciones profesionales. El empleo de esta norma se considera admisible ante un procedimiento judicial. (Navarro Clérigues, 2015-2016)

6.2. Tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012.

Previo debemos hablar sobre el sentido de "certificación de evidencia digital" esto lo entenderemos como todo proceso que realizamos para validar en forma científica el procedimiento de obtención de la evidencia digital. El procedimiento de certificación de evidencia digital puede basarse en el algoritmo MD5. Se utiliza para comprobar la integridad de un archivo que ha sido transmitido mediante copia, e-mail, ftp, entre otros, entre diferentes sistemas informáticos.

Dentro de los aspectos a tomar en cuenta en el manejo de la evidencia digital se encuentran: implementar los protocolos ISO/IEC 27037 a efecto de garantizar la integridad de la evidencia digital, la documentación del escenario criminal mediante fotografía y video, el acompañamiento de un Notario y el inicio de una cadena de

custodia física y digital para que pueda dársele valor probatorio a la evidencia electrónica objeto del análisis.

De las normas anteriormente descritas debemos destacar las que, al criterio del autor de esta tesis, son necesarias implementar en Guatemala, podemos enunciar las siguientes:

a) ISO, International Standard Organization, es una organización dedicada a promover el desarrollo de normas y regulaciones internacionales para la fabricación de productos, exceptos los electrónicos.

b) ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO e IEC (International Electrotechnical Commission) que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

c) ISO/IEC 270037: Es una guía que proporcionar directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales.

d) ISO/IEC 27041: Es una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.

e) ISO/IEC 27042: Es una guía con directrices para el Resultado de las evidencias digitales.

f) ISO/IEC 27043: Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

g) ISO/IEC 27050: En desarrollo. Es una guía general del proceso de eDiscovery, “Descubrimiento de datos electrónicos”, su adquisición, manipulación y preservación.

En el caso de las normas UNE son aplicadas específicamente en Europa de conformidad a la legislación de cada país europeo que ha ratificado diferentes convenios y acuerdos y las normas ISO han sido implementados en diferentes países latinoamericanos que en su legislación interna han adoptado estas normativas y en consonancia con el Convenio de Budapest.

Como lo menciona Di Lorio en su texto “El Rastro Digital del Delito”. Las Normas Internacionales no pretenden contradecir ni sustituir las leyes o normativas jurisdiccionales respecto a la adquisición, tratamiento o preservación de la evidencia digital, simplemente pretenden guiar en el mejor establecimiento de estas prácticas. Pese a constituir estándares indiscutibles, la problemática de estos documentos es que son acotados en su alcance, deben adaptarse a la normativa de un país y a la situación institucional. (Di lorio. et al.)

6.3. Guías utilizadas a nivel mundial para el tratamiento de la evidencia electrónica y digital.

De conformidad a Zuccardi y Gutiérrez en su libro “Informática Forense, menciona las guías más utilizadas a nivel mundial para el tratamiento de la evidencia digital, siendo las siguientes:

A. Guía de la IOCE. La IOCE [IOCE06], publico “Guía para las mejores prácticas en el examen forense de tecnología digital” (Guidelines for the best practices in the forensic examination of digital technology) [IOCE02]. El documento provee una serie de estándares, principios de calidad y aproximaciones para la detección prevención, recuperación, examinación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte. Su estructura es: a) Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo). b)

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

B. Investigación en la Escena del Crimen Electrónico (Guía DoJ 1) El Departamento de Justicia de los Estados Unidos de América (DoJ EEUU), publico “Investigación En La Escena Del Crimen Electrónico” (Electronic Crime Scene Investigation: A Guide for First Responders) [ElCr01]. Esta guía se enfoca más que todo en identificación y recolección de evidencia. Su estructura es: a) Dispositivos electrónicos (tipos de dispositivos se pueden encontrar y cuál puede ser la posible evidencia). b) Herramientas para investigar y equipo. c) Asegurar y evaluar la escena. d) Documentar la escena. e) Recolección de evidencia. f) Empaque, transporte y almacenamiento de la evidencia. g) Examen forense y clasificación de delitos. h) Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

C. Examen Forense de Evidencia Digital (Guía DoJ 2). Otra guía del DoJ EEUU, es “Examen Forense de Evidencia Digital” (Forensic Examination of Digital Evidence: A Guide for Law Enforcement) [FoEx04]. Esta guía está pensada para ser usada en el momento de examinar la evidencia digital. Su estructura es: a) Desarrollar políticas y procedimientos con el fin de darle un buen trato a la evidencia. b) Determinar el curso de la evidencia a partir del alcance del caso. c) Adquirir la evidencia. d) Examinar la

evidencia. e) Documentación y reportes. f) Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).

D. Computación Forense - Parte 2: Mejores Prácticas (Guía Hong Kong) El ISFS, Information Security and Forensic Society (Sociedad de Seguridad Informática y Forense) creada en Hong Kong, publico “Computación Forense - Parte 2: Mejores Prácticas” (Computer Forensics – Part 2: Best Practices) [CoFor04]. Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la corte. Su estructura es: a) Introducción a la computación forense. b) Calidad en la computación forense. c) Evidencia digital. d) Recolección de Evidencia. e) Consideraciones legales (orientado a la legislación de Hong Kong). f) Anexos.

E. Guía De Buenas Prácticas Para Evidencia Basada En Computadores (Guía Reino Unido) La ACPO, Association of Chief Police Officers (Asociación de jefes de Policía), del Reino Unido mediante su departamento de crimen por computador, publico “Guía de Buenas Prácticas para Evidencia basada en Computadores” (Good Practice Guide For Computer Based Evidence) [GoPra99]. La policía creó este documento con el fin de ser usado por sus miembros como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia. Su estructura es: a) Los principios de la evidencia basada en computadores. b) Oficiales atendiendo a la escena. c) Oficiales investigadores. d) Personal para la recuperación de evidencia basada en computadores. e) Testigos de consulta externos. f) Anexos (legislación relevante, glosario y formatos)

F. Guía Para El Manejo De Evidencia En IT (Guía Australia) Standards Australia (Estándares de Australia) publico “Guía Para El Manejo De Evidencia En IT” (HB171:2003 Handbook Guidelines for the management of IT Evidence) [HBIT03]. Esta guía no está disponible para su libre distribución, por esto para su investigación se

consultaron los artículos “Buenas Prácticas En La Administración De La Evidencia Digital” [BueAdm06] y “New Guidelines to Combat ECrime” [NeGu03]. Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital. Detalla el ciclo de administración de evidencia de la siguiente forma: a) Diseño de la evidencia. b) Producción de la evidencia. c) Recolección de la evidencia. d) Análisis de la evidencia. e) Reporte y presentación. f) Determinación de la relevancia de la evidencia. (Zuccardi & Gutierrez, 2006).

6.4. Metodología Forense aplicada al tratamiento de la evidencia electrónica y digital.

Actualmente existen a nivel mundial guías o directrices para que los expertos o peritos forenses digitales realicen correctamente el tratamiento de la evidencia electrónica y digital y éstas se han originado a partir de buenas prácticas y protocolos internacionales de los cuales ya hemos hecho referencia. Sin embargo, debemos tomar en cuenta que implementar esas buenas prácticas es requerido emplear métodos eficientes, no obstante, también debemos ser muy objetivos y decir que los métodos tienen debilidades y fortalezas y que se debe tener expertiz para usar correctamente el software forense además de tener claro los protocolos a utilizar en cada caso en particular.

Debo mencionar que actualmente en Guatemala cuando se procesa un escenario criminal en donde existe evidencia electrónica y digital los técnicos que incautan esos indicios se estima que tienen poco o nulo conocimiento sobre la volatilidad de la información que ahí se encuentra y que además la cadena de custodia digital es iniciada con muchas deficiencias, sin dejar por un lado, que el equipo utilizado no es el adecuado y el personal que manipula la evidencia electrónica y digital no toma en cuenta la características propias de esos de indicios, presumiendo entonces que está contaminada la evidencia electrónica y digital.

En otro escenario es posible que el personal del Ministerio Público tenga conocimiento en algunos protocolos forenses de extracción de información digital sin embargo se estima que se incurre en el error que esa atribución y trabajo lo realiza un Técnico en Soporte Informático o en su caso un Técnico en Investigaciones Criminalísticas de la Unidad de Asistencia Técnica del Ministerio Público, quienes a pesar de realizar la labor con todo el esfuerzo del caso no tienen las herramientas forenses necesarias y también un perfil adecuado e idóneo con expertiz, es decir, no llena los requisitos de ser un profesional en materia de informática forense y si nos vamos a aspectos administrativos se podría observar que el nombramiento o contrato de trabajo de estas personas no comprende esas funciones por lo que en un eventual debate oral y público esa prueba podría desecharse fácilmente por resultar inidóneo.

De conformidad Leopoldo Sebastián Gómez, en su texto “Evidencia digital en la investigación penal” refiere que:

> La adquisición completa de evidencia digital en el lugar del hecho surge como alternativa técnica, ya que evita eventuales daños al hardware y minimiza el impacto en la operatoria de una empresa o institución. Esta modalidad es principalmente aplicada en actuaciones periciales que requieran resguardar evidencia digital en casos civiles y tiene sus bondades en aquellos lugares en los que deba minimizarse el impacto en la operatoria del negocio, pero requiere contar con personal entrenado que actúe como DEFR y recursos tecnológicos disponibles para las labores de campo. Teniendo presente la cantidad de hechos delictivos que involucran el análisis pericial de material informático y la escasez de peritos informáticos, referidos como DES a la luz de los lineamientos ya expuestos por la ISO/IEC 27037:2012, simplemente resulta inviable que los mismos abandonen sus actividades de laboratorio y se desplacen permanentemente a realizar este tipo de labores más propias de un DEFR. Esta recolección del corpus digital in situ permite que la evidencia digital pueda ser examinada a posteriori, contando con una imagen forense de la evidencia original

> sobre la que puede practicarse la pericia informática. Sin embargo, de no tomarse los recaudos necesarios para la recolección anticipada de evidencia digital altamente volátil, como la que se localiza en la memoria RAM de los equipos informáticos, al extraer los medios de almacenamiento para generar una clonación o una imagen forense aún persiste el riesgo de la imposibilidad de acceso posterior a la evidencia digital si dichos dispositivos cuentan con métodos de cifrado para protección de datos (…) Esta recolección del corpus digital in situ permite que la evidencia digital pueda ser examinada a posteriori, contando con una imagen forense de la evidencia original sobre la que puede practicarse la pericia informática (…) La utilización de tecnología informática avanzada posibilita el análisis de grandes volúmenes de datos, siendo un ejemplo de ello el uso de computadoras y servidores con elevada capacidad de memoria y múltiples procesadores, arreglos de discos de estado sólido, aceleradoras gráficas para procesamiento en paralelo y tecnología de cómputo distribuido, que permita una reducción de tiempo durante el procesamiento masivo de información. (Sebastián Gómez, https://www.researchgate.net/, 2006)

Una crítica que se le da a la evidencia electrónica y digital es lo referente a la manipulación y la poca seguridad que da mantener integra la evidencia y para ello es necesario citar nuevamente al autor Sebastián Gómez que a su vez cita a Schmitt and Jordán quien indica que:

> En los últimos años surgieron algunas críticas a estos algoritmos fundadas en descubrimientos de métodos para generar colisiones. Es dable destacar que las debilidades planteadas por colisiones no son relevantes en el ámbito de la informática forense, ya que no comprometen una propiedad de MD5 y SHA-1 conocida como la resistencia a la pre imagen. Ello significa que si sólo se cuenta con una certificación hash generada a priori no es posible obtener un conjunto de datos de entrada que produzca este mismo valor. Más aún, la resistencia a la segunda pre imagen de MD5 y

SHA-1 garantiza que si se tiene un conjunto de datos de entrada y su respectivo valor hash (hablamos de la evidencia digital y su respectiva certificación digital) no es posible obtener un conjunto de datos diferente que arribe al mismo valor hash. Aunque podría ser posible manipular la información digital para producir dos valores hash idénticos a partir de diferentes datos de entrada, las alteraciones deben ser muy específicas. Esto significa que alterar la evidencia digital que tiene una certificación digital MD5 cuyo valor hash fue calculado a priori y manipularlo para que afecte la interpretación de la evidencia manteniendo el mismo valor hash es computacionalmente improbable. Estas conclusiones permiten afirmar que si un artefacto que conforma la evidencia digital fue certificado mediante MD5 o SHA-1, es viable volver a calcular el valor hash en un momento posterior y si ambos valores coinciden significa que la integridad de la evidencia se mantiene incólume. Queda clara entonces la importancia que tienen estos métodos computacionales en la informática forense para que la evidencia digital mantenga su integridad y sea admisible durante el proceso judicial. (Sebastián Gómez, https://www.researchgate.net/, 2006)

6.5. Propuesta de protocolo de acción para el procesamiento de la evidencia electrónica y digital en la escena del crimen.

De conformidad a los diferentes preceptos que se tienen sobre Criminalística y la experiencia en el ámbito forense, presento a continuación una propuesta para el tratamiento de la evidencia electrónica y digital para que pueda ser aplicado en el escenario criminal que el Ministerio Público procesa y que de conformidad a la ley le son encomendados, esto con el fin de apoyar la labor investigativa del ente fiscal y así reducir la labor pragmática y sin protocolos que a juicio del presente investigador se hace presente en cada equipo de escena del crimen del Ministerio Público que sin menospreciar la labor que realiza el ente investigativo se evidencia la carencia de aptitudes para tratar un escenario criminal digital, asimismo, esto coadyuvará a que la evidencia digital que se presente ante Juez competente y que más adelante él valorará

como prueba, evitando con ello arbitrariedades en la apreciación de la evidencia digital y electrónica.

De conformidad al estudio de los protocolos y estándares internacionales sobre el tratamiento de la evidencia electrónica y digital y bajo los parámetros de una metodología objetiva de aplicación, específicamente la norma ISO/IEC 27037:2012 “Guía para la identificación, recolección, adquisición y preservación de la evidencia digital”, ISO/IEC 27042:2015 “Guía para el Resultado de la evidencia digital”, de la informática forense presento una propuesta concreta general, tanto para el ámbito privado como aplicado al ámbito público específicamente los actores del sector justicia en materia penal y en éste último hago la observación que el ente encargado de la investigación penal en Guatemala considere esta propuesta y sirva como guía y con ello mejore el trabajo que realiza en cuanto al manejo de la evidencia electrónica y digital, siendo el siguiente:

A. Aspectos previos.

I. El personal de la Dirección de Investigación Criminalísticas del Ministerio Público debe tener un entrenamiento constante en el manejo y tratamiento de la evidencia electrónica y digital y verificar que su preparación sea certificada por un ente reconocido o profesionales de experiencia para ello se recomienda que los equipos que estén conformados siempre exista un especialista en evidencia electrónica y digital es decir el equipo de escena del crimen por lo mínimo debe estar conformado así: embalador, planimetrista, coordinador del equipo y el Perito Forense Digital con funciones de Primer Respondiente la escena del crimen (encargado de la adquisición y recolección de la evidencia con conocimientos científicos en informática forense y criminalístico), con la guía del fiscal encargado de procesar la escena del crimen.

II. Previo a procesar la escena del crimen el personal encargado de realizar esta labor debe contar con el equipo adecuado tales como: guantes de vinilo o nitrilo, trajes de bioseguridad, cubre bocas o mascarilla certificada, cubre calzado, lentes de seguridad, cofia o capucha.

III. El equipo de escena del crimen debe contar con los insumos convencionales para el procesamiento de la escena, pero adicional el primer respondiente debe contar con un kit para suficiente para llevar a cabo su labor como por ejemplo clonadora o duplicadora forense de discos duros, puntas para conexiones de dispositivos, clonadora forense para pendrives y tarjetas de memoria, bloqueadores de escritura, cables, bolsas y cajas de Faraday. Actualmente existen maletines de extracción y análisis de información forense digital o también llamados estaciones forenses que reúne el hardware necesario.

IV. Previo a que el equipo de escena del crimen o en su caso el Perito Forense Digital en función de Primer Respondiente en un entorno privado o empresarial empiece su función debe conocer los protocolos a seguir para manipular los dispositivos electrónicos y el protocolo a seguir para extraer la información que se requiera, se sugiere llevar en forma escrita los protocolos y solo usarse en caso se tenga duda sobre el procedimiento a seguir.

V. Cuando sea necesario el secuestro de dispositivos electrónicos deben seguirse los protocolos correspondientes y consecuentemente iniciar la cadena de custodia física y digital

VI. Agotar el procedimiento de extracción de información y clonación forense creando la imagen de disco correspondiente en el lugar mismo de la escena del crimen, según lo permitan las circunstancias y el contexto del caso en concreto.

VII. Cuando se deba procesar un escenario criminal en donde existan evidencias electrónica, digital y física de otra categoría es necesario que el equipo de –DICRI- y el fiscal encargado decidan cual procesarán primero, en virtud que no es técnico hacerlo en forma mixta o conjunta en virtud que cuando nos referimos a dispositivos electrónicos y los datos ahí contenidos debemos tomar en consideración la volatilidad de la información que conlleva a una perdida permanente si no se actúa de conformidad a los protocolos y normas internacionales, se sugiere procesar la evidencia electrónica y digital luego el resto de indicios que se encuentren.

VIII. Si es posible obtener información sobre contraseñas ya sea aportadas en forma voluntaria o las obtenidas en el proceso de extracción de información in situ éstas deben hacerlas constar el fiscal en el acta de allanamiento.

IX. Debe tomarse video y fotografía de todo el procesamiento del escenario criminal incluso antes de mover o desconectar los dispositivos.

X. No se deben tocar o manipular todo tipo de indicios sobre material informático sin el equipo necesario en virtud del principio de intercambio de Locard que indica cuando dos cuerpos entran en contacto existe intercambio de material físico el uno con el otro.

XI. Si los equipos están encendidos deben desconectarse los cables de red y desconectarlos de la red de energía eléctrica desde su respectiva toma y no desde el enchufe de la pared. Si los equipos están apagados deben quedarse apagados y solo proceder a identificar las características que lo individualicen y luego embalarlos en una bolsa o caja de Faraday. También es necesario apagar las conexiones Bluetooth o wifi a las que estuviere conectado el equipo, en el caso de una computadora portátil que está encendida debe quitarse la batería.

XII. Identificar los equipos que están conectados a una línea de teléfono y para ello debe procurarse ubicar el número de teléfono que le corresponde y consignar ese dato en el acta de allanamiento.

XIII. Se debe priorizar secuestrar dispositivos o equipos informáticos que almacenen grandes cantidades de información en virtud que en ocasiones la extracción de información in situ resulta inviable por el factor tiempo, en estos casos, en estos casos se procederá a extraer la información en un laboratorio forense.

XIV. Se debe colocar cinta o sellar cada entrada eléctrica y todos los puertos periféricos de los equipos para evitar que con o sin intención conecten cables que puedan destruir o dejar inservible el dispositivo o equipo informático.

XV. En la escena criminal el Perito Forense Digital debe seguir los protocolos necesarios para mantener la integridad de la prueba electrónica, digital y las convencionales o tradicionales.

XVI. Debemos considerar que en el campo de la informática forense se aplica la totalidad de dispositivos electrónicos y cada uno tiene su tratamiento diferente y por lo tanto deben seguirse los protocolos afines para cada uno.

XVII. Los dispositivos electrónicos que constituyan evidencia electrónica tienen particularidades diferentes en cuanto a su almacenamiento y transporte y que de

alguna forma son afectados por la temperatura la energía electroestática, golpes, humedad; por lo que se debe ser cuidadoso para su salvaguarda y transporte.

XVIII. Como parte del protocolo a seguir en un escenario criminal se debe etiquetar, documentar, marcar, fotografías, grabar y rotular todos los dispositivos electrónicos encontrados.

XIX. Identificar cada uno de los cables que tuviere conectado el dispositivo o equipo electrónico.

B. Errores comunes que deben superarse en el tratamiento de la evidencia electrónica y digital.

I. El escenario criminal digital debe ser manipulado y procesado por el personal capacitado y certificado en evidencia electrónica y digital, en el caso del ámbito privado no debe permitirse que el personal de la dirección o unidad de Tecnologías de Información sean quienes intervengan en el procedimiento de recolección de la evidencia electrónica y digital si no tiene las competencias necesarias; en el caso del ámbito público, los equipos de escena del crimen de la Unidad de Recolección de Evidencias de la Dirección de Investigaciones Criminalísticas del Ministerio Público deben evaluar el tipo de escena a procesar en virtud que si existe la probabilidad de encontrar evidencia electrónica (dispositivos electrónicos) o evidencia digital (información y datos en los dispositivos electrónicos) deben llamar al equipo especializado en manipular esa escena. Esto requiere que el Ministerio Público dote de las competencias necesarias a sus colaboradores a efecto de procesar una escena criminal con evidencia electrónica y digital de conformidad a ISO/IEC 27037:2012 “Guía para la identificación, recolección, adquisición y preservación de la evidencia digital”, superándose la limitante actual en donde la unidad “UFED” de la Dirección de Investigaciones Criminalísticas del Ministerio Público solo actúa en casos de alto impacto, casos seleccionados o casos sobre pornografía infantil y trata de personas, asimismo también existe personal de la Dirección de Análisis Criminal que a pesar que cuenta con técnicos y herramientas

forenses, estos son utilizados en forma errónea y con fines distintos a los que podría emplearse en el campo de la informática forense.

II. El fiscal que acompaña a la –DICRI- debe circunscribirse a procesar la escena del crimen dirigiendo al personal de –DICRI- para sean ellos quienes a través de sus especialistas en evidencia electrónica y digital realicen su labor.

III. En caso de un allanamiento siempre existirá el riesgo de que un elemento de la Policía Nacional Civil, personal del Ministerio Público o un familiar manipule de alguna forma algún dispositivo electrónico, ya sea en forma voluntaria o involuntaria, un ejemplo claro es apagando o manipulando un dispositivo electrónico, en este caso desde el momento que se inicie la diligencia debe asegurarse y resguardar la escena criminal y ubicar los indicios que serán útiles para la investigación o el caso concreto.

IV. En ámbito público, en una investigación realizada por el Ministerio Público, cuando ya se han secuestrado los dispositivos electrónicos o se tiene la evidencia electrónica y digital el fiscal no debe abrir el embalaje que la contiene sino hasta la presentación en el debate oral y público o según sea requerido y necesario presentarlo ante juez competente, para ello es necesario que tanto el fiscal como los otros sujetos procesales tengan copias integras de la información sujeta a investigación y que fue obtenida de la original cuando se realizó la clonación o el duplicado en el escenario criminal, en ese sentido la cadena de custodia física y digital se rompe cuando el fiscal “efectúa una inspección ocular” en la sede de la fiscalía sin que estén presentes los otros sujetos procesales, debe eliminarse esta mala práctica y que de por sí ha contaminado ya la evidencia.

V. Cuando se incauta un dispositivo electrónico este debe ser embalado en bolsas o cajas de Faraday para asegurar que la información que ahí se contiene no sea manipulada o modificada en forma remota, cuando se encuentra en sobres manila o cajas de cartón, cajas plásticas o cualquier objeto similar se dudará sobre la integridad de la evidencia electrónica y digital en virtud que no se tendrá certeza o seguridad que no ha sido manipulada.

C. Buenas prácticas para el tratamiento de la evidencia electrónica y digital.

I) *Primer Respondiente*:

a) Al momento de recibir la llamada de primer respondiente, buscar apoyo de un segundo perito forense digital y de un Notario.

b) Llegar a la escena, identificando los actores, el entorno, definiendo como vas a proceder. Este paso es fundamental para la recolección de evidencia in situ.

c) Empezar a actuar según el protocolo general que se definió previamente.

d) Acordonar el área.

e) Toda acción que haga el primer respondiente, debe identificarse en voz alta para que quede documentado en video.

f) Documentar cualquier anomalía encontrada, ya sea en la escena o de parte de una tercera persona.

g) En un caso mixto (balística e informática, por ejemplo), hay que extraer la evidencia lo más rápido posible, y analizar la evidencia en el laboratorio.

h) Realizar notas detalladas, incluyendo fecha y hora indicando si se utiliza horario local o UTC.

i) Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.

j) En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.

k) Recoger la información según el orden de volatilidad (de mayor a menor). 1. Registros y contenido de la caché 2. Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria. 3. Información temporal del sistema. 4. Disco. 5. Logs del sistema. 6. Configuración física y topología de la red informática.

II) *En el escenario criminal*:

a) Se debe documentar todo el procedimiento mediante fotografía y video observando que el equipo especialista use en todo momento los guantes de nitrilo y el equipo de bioseguridad completo.
b) Hace constar en acta ministerial todos los puntos necesarios a efecto de establecer la identificación, recolección y adquisición de la evidencia electrónica y digital.
c) Realizar planimetría del escenario criminal en donde aparezca toda la evidencia electrónica encontrada.
d) Deben aislarse los dispositivos electrónicos de las personas y solo el Perito Forense Digital y el equipo especialista puede procesar la evidencia electrónica y digital.
e) No se deben ingresar dispositivos electrónicos ni metálicos o que tenga alguna frecuencia de comunicación en virtud que podrían alterar la evidencia digital.
f) Utilizar insumos digitales estériles o vírgenes para cada proceso de recolección a fin de evitar alguna modificación o alteración o magnética en los datos o información recolectada y asimismo los equipos deben contar con licencia original del hardware utilizado en la recolección, almacenamiento y análisis de información, además el antivirus debe ser original y estar actualizado.
g) Si el equipo está encendido, dejarlo encendido, si está apagado dejarlo en ese estado para evitar que se borren los datos volátiles.
h) Verificar si en las ranuras del dispositivo se encuentran conectados dispositivos de almacenamiento tales como tarjetas micro sd, memorias USB, etc.
i) Sellar con cinta tornillos, puertos o cualquier entrada que tenga el dispositivo a efecto de evitar que se garantizar que el dispositivo electrónico se encuentra integro con las mismas piezas.

j) Utilizar bolsas o cajas tipo Faraday para embalar los dispositivos electrónicos, no se deben usar bolsas plásticas por la energía electroestática que puede ocasionar y causar daño al dispositivo.

k) Antes de recolectar los indicios electrónicos se debe observar e identificar precisamente lo que se recolectará y para ello el Primer Respondiente o especialista encargado de recolectar la evidencia electrónica y digital categorizará cada elemento encontrado empezando por aquellos dispositivos en donde la información sea más volátil y considerando priorizar primero los elementos más pequeños y luego los grandes en volumen.

l) En un escenario criminal (ámbito público) se debe tener a la vista la autorización de juez competente para la diligencia de allanamiento, inspección, registro, secuestro y análisis de evidencia electrónica y digital.

D. Equipos de cómputo tales como computadoras de escritorio, portátiles, tabletas electrónicas, entre otros.

I) <u>Encendido.</u>

a) Evitar mover el mouse o touchpad si no ha instalado y conectado previamente el hardware forense correspondiente, posteriormente puede mover el mouse para que no se apague la pantalla y se bloquee.

b) Verificar la fuente de poder a la que está conectada, para el efecto se deberá desconectar el cable del dispositivo encendido o en su defecto quitar la batería si no fuese necesario extraer la información in situ, clonaje de información y creación de imagen forense o algún otro procedimiento.

c) Extraer los dispositivos de almacenamiento instalados.

d) Conectar los dispositivos bloqueadores de escritura.

e) In situ y si las condiciones del escenario criminal lo permiten, se debe crear una imagen forense de la información mediante la técnica del Bit a Bit.

f) Generar el algoritmo Hash a cada uno de los procedimientos, para el efecto también se generará la cadena de custodia física y digital, ésta última también con su código Hash.
g) Firmar digitalmente la imagen forense que se ha generado.
h) De la imagen forense creada deberán crearse clones o copias digitales para que puedan entregarse a los sujetos procesales para los usos correspondientes y legales. La imagen forense original debe almacenarse en un medio de almacenamiento contra escritura y que sea solo de lectura, luego se generará la cadena de custodia digital, para que luego dicho medio de almacenamiento sea embalado en una bolsa de Faraday e iniciándose la cadena de custodia física.

II) *Apagado*.

a) Identificar los dispositivos de almacenamiento.
b) Extraer los dispositivos de almacenamiento instalados
c) Conectar los dispositivos bloqueadores de escritura.
d) In situ y si las condiciones del escenario criminal lo permiten, se debe crear una imagen forense de la información mediante la técnica del Bit a Bit.
e) Generar el algoritmo Hash a cada uno de los procedimientos, para el efecto también se generará la cadena de custodia física y digital, ésta última también con su código Hash.
f) Firmar digitalmente la imagen forense que se ha generado.
g) De la imagen forense creada deberán crearse clones o copias digitales para que puedan entregarse a los sujetos procesales para los usos correspondientes y legales. La imagen forense original debe almacenarse en un medio de almacenamiento contra escritura y que sea solo de lectura, luego se generará la cadena de custodia digital, para que luego dicho medio de almacenamiento sea embalado en una bolsa de Faraday e iniciándose la cadena de custodia física.

E. Dispositivos de comunicación como Router y Firewall.

- *Encendido y apagado*.
    a) Recolectar datos volátiles.
    b) Apagar el dispositivo sin mayor protocolo (en forma abrupta).
    c) Extraer los dispositivos de almacenamiento instalados.
    d) Conectar los dispositivos bloqueadores de escritura.
    e) In situ y si las condiciones del escenario criminal lo permiten, se debe crear una imagen forense de la información mediante la técnica del Bit a Bit.
    f) Generar el algoritmo Hash a cada uno de los procedimientos, para el efecto también se generará la cadena de custodia física y digital, ésta última también con su código Hash.
    g) Firmar digitalmente la imagen forense que se ha generado.
    h) De la imagen forense creada deberán crearse clones o copias digitales para que puedan entregarse a los sujetos procesales para los usos correspondientes y legales. La imagen forense original debe almacenarse en un medio de almacenamiento contra escritura y que sea solo de lectura, luego se generará la cadena de custodia digital, para que luego dicho medio de almacenamiento sea embalado en una bolsa de Faraday e iniciándose la cadena de custodia física.

F. Dispositivos de captura de datos, imágenes y audios tales como grabadoras digitales, cámaras de video, reproductor mp3, entre otros.

a) Si se encuentra encendido se debe apagar el dispositivo electrónico.
b) Extraer la batería o desconectarlo de la corriente eléctrica.
c) Extraer los dispositivos de almacenamiento instalados.
d) Conectar los dispositivos bloqueadores de escritura.

e) In situ y si las condiciones del escenario criminal lo permiten, se debe crear una imagen forense de la información mediante la técnica del Bit a Bit.
f) Generar el algoritmo Hash a cada uno de los procedimientos, para el efecto también se generará la cadena de custodia física y digital, ésta última también con su código Hash.
g) Firmar digitalmente la imagen forense que se ha generado.
h) De la imagen forense creada deberán crearse clones o copias digitales para que puedan entregarse a los sujetos procesales para los usos correspondientes y legales. La imagen forense original debe almacenarse en un medio de almacenamiento contra escritura y que sea solo de lectura, luego se generará la cadena de custodia digital, para que luego dicho medio de almacenamiento sea embalado en una bolsa de Faraday e iniciándose la cadena de custodia física.

G. Teléfonos celulares y dispositivos electrónicos de comunicación:

a) Si está encendido, bloquear la señal telefónica u otra onda similar.
b) Si está encendido, generar el código IMEI (*#06#) para identificar el dispositivo.
c) Introducirlo en una bolsa de Faraday.
d) Extraer la información mediante las herramientas forenses correspondientes.
e) Extraer batería y la tarjeta de memoria.
f) Realizar una imagen forense de la tarjeta de memoria.
g) Extraer la información del teléfono y de la tarjeta de memoria.
h) Generar el algoritmo Hash a cada uno de los procedimientos, para el efecto también se generará la cadena de custodia física y digital, ésta última también con su código Hash.
i) Firmar digitalmente la imagen forense que se ha generado.
j) Rotular e identificar la evidencia incautada.

H. Dispositivos electrónicos de impresión.

a) Desconectar de la red de datos y voz.
b) Iniciar la recolección de datos volátiles y seguidamente generar los Logs o registros del dispositivo.
c) Apagar abruptamente o quitar la batería.
d) Generar el algoritmo Hash a cada uno de los procedimientos, para el efecto también se generará la cadena de custodia física y digital, ésta última también con su código Hash.
e) Firmar digitalmente la imagen forense que se ha generado.
f) Rotular e identificar la evidencia incautada.

Es menester indicar que existen más protocolos que son particulares y aplicables a cada dispositivo electrónico y para efectos de este trabajo de investigación solo se han presentado los más importantes a juicio del autor. Por último, debemos recordar que los procedimientos indicados pueden ejecutarse con el auxilio de diferentes herramientas forenses tales como FTK Imager[14], Autopsy[15], OSForensics[16], Caine[17], no solo en la fase de adquisición, almacenamiento y preservación de la información, sino también en la fase de análisis y presentación de resultados. Es importante mencionar que existen más opciones nos llevan al mismo fin que es el tratamiento de la evidencia electrónica y digital.

[14] Es una herramienta para realizar réplicas y visualización previa de datos, la cual permite una evaluación rápida de evidencia electrónica para determinar si se garantiza un análisis posterior con una herramienta forense como AccessData Forensic Toolkit. FTK Imager también puede crear copias perfectas (imágenes forenses) de datos de computadora sin realizar cambios en la evidencia original. http://www.reydes.com/d/?q=Crear_la_Imagen_Forense_desde_una_Unidad_utilizando_FTK_Imager

[15] Es un software informático que simplifica la implementación de muchos de los programas y complementos de código abierto utilizados en The Sleuth Kit . [1] La interfaz gráfica de usuario muestra los resultados de la búsqueda forense del volumen subyacente, lo que facilita a los investigadores marcar las secciones de datos pertinentes. https://en.wikipedia.org/wiki/Autopsy_(software)

[16] Software forense que ayuda a ubicar datos relevantes más rápido a través de la búsqueda e indexación de archivos de alto rendimiento. Extraiga contraseñas, descifre archivos y recupere archivos eliminados rápida y automáticamente de los sistemas de archivos de Windows, Mac y Linux. https://www.osforensics.com/index.html

[17] se diferencia de las demás distribuciones de su tipo (Forensic Boot CD, Helix, Deft, etc..) por su facilidad de uso y que proporcionar una interfaz gráfica homogénea que guía a los investigadores digitales durante la adquisición y el análisis de las pruebas electrónicas, y ofrece un proceso semiautomático durante la documentación y generación de informes. https://www.dragonjar.org/distribucion-live-cd-analisis-forense.xhtml

CAPITULO VII

El Rol del Perito Forense Digital.

7.1. Peritos informáticos.

Es necesario apuntar las características fundamentales que diferencian y resaltan la función de los expertos en pericias forenses digitales, recibiendo el nombre de peritos forenses digitales, peritos digitales, peritos informáticos, entre otras muchas más denominaciones.

Una definición interesante sobre el Perito Informático que refiere Emilio del Peso Navarro en su obra “Peritajes Informáticos”, es que este experto es “un profesional experto y titulado, dotado de conocimientos legales, teóricos y prácticos especializados en informática y tecnologías de la información, capaz de asesorar o elevar un dictamen comprensible y a la vez técnico sobre un litigio o cualquier otra situación que se le requiera” (Del Peso Navarro, 2001).

Debemos apuntar que en aspectos generales existen dos tipos de actuación de este tipo de expertos, una en el ámbito privado y otra en la esfera pública. El Perito Forense Digital tiene una tarea ardua y es que debe realizar una tarea de auditoría, cotejo, revisión y presentación de los resultados de la evidencia que ha sido sometida a su expertiz, tomando en cuenta que su función muchas veces es de asesoría y consultoría. No basta con poseer los conocimientos técnicos, legales y prácticos, sino que debe garantizar que el resultado de su trabajo sea objetivo, metódico, demostrable, reproducible, veraz, auditable, creíble, honesto y profesional. Es menester indicar que el Perito Forense Digital debe aplicar las técnicas y métodos forenses de conformidad a los estándares y protocolos internacionales, incluyendo las buenas prácticas con el fin de preservar con certeza jurídica la evidencia electrónica y digital.

En Guatemala actualmente existen diferentes personas entusiastas que se han aventurado en el campo de la informática forense y se dicen llamar “Expertos en Informática Forense” y se arrogan derechos y privilegios para abordar este campo, sin

embargo, esta intención queda limitada a una intención en muchos casos de buena fe con el objeto de coadyuvar en determinada investigación y en otras de mala fe con el objeto de desestabilizar una investigación. También existe la creencia que una persona por tener un título determinado es suficiente para practicar la informática forense y consecuentemente el tratamiento de la evidencia electrónica y digital, tal es el caso que se presupone que un Ingeniero en Sistemas o ciencias afines o un Criminalista con su función per se, es suficiente para realizar este tipo de pericias, sin embargo se incurre en un error grave ya que en las aulas universitarias y técnicas que existen en Guatemala son muy pocas las que en realidad aportan una formación científica y técnica y esto se puede evidenciar en los informes que aquellos profesionales presentan, toda vez que se carecen de sustento técnico y formal consecuentemente no tiene una base apegado a los protocolos y estándares internacionales.

No existe un programa de preparación universitaria para la formación de expertos en informática forense o Peritos Forenses Digitales, sin embargo existen empresas que se ha preocupado por este tipo de formación y aportan cierto entrenamiento para el manejo de herramientas, técnicas y metodología en informática forense, siendo esto en muchas ocasiones suficiente para que puedan presentarse informes de investigación sustentados ya sea ante la empresa que requirió los servicios en su caso ante un juez para que emita juicio y le dé el valor probatorio correspondiente. Podemos afirmar entonces que en Guatemala existe poco auge de esta profesión que hoy en día es un imprescindible en materia de investigación criminal.

En otros países existe la voluntad política para la formación de Peritos Informáticos o Perito Forenses Digitales tal es el caso de Brasil en donde existen concursos de oposición para ocupar cargos de Perito Criminal Federal. Particularmente para el área de informática forense y en el rol profesional equivalente al cargo de perito informático sólo se admiten aspirantes con carreras universitarias de grado en informática que estén reconocidas por la Dirección o Ministerio de Educación de determinado país siendo estos cargos excluyentes para quienes no cumplan con este requisito. En el caso de Argentina se ha avanzado en este tema y el Poder Judicial y el

Ministerio Público Fiscal ha iniciado a crear espacios para estos expertos forenses, además ha creado laboratorios forenses con profesionales graduados en informática, accediendo al puesto mediante concursos por oposición.

Como lo refiere Leopoldo Sebastián Gómez en su obra “Evidencia Digital en la Investigación Penal” refiere que:

> este perfil profesional del perito informático será el que abra paso a la ciencia y permita ir dando cierre a la etapa de la artesanía en el desarrollo histórico de la informática forense. Se revertirá la composición actual de este perfil mitológico del perito informático, que mantiene mucho de arte y nada de ciencia. Sólo entonces comenzará la conformación de una nueva generación de peritos informáticos con un perfil científico adecuado, que sean capaces de hacer contribuciones valiosas para el desarrollo de la profesión, quienes podrán ejercer y asistir con saberes especializados a los responsables de la investigación penal. (Sebastián Gómez, 2018).

En el caso de España se contemplan algunos requisitos que deben cumplir las personas que desean ejercer la profesión de Perito Forense Digital, entre ellos están: Tener un título a nivel universitario ya sea como Ingeniero en Informática, Licenciado en Informática, Master en Ingeniería Informática, Ingeniero Técnico en Informática, Diplomado en Informática. Sin embargo los protocolos internacionales al analizarlos y que se han enumerado en un capítulo anterior evidencias que deben tenerse los siguientes conocimientos: Formación en el área legal y judicial, criminalística, criminología, en técnicas de investigación, técnicas de recopilación de evidencias y pruebas periciales, auditoría organizacional, administración de riesgos, conocimientos en Tecnologías de la Información; además resulta interesante que una tendencia que existe en la conformación de un equipo multidisciplinario, un ejemplo de ello es la forma en que estaba conformado el equipo de Expertos en Informática Forense de la Comisión Internacional contra la Impunidad en Guatemala quienes así desempeñaban su función.

7.2. Ámbitos de actuación.

Plantea Leopoldo Sebastián Gómez en su obra “Evidencia Digital en la Investigación Penal” la forma en que realiza su función el Perito Forense Digital afirmando:

> sí echamos la mirada atrás, la mayoría de demandas de peritaciones informáticas se desarrollaban dentro del ámbito particular o empresarial, pero cada vez más, la figura del perito informático forense es requerida como auxiliar de la justicia para el dictamen de evidencias tecnológicas que faciliten al juez el esclarecimiento de un litigio. Por otro lado, sus conocimientos de análisis forense digital son demandados por empresas, organizaciones y gobiernos para fortalecer la seguridad informática, y del resultado de su investigación ante un ciberataque, determinar las medidas de respuesta y nuevas políticas de seguridad a implantar. Apuntar, que los especialistas en ciberseguridad requieren de conocimientos, entre otros, de análisis forense, análisis de malware, análisis y evaluación de vulnerabilidades, gestión de incidentes, manejo de herramientas hacking ético, auditoria de redes; áreas todas ellas con competencias del perito informático forense. (Sebastián Gómez, Evidencia Digital en la Investigación Penal, 2018)

En cuanto al ámbito judicial sigue enfatizando el autor que:

> el perito informático judicial, es aquel perito informático que desarrolla su labor dentro de un procedimiento judicial sea penal o criminal. Puede ser designado por cualquiera de las partes o a petición del tribunal. Cuando un perito informático forense es nombrado por un magistrado o un juez, se transforma en auxiliar de la justicia y debe realizar la función pública según el cargo conferido y de acuerdo a derecho (…) en el ámbito judicial, el perito informático forense, es un experto designado por la autoridad del proceso judicial, para que mediante investigación especializada en materia informática

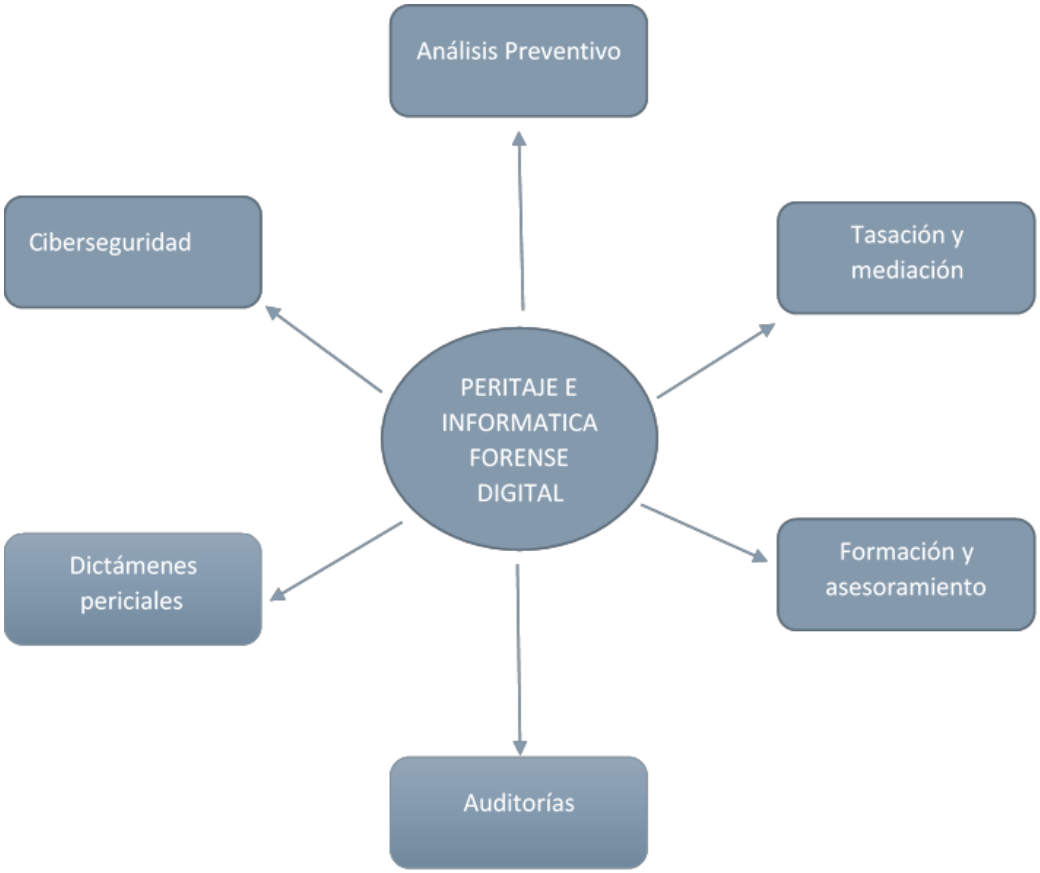
> en base a los requerimientos exigidos, dictamine con objetividad, honestidad, imparcialidad y veracidad, las conclusiones de su pericia mediante un informe o dictamen pericial. El resultado de su investigación es aportado en función de la localización de las evidencias digitales, las herramientas utilizadas para el análisis forense, los métodos y normas aplicadas y su desempeño como experto en la materia encomendada. La administración de justicia y abogados, están comprobando lo expeditivo e infalible que resulta la localización de las evidencias digitales, que sirven de apoyo para el esclarecimiento de los casos, por lo que contar con un perito informático forense puede ser vital para evitar o imputar una condena. (Sebastián Gómez, Evidencia Digital en la Investigación Penal, 2018)

Es indudable la importancia que tiene la función del Perito Forense Digital en la esfera de la investigación no importando el ámbito en el que se desenvuelva y es por eso necesario e imperativo invertir en la formación de profesionales de este campo, siendo interesante visualizar la función de este experto también en el área del arbitraje.

Es menester indicar que como parte de los postulados de la ética profesional del Perito Forense Digital residen los criterios fundamentales de la profesión en forma objetiva y apegada a las normativas y protocolos internacionales y también de conformidad a estatutos propios de la profesión, recordando que en el caso de Guatemala en algunas instituciones estatales como el Ministerio Público y el Instituto Nacional de Ciencias Forenses de Guatemala, existen algunos expertos que se desenvuelven en el campo de la Informática Forense, sin embargo vale la pena preguntarse qué código deontológico cumplen toda vez que en la mayoría de casos las profesiones de estas personas son de otra naturaleza y su Colegio Profesional dista de alguno que se refiera a la Informática Forense, en este caso se estima que los Peritos Forenses Digitales debieran estar adscritos al Colegio de Abogados y Notarios de Guatemala por ser el ente colegiado con mayor similitud de características que podría acoger a este grupo de profesionales dispersos, tomando en consideración la labor que realizan en el ámbito forense.

7.3. **Tipos de Informática Forense.** (Navarro Clérigues, 2015-2016)

Sostiene el autor Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos” que existe una clasificación de peritajes informático forenses de conformidad a la labor diaria que realizan, se presentan a continuación dos esquemas de su autoría, siendo los siguientes:



	Descripción	Actuaciones
FORENSE DIGITAL O TECNOLOGICO	El peritaje más relacionado con la tecnología. Se podría incluir el análisis forense en materia de ciberseguridad y peritaje judicial. Su objetivo es obtener evidencias digitales que se encuentran en dispositivos físicos o virtuales. Realizar el análisis forense en busca de indicios y aportar como resultado de su investigación un informe o dictamen pericial.	- Identificación y recopilación de evidencias. - Análisis forense de dispositivos IT. - Análisis de redes y su tráfico. - Análisis de la información y contenido. - Trazas y rastros de los ficheros. - Falsedad y manipulación de ficheros. - Recuperación y reconstrucción inf. - Tratamiento de imágenes y multimedia. - Ciberseguridad y hacking ético.
DE GESTIÓN O DE MANAGEMENT	Su objetivo es la obtención de la información, evaluación y constatación de la misma para poder establecer las relaciones y compromisos contractuales que se originan entre proveedor y cliente bien sean en los conceptos de proyectos, implantaciones de soluciones, productos o servicios, diseño y desarrollo de aplicaciones informáticas, la explotación de los sistemas, implementaciones de seguridad y estándares normativos.	- Gestión de la protección de datos. - Gestión de proyectos. - Explotación de los servicios. - Gestión IT *Governance*. - Gestión de categorías y roles. - Gestión contractual y de acuerdos. - Gestión de consultoría y soporte. - Propiedad intelectual e industrial. - Gestión de la seguridad informática.
TASADOR TECNOLOGICO	El objetivo de la tasación informática es valorar económicamente determinados activos informáticos, mediante distintas técnicas que incluyen el cálculo del retorno de la inversión para un proyecto informático, del esfuerzo en personas-meses invertido en la construcción de un proyecto software, del costo de determinadas licencias de software ilegalmente utilizadas, del valor económico de equipos informáticos teniendo en cuenta la antigüedad de los mismos y la inflación, etc.	- Estimaciones de daños y perjuicios. - Creación y fusión de empresas. - Compra de empresas y procesos. - Escisiones o disoluciones de empresas. - Liquidación de empresas a concurso de acreedores. - Estimación de inversiones. - Valoraciones internas de activos. - Auditorias contables. - Recapitalización de la empresa.
AUDITOR	Los principales objetivos de la auditoria informática son: - el análisis de la eficiencia de los sistemas informáticos, evaluando si hay carencias o si, por el contrario, están sobredimensionados. - la verificación de la existencia de unas mínimas pautas de protección de la información, tanto desde el interior, como desde el exterior. - la revisión de la eficaz gestión de los recursos informáticos, estableciendo mecanismos de control pasivos (prevención de ataques), y activos (capacidad resiliencia). - generar un balance de los riesgos en TI (Tecnologías de la Información). - realizar un control de la inversión en un entorno de TI.	- Auditoría de la gestión de la contratación de bienes y servicios. - Auditoría legal, cumplimiento LOPD. - Auditoría de los datos. - Auditoría de las bases de datos. - Auditoría de la seguridad de datos como disponibilidad, integridad, confidencialidad, autenticación y no repudio. - Auditoría de la seguridad lógica, referida a autentificación. - Auditoría de las comunicaciones. - Auditoría de la seguridad en producción, frente a errores, accidentes y fraudes.
MEDIADOR	La mediación puede permitir el realizar un acercamiento entre dos partes bajo un conflicto. Proporciona un ahorra de tiempo y costes a las empresas.	- Mediación en conflictos de programación de páginas webs. - Incumplimiento de servicios TI. - Incumplimiento de soporte técnico.

7.4. Informes Forenses.

En la lectura que hemos efectuado en los anteriores temas y subtemas hemos apreciado extremos importantes que se desarrollan en la informática forense, sin embargo, debemos indicar que todo el trabajo que realiza el Perito Forense Digital no tendría razón de ser si no se presentan los resultados, esto se realiza mediante la elaboración de informes que de conformidad a los protocolos y estándares internacionales podemos resumirlos en tres: Informe técnico, ejecutivo y mixto.

El informe técnico detalla todos los procedimientos, técnicas y métodos empleados por el Perito Forense Digital, es decir la parte técnica de todo el peritaje realizado, comúnmente cuando esto se presenta ante un juez, la mejor forma de someterlo al contradictorio será mediante el apoyo de un Consultor Técnico que tenga la expertiz para conocer y cuestionar los aspectos técnicos. El segundo que es el informe ejecutivo consiste en un resumen de todo el análisis realizado, así como las conclusiones a las que se ha llegado, este informe es presentado comúnmente para que los sujetos procesales puedan indagar y profundizar sobre la investigación realizada en donde ha sido objeto de análisis la evidencia electrónica y digital, es decir se presenta en una redacción clara y precisa para abogados, jueces, fiscales, etc. El tercer informe que es el mixto es una combinación del informe técnico y el ejecutivo.

El informe que se presenta no debe parecer que sea una demostración de las habilidades y capacidades técnicas del perito sino por el contrario éste debe dar respuesta a las cuestiones planteadas en el inicio de la investigación. La información recabada debe de justificar cuestiones relativas a la resolución del caso, se debe tomar en cuenta que el informe debe seguir una estructura documental claramente definida. En el contexto europeo la norma aplicada es la UNE 197010:2015 “Contenido mínimo de los informes periciales TIC”.

Desde la posición de Jeymy Cano en su obra “Computación Forense” refiere la estructura y contenido de un informe pericial forense digital, estableciendo lo siguiente:

1. Encabezado del informe que identifica, la fecha de entrega del informe, que se quiere hacer, número de identificación del caso, quienes participan, la clasificación del nivel de seguridad y los peritos participantes en la investigación.

2. Introducción, donde se detalla las características básicas del caso extraídas de los datos ofrecidos por las partes solicitantes. Se determina el alcance de la pericia que se adelanta, con el fin de limitar los análisis y exploraciones a lo que requiere para el caso particular.

3. Validación y verificación de la cadena de custodia, aquí se detalla y registra la evidencia con su formato de cadena de custodia, donde se describe, que se recibe, de quién, en qué fecha, las características de los elementos, sus marcas y modelos, números de serie, los nombres de los peritos que lo reciben, la identificación del caso.

4. Procedimientos de preparación y adecuación de la evidencia recibida, se describen los procedimientos relacionados con los dispositivos informáticos que se disponen para la copia del material recibido, las herramientas y programas utilizados para esta labor y posterior análisis, las verificaciones de las copias y el detalle del análisis que se va a realizar según lo descrito en la introducción.

5. Análisis de evidencias, aquí se realiza el análisis detallado de las copias de las evidencias, usando herramientas software y hardware validados y verificados en la fase anterior. Se detallan las técnicas utilizadas para identificar y extraer los datos de los dispositivos entregados para su análisis.

6. Hallazgos identificados, en esta sección se presenta lo relevante encontrado de la exploración de las evidencias y que sea relacionado con la investigación del caso. Se presentan tal y como se indica en las herramientas, sin análisis ni opiniones al respecto.

7. Conclusiones, aquí se describen los análisis de los hallazgos en el contexto de la investigación, basados en las formas científicas y técnicas que sean válidas por un tercero si así se requiere. Las afirmaciones que se hagan deben corresponder a lo que

la formalidad técnica establece, a las características de los dispositivos analizados y los hechos investigados en el caso.

8. Firma de los peritos, con la firma el perito refrenda y se hace responsable del contenido del informe o dictamen y todo lo que allí se encuentre. Conviene firmar con pluma especial y de color distinto al negro y en todas las hojas como medida de confiabilidad sobre el informe, por si un tercero quisiera alterar el contenido del mismo sin autorización. (Cano J. , 2009)

A propósito de completar el contenido que describe el autor Cano, a criterio personal sugiero que en el informe debe considerarse además: anexos, declaración de confidencialidad en el caso de una investigación en el ámbito privado, foliación de cada página, indicar la ubicación geográfica desde donde se realizó el informe y si fuese necesario consignar las coordenadas UTM (Universal Transverse Mercator) fecha clara y precisa de emisión del informe o dictamen pericial, las competencias y calidades de investigador, indicar los soportes en los que se adjunta el informe, de preferencia en Disco Compacto o en Blue Ray.

El autor Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos” sugiere aspectos importantes a incluir en el informe siendo los siguientes:

- Descripción del sistema de información analizado.
- Gestión de la cadena de custodia.
- Fecha y hora de intervención.
- Condiciones de funcionamiento del sistema.
- Medidas que se han tomado para salvaguardar el sistema de información.
- Procedimiento y documentación.
- Política de seguridad de la instalación donde está operando el equipo, incluyendo copias de seguridad.

- Identificación del personal con acceso al equipo, como mínimo el administrador el sistema.
- Topología de red, cortafuegos, NAT (Network Address Translation), VPN (Virtual Private Network), enlaces a internet, entre otros.
- Normativa aplicada en la instalación afectada. (Navarro Clérigues, 2015-2016)

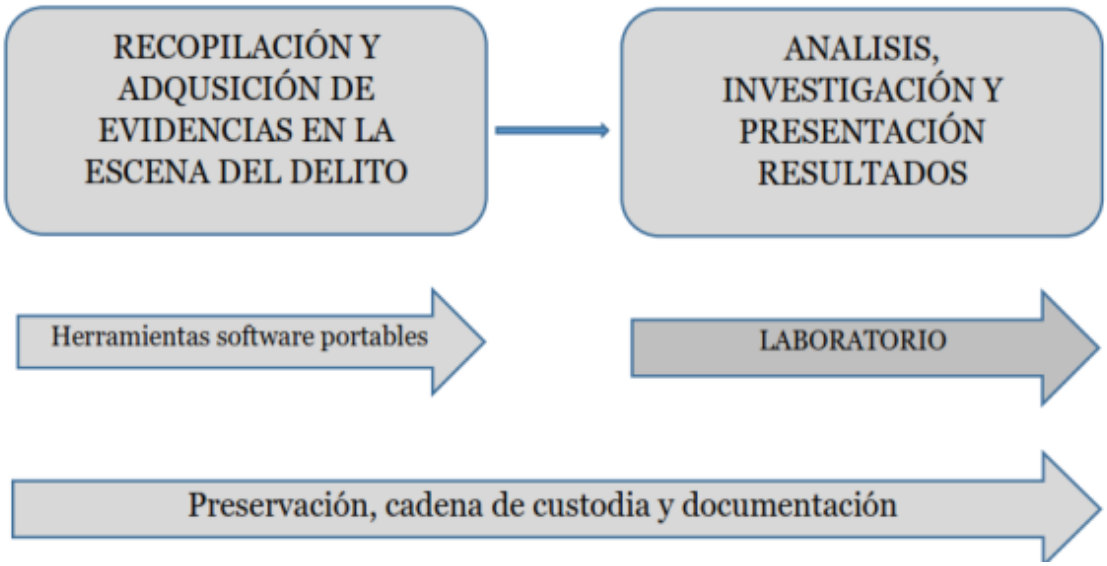
El autor ya referido también hace alusión a la autenticación del correo electrónico, destacando lo siguiente:

- Valorar la seguridad del mecanismo de firma electrónica del correo.
- Si no va firmado, hacer análisis de la cabecera o ver si existe un tercero con copia del mensaje.
- Cotejo de las cabeceras del correo electrónico con los históricos de los servidores utilizados.
- Informe del proveedor de internet, si procediera. (Navarro Clérigues, 2015-2016).

7.5. Herramientas de análisis forense digital y Laboratorio Forense.

Dentro del campo del análisis forense existen una gran diversidad de herramientas que nos ayudan a realizar diferentes tipos estudios a la evidencia electrónica y digital, hay herramientas físicas (hardware) es decir dispositivos en una gran variedad que son utilizados en el escenario criminal o en un laboratorio forense, este conjunto de dispositivos realizan diferentes tareas tales como extracción y análisis de información, seguimiento y ubicación de objetos y personas, filtración y segmentación de información, entre muchas más. También existen herramientas forenses consistentes en programas o software siendo estas herramientas fundamentales en el campo de la informática forense. Las herramientas forenses son utilizadas para analizar discos duros, memorias de almacenamiento, infraestructuras de red, software, móviles, portátiles, etc.

Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos” propone un esquema sobre las herramientas forenses siendo el que se presenta a continuación:



En la opinión de Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos” se usan diferentes herramientas forenses según sea el caso indicando además que:

> en la fase de adquisición de evidencias, la más crítica, se deben utilizar herramientas software portables, ejecutables desde unidades externas –DVD y/o USB- con el fin de no alterar la escena del delito por la instalación de aplicaciones forenses en los sistemas a analizar. Por otro lado, una vez recopiladas y custodiadas las pruebas, estas se analizan en el laboratorio forense donde se puede aplicar la tecnología hardware y software forense más sofisticado para la obtención y análisis de las evidencias extraídas. Así pues, tenemos software portable forense, y hardware tecnológico y suites de software o distribuciones utilizado en los laboratorios forenses por equipos de expertos. (Navarro Clérigues, 2015-2016)

Es importante mencionar que en el ámbito forense existe una innumerable cantidad de herramientas y que son utilizadas de conformidad a la naturaleza y especificidad del análisis. Siguiendo al autor Jorge Navarro él enlista algunas herramientas en una forma general, siendo relevantes por el aporte que nos da, siendo las siguientes:

a. Montaje y virtualización de unidades: Tales como Indisk, Osfmount, FTK Imager, live view, MountimagePro, Raw2mdk.
b. Análisis y adquisición de la memoria: Como ejemplo están Dumplt, Process Dumper, Responder CE, RedLine, Memorize, Volatility.
c. Recuperación y tratamiento de discos: PhotoRec, Scalpel, NTFS Recovery RS, Recuva, RaidReconstructor, Restoration, FreeRecover, R-Studio, IEF, Bulk Extractor Viewer, CNWrecovery, GuyMager, GParted, Unblock.
d. Análisis del sistema de ficheros: Tales como Analyze MFT, INDXParse, MFT Tools, MFT Parser, FileAssassin, WinHex.
e. Análisis del registro de Windows: Estan los programas RegRipper, Windows Registry Recovery, Shellbag Forensics, Registry Decoder.
f. Recuperación de contraseñas de Windows: Tales como Ntpasswd, Pwdump7, SAMInside, Ophcrack, l0phtcrack, ChromePass.
g. Utilidades de análisis de Red. Existen programas como WireShark, NetworkMiner, Netwitness Investigator, Network Appliance Forensic, Xplico, Snort, Splunk, AlientVault, Firebug.
h. Herramientas de análisis de amenazas y vulnerabilidades: Tales como PDF Tools, PDF StreamDumper, SWF Mastah, Captura Bat, Regshot, LordPE, OllyDbg, Jsunpack-n, OfficeMalScanner, SAS, ClamWin, Xteg, ProcessHacker.

i. Utilidades de análisis de dispositivos móviles y tablets: Tales como IphoneBrowser, IPhone Analyzer, Iphone-Dataprotection, SpyPhone. En el caso de sistemas Android está Android-locdump, androguard, Viaforensics, Osaf, Santoku. (Navarro Clérigues, 2015-2016)

Se advierte que en el campo del análisis forense digital se prefiere utilizar programas, paquetes, distribuciones o suites que sean comerciales y con licencia, sin embargo, en muchas ocasiones se utilizan distribuciones gratuitas que en tienen limitantes tales como el tiempo de uso o el acceso a determinadas funciones dentro de la herramienta de análisis forense. Las distribuciones generalmente funcionan como Live DVD y no altera ningún dato del disco duro o dispositivo de almacenamiento del equipo a analizar. Recordar que para realizar un análisis forense es fundamental no alterar las pruebas, en este caso los datos del almacenamiento interno. Por tanto, se montan todas las particiones de los discos en modo de sólo lectura, una medida fundamental para preservar los datos intactos.

En Guatemala hemos visto en los últimos años que los casos de índole penal han proliferado como instrumento u objeto el uso de dispositivos electrónicos y como consecuencia hay un gran campo que estudiar en el área de la evidencia electrónica y digital. Algunas empresas se han preocupado por estudiar y abordar estos temas, no así los diferentes actores del sector justicia quienes aún no han visualizado la gran responsabilidad que tienen en abordar este tipo de temas. Hoy en día existe una elevada demanda de servicios en informática forense, peritaje informático y auditorias seguridades y similares, causando que no solamente los cuerpos de seguridad y militar accedan a este tipo de información, sino por el contrario sea de conocimiento de más actores sociales y del sector justicia. Es necesario implementar laboratorios de análisis forense digital en el Ministerio Público como ente encargado de la investigación y persecución penal, tal y como lo he comentado en otras líneas el Instituto Nacional de Ciencias Forenses cuenta ya con un laboratorio de informática forense siendo por si insuficiente para cubrir a toda la República de Guatemala.

CAPITULO VIII

El Diligenciamiento, Ofrecimiento y Valoración de la Prueba Electrónica y Digital en Casos de Delincuencia Organizada.

Para abordar con propiedad este capítulo es necesario recordar algunos conceptos que nos ayudarán a comprender con mejor amplitud los contenidos de este apartado. Retomemos los extremos que estructuran a la Informática Forense.

8.1. Informática forense.

Dentro del área de la Informática Forense es importante recordar y destacar los fines que persigue, una de ellas es la recolección de la evidencia electrónica y digital, sin olvidar que también es fundamental para la persecución criminal y la creación de mecanismos para evitar y minimizar los daños causados por los cibercriminales. Es importante señalar que dentro de la ciencia de la informática forense se estudian los diferentes mecanismos para obtener la evidencia electrónica y digital, la generación de la huella digital a través de diferentes algoritmos tales como el MD5, SHA1, SHA256, SHA512, entre otros. No menos importante es apuntar que también en este tema de estudio se aborda la forma de preservar la cadena de custodia física y digital de la evidencia encontrada en un escenario criminal digital. Como lo apuntamos en otros capítulos uno de los principios rectores dentro de la informática forense se encuentra el principio de Locard que nos enseña que siempre habrá un rastro o huella al momento que exista contacto de un dispositivo, objeto o persona.

Un elemento que no puede obviarse es lo relativo a todas aquellas herramientas forenses que hacen posible una investigación adecuada y que son utilizadas por las unidades de inteligencia de investigación criminal, puedo citar al software de nombre *Encase* que es una herramienta que tiene varias funciones algunas de las destacas es la duplicación o clonación de un disco duro objeto de investigación, siendo este software confiable y seguro que salvaguarda la integridad de la información que está dentro del dispositivo objeto de análisis.

Otra herramienta muy útil y que ofrece seguridad y confiabilidad es el programa llamado FTK (Forensic Toolkit Access de AccessData) en virtud que dentro de sus bondadosas funciones se encuentra la recopilación de información de los dispositivos objeto de análisis mediante la aplicación de filtros eficaces, siendo además la herramienta recomendada para analizar correo electrónico.

Plantea el autor Di Lorio en su texto El Rastro Digital del Delito que:

> la Informática Forense es considerada una rama de las ciencias forenses que se encarga de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital. Es el uso de las Tecnologías de la Información para recuperar evidencia digital. Existen distintas fases y modalidades de actuación relacionadas con la informática forense que, a lo largo de un proceso penal, llevan a cabo expertos, investigadores y profesionales del derecho. Por ejemplo, la planificación previa, la identificación, recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital para ayudar a esclarecer y/o probar sucesos de naturaleza delictiva. Con el desarrollo de esta disciplina se ha trabajado sobre su principal objeto de estudio: la evidencia digital (…) Es de importancia destacar que los datos o evidencia digital siempre están almacenados en un soporte real, siendo este último de tipo físico, por lo que esta clase de evidencia podría considerarse igualmente física. (Di lorio. et al.)

El mismo autor explica que elementos pueden convertirse en evidencia digital, indicando algunos relevantes tales como:

> un archivo en un medio de almacenamiento, una línea de texto en un log de transacciones, el registro de acceso a un sitio web, datos en el registro de auditoría de una aplicación, datos de una ocurrencia en los registros de eventos del sistema (…) No sólo el contenido visible de un documento, sino también los metadatos, registros del

sistema y otras clases de evidencia digital, pueden ser relevantes para descubrir y/o probar los vínculos entre los distintos aspectos de un suceso. Ahora bien, los diversos rastros digitales que deja el contacto entre escena, víctima y victimario (intercambios en los cuales también interactúan otras variables, tales como momentos, instrumentos, objetos y consecuencias) requieren de un análisis complejo para poder reconstruir esta vinculación. La aplicación forense de la informática proporciona los principios y técnicas aplicables para identificar, obtener, analizar e interpretar la evidencia digital durante una investigación. La evidencia se convierte luego en elemento material probatorio cuando el perito la somete a examen, pues de manera separada, evidencia, dictamen pericial y testimonio del perito, serán cada uno, elemento material probatorio. La presentación de estos en audiencia pública ante autoridad judicial y contradicción de las partes será la prueba. (Di lorio. et al.)

8.2. La informática forense aplicada a la prueba electrónica y digital.

Para los profesionales del derecho y ciencias afines que día a día realizan diferentes roles o funciones en el ámbito forense guatemalteco no es un secreto que aún existen muchos desafíos por alcanzar en el área litigiosa y voluntaria cuando hablamos de evidencia electrónica y digital. Y es que debemos acotar de conformidad a la teoría de la prueba, si se desea demostrar la verdad de un hecho, de su existencia o inexistencia debe comprobarse de conformidad a lo que la ley establece. Y es que uno de los temas que ha generado mayor polémica es cómo establecer la validez de la prueba digital y electrónica. En forma reiterada he apuntado que uno de los objetivos de seguir los protocolos forenses en materia de evidencia electrónica y digital es llevar al juez la convicción de certeza y seguridad sobre las circunstancias acaecidas para que sea sometida la prueba al contradictorio correspondiente.

En los tribunales de justicia los jueces tienen una ardua labor al momento de verificar y calificar la prueba electrónica y digital que se les presenta ya que uno de los problemas que ocurre frecuentemente y se pone en tela de juicio es si la prueba

electrónica y digital se reviste de seguridad jurídica. Hoy en día en Guatemala se ha iniciado con la celebración de debates (materia penal) utilizando la videoconferencia como mecanismo auxiliar sin embargo debemos preguntarnos si en verdad existe en nuestro país un soporte jurídico confiable que permita valorar y calificar la prueba electrónica y digital.

Mi opinión y que sustenta la hipótesis de este trabajo, es que los jueces no cuentan con los instrumentos, técnicas y metodología que permita ilustrar de una forma correcta la veracidad de la información que en un primer escenario es presentado en forma electrónica (informática jurídica) tales como documentos electrónicos, firmas electrónicas y/o digitales, certificados electrónicos, entre otros y en un segundo escenario se presenta la evidencia electrónica y digital *per se* considerando que tampoco se tiene conocimiento de los estándares necesarios que debe cumplir esa prueba para que sea sometida al contradictorio y se le dé el valor probatorio correspondiente y en ese sentido el Ministerio Público no cuenta con los insumos necesarios para comprobar o acreditar su tesis fiscal en donde existe prueba electrónica y digital. Tanto en el primero como en el segundo escenario la fuerza probatoria es motivada en forma diferente por tratarse de aspectos de la informática forense y la informática jurídica. También es necesario agregar que muchas veces estos elementos probatorios son suficientes para acreditar hechos o circunstancias que tienen íntima relación con el caso sin embargo no se les da el valor probatorio que le corresponde y el juez toma alternativas para su valoración tales como tomarlo como prueba indiciaria o complementaria y aunque actúe un Consultor Técnico tal y como lo regula y faculta el Código Procesal Penal de Guatemala Decreto 51-92 del Congreso de le República, éste no es suficiente y muchas veces no se le da valor probatorio, siendo el desconocimiento o tergiversación de las reglas y estándares el mal de males y que es aplicada por los jueces e interpretada por fiscales y Abogados defensores en forma errónea.

Todo lo anterior ha ocasionado que los jueces en el ámbito penal de Guatemala, la gran mayoría de veces no fundamente sus resoluciones basadas en una prueba electrónica y digital como un medio de prueba autónomo siendo que únicamente

vinculan este tipo de prueba a otros elementos probatorios de diferente naturaleza o indiciario, causando con ello una nula eficacia y utilidad de la prueba electrónica y digital. Es preocupante esta situación en virtud de la proliferación en grandes proporciones del uso de la tecnología y que con ello ha venido aparejada la comisión de diversos hechos ilícitos en donde se utiliza a la tecnología como fin o medio.

Del comentario expuesto debemos considerar todo dispositivo de almacenamiento digital produce información y consecuentemente se convierte en material probatorio que de conformidad a las particularidades del caso concreto pueden servir como medio de prueba en un juicio y para llegar a esta fase es necesario agotar una serie de pasos que los mismos protocolos y estándares internacionales establecen con el fin de mantener en forma íntegra la evidencia electrónica y digital que después se convertirá en prueba.

En la práctica forense hay varias formas en las que se realiza este proceso de adquisición de evidencia electrónica y digital, siendo una de ellas las llamadas de bit a bit que consiste en un procedimiento forense en el que se realiza una copia exacta de un dispositivo de almacenamiento de información. En países como Colombia y España usan un procedimiento en donde interviene un Notario que da fe de todo el proceso en donde se hace constar el algoritmo Hash o el identificador técnico de la evidencia; además de este procedimiento se encuentra la opción de crear una imagen forense o clonaje de información del dispositivo que es un procedimiento a través del cual se copia en forma íntegra la información tal cual es de su original creando una copia idéntica de la información.

Montoya Rojas afirma en su obra “La informática forense como herramienta para la aplicación de la prueba electrónica” indica que:

> tanto los algoritmos HASH como la copia bit a bit son herramientas de la ciencia forense para analizar la información contenida en los dispositivos de almacenamiento y verificar que la misma no haya sufrido cambios sustanciales en el contenido. A pesar que los algoritmos busquen conservar la cadena de custodia y la copia bit a bit verificar la

> autenticidad de la información contenida en cualquier medio de almacenamiento, en estricto sentido, como ya se señaló, su objetivo, a luz del derecho, es servir de medio para garantizar o dar seguridad a los medios probatorios. (Montoya Rojas)

Existen elementos fundamentales para asegurar la integridad de la prueba electrónica y digital, siendo reflejados a través de una cadena de custodia digital respaldados mediante algoritmos. Este tipo de temáticas están llamadas a desarrollarse a los diferentes actores del sector justicia a fin de mejorar el conocimiento en el campo de la informática forense.

8.3. Valor Probatorio de los documentos electrónicos.

El derecho ha evolucionado a lo largo de la historia y es que ello tiene su fundamento en las diferentes corrientes doctrinarias que han marcado las legislaciones de los estados a nivel mundial, sin olvida además que las ciencias han ayudado a que los diferentes sistemas probatorios también evolucionen en forma gradual y de conformidad a los diferentes escenarios sociales y jurídicos. En varios capítulos de esta investigación hemos mencionado y hasta cuestionado la forma en que la tecnología, informática forense y el derecho informático ha incidido en las diferentes ramas del derecho, es menester entonces preguntarnos si el derecho informático y la informática forense ha cambiado el sistema probatorio de los diferentes estados del mundo.

Argumenta Julio Téllez en su obra “Derecho Informático” que:

> La teoría de la prueba se subordina a la teoría general del proceso, entendido éste como el conjunto complejo de actos, provenientes del Estado, de las partes y de terceros ajenos a la relación sustancia. De esta manera, es menester mencionar el debate en materia probatoria referente a la unidad o diversidad de procesos, para plantear igualmente la existencia de distintas pruebas (civiles, laborales, contenciosas, administrativas). Al respecto, es válido pensar que la prueba judicial es única, sin importar el área jurisdiccional donde se utilice, porque los principios universales que

rigen el proceso son también los que orientan la prueba. Por otra parte, la teoría de la prueba judicial no se limita de manera exclusiva a la temática de la prueba procesal, sino que está referida a consideraciones extra potenciales, técnicas y procedimientos. (Téllez, 2008)

Sigue manifestando el autor citado anteriormente que:

Existe una tendencia a identificar los conceptos de documento e instrumento o escrito, siendo esto consecuencia de que el Código Civil de Napoleón hace referencia sólo a los instrumentos o escritos, clasificándolos en públicos o privados. Pero dicha identificación es errónea, pues hay documentos no instrumentales que no son escritos, tales como dibujos, cuadros, fotografías, películas, etc., que son aceptados como medios de prueba. El concepto de documento es muy amplio, y comprende todos los objetos que pueden ser llevados ante un juez y que sirven de medio probatorio porque representan un pensamiento. En cambio, el instrumento es una variedad del documento; son aquellos escritos destinados a consignar una relación jurídica. Los hechos jurídicamente relevantes (materiales, en el sentido de transformación de la realidad, o inmateriales, como expresión de la memoria, la voluntad la inteligencia). (Téllez, 2008)

Teniendo en cuenta los argumento de este autor, se estima que la misma evolución de la sociedad exige ahora que los sistema probatorios de los diferentes estados incluyan dentro de su estructura aquello procedimientos que estudien, aborden e interpreten de mejor forma la prueba electrónica y digital utilizando para el efecto la ciencia de la informática forense y los protocolos internacionales en materia de evidencia electrónica y digital de los cuales existen numerosos estudios, todo esto para optimizar los beneficios que presenta la tecnología frente a los medios tradicionales de valoración de la prueba, esto de conformidad al principio ***favor probationem y las máximas del derecho probatorio digital***.

Tomamos la definición de Julio Téllez que en su obra “Derecho Informático” refiere que el documento electrónico:

> se alude a que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales y en que la actividad de una computadora o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales. El ejemplo más común lo constituyen los documentos especialmente construidos para el uso de las terminales de un sistema, como es el caso de las tarjetas magnéticas para acceder a las cuentas bancarias, vía cajeros automáticos. Técnicamente el documento electrónico es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que, sometidos a un adecuado proceso, permiten su traducción a lenguaje natural mediante una pantalla o una impresora. (Téllez, 2008)

Podemos concluir entonces que el documento electrónico es creado mediante un sistema informático cuya huella digital queda registrada en un dispositivo de almacenamiento interno o externo de información.

Sigue agregando Julio Téllez que

> existe una segunda especie de documento electrónico que surge cuando son impresos computacionalmente o provienen de un sistema informatizado, es decir que ha sido plasmado al papel o llevado a la pantalla de la computadora con información proveniente de un documento electrónico en sentido estricto. Bajo documento electrónico se consideran datos o informaciones que tienen relevancia jurídica, los cuales son transmitidos o registrados por vía electrónica, especialmente a través del

procesamiento electrónico de datos, pero también por medio de simples soportes de sonido. (Téllez, 2008)

En nuestro contexto guatemalteco cada día es más común que las diferentes instituciones gubernamentales manejen sus documentos en forma electrónica, utilizando para ello la figura del documento escaneado, obviamente también dentro de las instituciones del sector justicia actualmente se utiliza el acreditamiento de la información utilizando medios de almacenamiento de información tales como discos compactos, memorias flash, discos duros externos y otros. Cuando la información es voluminosa se utilizan las referidas técnicas sin embargo en un gran porcentaje carecen de valor probatorio y de seguridad jurídica. Por ejemplo, el uso de facturas, cheques y títulos de crédito que son faccionados mediante sistemas computarizados y éstos enfrentan el problema que cuando son llevados ante un juez no son valoradas de la forma correcta y es que existe el error que se utiliza un sistema de valoración de la prueba en forma tradicional y no incluyen en su apreciación el valor de los protocolos internacionales atinentes y aplicables la prueba electrónica y digital.

Es importante conocer algunos aspectos relevante para darle valor probatorio a los documentos electrónicos y es que en diferentes países del mundo la problemática es diferente en virtud que en los países en donde el uso de la tecnología se ha hecho más práctico y accesible ha sido menos confuso y problemático como el caso de los países nórdicos, Estados Unidos, Gran Bretaña y Alemania, además que en estos países predomina la libertad de la prueba, sin embargo en países como Francia, Italia y Bélgica ha sido más complejo en virtud que predomina la prueba escrita. Por ejemplo, en esos países con un sistema probatorio con mayor apertura el sistema bancario ha implementado el uso de microfichas que no son susceptibles de modificación. También se han implementado el uso de la telecopia en la que los originales quedan en manos de los titulares, mientras que las copias, como son más inalterables, pueden aportarse en niveles contenciosos o también aquellos provocados por la introducción de soportes irreversibles tratables por computadora.

Otro aspecto interesante que se ha utilizado es la digitalización, criptografía y la esteganografía. Existe una tendencia general es que en el caso de firmas deben ser reconocidas por la ley mediante instituciones o entes certificadores que den validez y autenticidad a las mismas. En Estados Unidos se implementó un sistema de doble clave o verificación que brinda mayor protección en el área de las transacciones en línea. También se ha utilizado el mecanismo de las llaves asimétricas en donde una es pública y la otra privada que permite al firmante mediante la llave privada, y al destinatario por la llave pública, respectivamente, verificar el origen y la integridad de uno o varios documentos informáticos.

Cita Julio Téllez del análisis de la legislación española, que

> el escrito en forma electrónica está admitido como prueba con igual fuerza que el escrito en soporte papel, bajo reserva de que pueda ser debidamente identificada la persona de la que emana, y que sea generado y conservado en condiciones que permitan garantizar su integridad. En el caso en que las partes convengan el uso de medios electrónicos, de cómputo o de telecomunicaciones para el envío, intercambio y en su caso confirmación de las órdenes y demás avisos que deban darse, habrá de precisar las claves de identificación recíproca y las responsabilidades que conlleve su utilización. Las claves de identificación que se convenga utilizar conforme a este artículo sustituirán a la firma autógrafa, por lo que las constancias documentales o técnicas en donde aparezcan producirán los mismos efectos que las leyes otorguen a los documentos escritos por las partes y, en consecuencia, tendrán el mismo valor probatorio. Se complementa la regulación al respecto ya que se establecen los lineamientos que deberán seguirse para la utilización de la firma electrónica, los mensajes de datos, los certificados electrónicos y los requisitos y obligaciones de los prestadores de servicio de certificación (PSC), adoptando básicamente los principios de la Ley modelo sobre firma electrónica.(Téllez, 2008).

En el caso de Guatemala debemos analizar la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Decreto 47-2008 del Congreso de la República que contiene los preceptos legales en materia probatoria de los documentos electrónicos.

8.4. La Prueba Electrónica y su Validez Procesal.

Corresponde ahora conocer algunas consideraciones importantes sobre el proceso de análisis forense que es también parte integra del recorrido que efectúa la evidencia digital electrónica y digital para llegar a ser presentada ante un juez competente como plena prueba. Un investigador forense en instante de tener a su vista la evidencia debe empezar a dar respuestas a las siguientes interrogantes: 1. ¿Qué se debe investigar? Es decir que pruebas deben buscar. 2. ¿Dónde? Es decir que dispositivos se analizarán (ordenador, celulares, sistemas, redes, etc) 3. ¿Dónde se cometió el delito? Para esto debemos verificar algunos aspectos como la fecha y hora local del dispositivo o elemento a analizar (horario UTC). 4. ¿Por qué? Es el objetivo o fin que se busca encontrar. 5. ¿Quién es el autor del acto o hecho que se investiga? Es ubicar a los responsables que en el mundo de la tecnología es una ardua labor. 6. ¿Cómo se llevó a cabo? Es determinar el procedimiento empleado para cometer el hecho o acto.

Debemos recordar las fases que estructuran un análisis forense digital, siendo las siguientes: a) Identificación del evento de seguridad o incidente. b) Recopilación de evidencias. c) Preservación de la evidencia. d) Análisis de la evidencia. d) Documentación. e) Presentación de los resultados encontrados.

Sostiene y explica a detalle el autor Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos” los pasos que componen el análisis forense digital, siendo así:

a) Identificación del incidente. Se debe informar al perito forense informático, lo más detalladamente posible, de los hechos, efectos producidos, escena del delito o entorno,

quién ha informado del incidente a las autoridades o responsables, como se ha detectado, etc.

b) Recopilación de evidencias. Se debe garantizar la recopilación de todas las evidencias, no perder ninguna es lo ideal. Acciones como: no apagar los equipos, identificar los dispositivos a recopilar, documentar el proceso, precintar todos los elementos objeto de análisis para su transporte, etc.

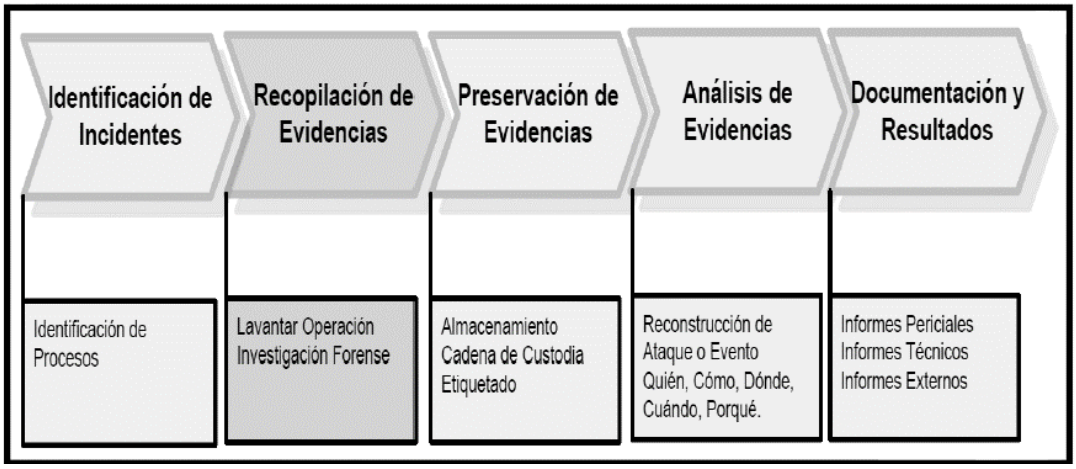
c) Preservación de la evidencia. Es la etapa en la que se adquieren las evidencias. Esta fase es muy importante. Cualquier error en la toma de evidencias podría echar por tierra la investigación o que las pruebas no sean admisibles ante un tribunal. Importante iniciar proceso de cadena de custodia.

d) Análisis. A la hora de realizar el análisis de la información recopilada hay que tener presente el tipo de incidente al que se dará respuesta. De esta forma se agiliza el proceso al fijar las evidencias objeto de un análisis en profundidad. Aunque nunca se debe caer en el error de descartar lo que nos pueda parecer obvio, hay que ser totalmente objetivos en todo el proceso.

e) Documentación y presentación. La documentación debe ser metódica, detallada y patente desde el principio del análisis. El archivo documental de la investigación debe contener, al menos: videos o fotografías del escenario y de las pruebas tecnológicas, control en la cadena de custodia de las pruebas y una bitácora con fechas y horas de las acciones realizadas sobre las evidencias. La presentación del informe o dictamen tiene que ser de fácil comprensión, donde se detalle objetivamente las conclusiones obtenidas y se explique claramente el proceso de obtención de las evidencias. No realizar juicios de valor ni afirmaciones que no se puedan demostrar. (Navarro Clérigues, 2015-2016)

Podemos apreciar que existe un orden en estas fases, sin embargo, debemos advertir que la fase de documentación debe realizarse en todo el procedimiento de análisis forense digital.

El autor citado presenta un diagrama sobre las fases del análisis forense digital, siendo el siguiente:



Agrega Jorge Navarro en su obra “Guía actualizada para futuros peritos informáticos” lo siguiente:

> se debe prestar especial atención a los procedimientos de recopilación y almacenamiento de las evidencias en la escena del delito y asegurar la cadena de custodia de las mismas. Aplicar métodos y pautas para que estas no se alteren a lo largo del proceso y que sean reproducibles por terceras partes en cualquier momento. Y seguir en todo el proceso las fases de análisis forense digital basadas un método normalizado. Para lograrlo, los peritos informáticos forenses basan sus investigaciones periciales y análisis forenses digitales, en normas y guías nacionales e internacionales publicadas al respecto, como RFC (Request for Comments), (Navarro Clérigues, 2015-2016)

a) *La función del Notario en la prueba electrónica y digital y relevancia en las actuaciones del Ministerio Público.*

En la legislación guatemalteca el Notario tiene una función importante en virtud de la investidura jurídica que el Estado le otorga mediante la Fe Publica que ostenta, es decir los actos en los que actúa a requerimiento de parte son respaldados con esa característica personalísima que es inherente a la función que desempeña el Notario. Se advierte que de conformidad a las funciones que rigen el actuar del Notario una de las conocidas ante el usuario final es la función ***asesora, autenticadora y legitimadora***, toda vez que la persona que acude ante los oficios de un Notario espera una asesoría personalizada de calidad y que se ajuste a sus necesidades, posteriormente la firma y estampa del sello del Notario da esa calidad y certeza jurídica al documento y que es plena prueba, no está por demás advertir que todo documento faccionado y autorizado por Notario puede ser redargüido de falsedad a través de los mecanismos legales correspondientes. Y es que si decimos que un documento puede ser atacado por alguna falsedad también lo es que los correos electrónicos, mensajes de texto, mensajes enviados por servidores de mensajería instantánea (WhatsApp, Messenger, Snapchat, Telegram, entre otros) también pueden ser objeto de alteraciones que consecuentemente sean falsos, esto último, al alcance mediante el uso de determinados programas, tutoriales en línea y un poco de tiempo.

Existen un sinnúmero de ejemplos de la forma en que la prueba electrónica y digital es manejada y usada en el ámbito forense. Que pasaría entonces si hablamos de un Notario si podría obtener prueba electrónica y digital en un caso que sea remitido para su conocimiento y los requirentes desean que se haga constar hechos y circunstancias o desean llegar a un arreglo extrajudicial. ¿Qué procedimiento o protocolo debe seguir el Notario? Esto nos demuestra que el ámbito de la evidencia electrónica y digital no solo se circunscribe a la esfera del Derecho Penal, sino que además es relevante y útil en otras ramas del Derecho.

Una de las propuestas que se plasman en uno de estos capítulos es lo relativo a la función esencial que podría tener el Notario en el contexto de la documentación de la evidencia electrónica y digital toda vez que si el Notario actuara en el escenario criminal

se revestirían como auténticos varios actos, sin embargo acá es donde entra en discusión y ponderación la fe pública notarial y la fe administrativa que poseen los empleados y funcionarios del Ministerio Público que procesan y tratan la escena criminal y consecuentemente la evidencia electrónica y digital, este es un punto que sé que dará mucho de qué hablar en un futuro no tan lejano.

Cuando se escucha el término “prueba electrónica” se visualiza un sinnúmero de dispositivos electrónicos con computadoras y varios cables conectados entre sí, sin embargo debemos mencionar a la prueba digital que también es relevante en un análisis forense en virtud que si la conceptualizamos podemos decir que ésta es un rastro o registro que queda después de haber utilizado un dispositivo electrónico (computadora, teléfono celular, dron, memorias USB, cámaras de seguridad, servidores de datos, tarjeta de crédito, entre otros). Es por eso que no solo debe concebirse el termino prueba electrónica y digital en lo procesal, sino también en el ámbito privado; advirtiendo además que si nos referimos a prueba electrónica debemos comprender que se refiere específicamente a los dispositivos electrónicos, no obstante, aclarado esto, diferentes autores mezclan ambos términos, pero técnicamente es diferente referirnos a prueba electrónica y prueba digital

Son diversas las posturas que se conciben y que explican el concepto de la prueba electrónica y digital. Por ejemplo, dentro del medio forense guatemalteco se utiliza el termino electrónico en diferentes escenarios, tal es el caso de diversas instituciones que han implementado sistemas, mecanismos y controles electrónicos con el fin de agilizar diferentes procedimientos que proveen beneficios en costo y tiempo al usuario final. En sentido más restringido, ponemos como ejemplo el actuar del Notario y de los funcionarios judiciales que expiden documentos y que en algunos casos en lugar de extenderlo en formato físico lo remiten a donde corresponde en formato electrónico almacenado en soportes como un disco compacto o un DVD. Como primer escenario, debemos reflexionar que al hablar de un documento electrónico es porque lleva implícito una firma electrónica, misma que de conformidad a la legislación guatemalteca y estándares internacionales tiene fuerza probatoria. Un segundo escenario en donde sale a relucir el termino electrónico en relación al medio forense es cuando se pretende

conocer la verdad histórica de un hecho en donde existen diversidad de indicios electrónicos que mediante un procedimiento adecuado podremos hablar en su momento de prueba electrónica y que estos por si mismos no pueden concebirse o encuadrar como un documento electrónico, sino por el contrario deben tener una característica determinada para ser validos ante un juez competente y tener la fuerza probatoria correspondiente.

Tomaremos la explicación que hace Ricardo Oliva y Sonsoles Valero en su obra "La Prueba Electrónica", enfatizado que en materia informática la prueba pericial es la practicada por un perito, que es aquel que, debido a sus conocimientos especializados en una materia, está en una posición adecuada para aportar conocimientos técnicos que el Juez no posee, y emitir un dictamen sobre unos hechos que permiten a éste valorar adecuadamente el objeto de la pericia" (Oliva. et al.)

Evidentemente el perito debe tener las calidades legales y técnicas para que puedan actuar dentro de un juicio; por ejemplo, podemos citar en lo que para el efecto establece el artículo 174 del Código Procesal Civil y Mercantil, indicando que (…) las partes y sus abogados podrán concurrir a la diligencia de reconocimiento y hacer de palabra al juez las observaciones que estimen oportunas. El juez y las partes podrán hacerse acompañar por peritos de su confianza, los que en el acto del reconocimiento podrán exponer sus puntos de vista verbalmente, si fueren requeridos por el juez.

En la prueba digital como elemento probatorio en sentido lato, debe revestir de todas las calidades y requisitos para que pueda ser valorada por juez competente y dicha prueba acreditará o desacreditará un extremo de esa verdad histórica o material que se busca, además debe haber pasado por el análisis de un experto o perito que indique que dicho material probatorio se encuentra conservado en forma íntegra, no ha sido alterado o modificado su contenido. En cambio, la prueba documental, en sentido estricto, es utilizada para documentar un hecho, como por ejemplo una entrevista, un acta notarial, una inspección ocular documentada en acta ministerial.

Es de conocimiento público que, de conformidad a la organización del Ministerio Público, existen diferentes roles que se desarrollan encaminadas a la persecución

penal y la investigación de los delitos de acción pública. Dentro de esta estructura se encuentra la función del Auxiliar Fiscal quien es quien tiene la carga de la investigación preliminar y a cargo la etapa preparatoria del proceso penal, no obstante, sabemos que en la realidad están sobrecargados de trabajo y hasta resultan efectuando funciones que compete a los superiores en la jerarquía.

La función de Auxiliar Fiscal es de agotar todos los medios de investigación necesarios para considerar llevar ante juez competente su requerimiento fiscal que podría ser una citación o aprehensión para que el sindicado se presente a solventar su situación jurídica ante juez competente. Pero es interesante que dentro de la investigación que realiza el Auxiliar Fiscal se enfrente con una diversidad de asuntos complejos en materia informática tales como limitación de recursos para procesar un escenario criminal digital, carencia de herramientas e insumos para ordenar el resguardo de la evidencia electrónica y digital, falta de preparación sobre temas de análisis forense digital, todo lo anterior conlleva a una deficiente labor que no es deducible al Auxiliar Fiscal o en su caso al encargado de la Dirección de Investigaciones Criminalísticas, por el contrario ellos realizan la función de la mejor forma y el problema radica en las autoridades pertinentes. No hay que dejar por un lado la importante función que tiene un Agente Fiscal que es quien además de guiar y orientar la función del Auxiliar Fiscal, también se encarga de litigar los casos en la etapa intermedia y la etapa de debate oral y público según las funciones que le son inherentes de conformidad a la Ley Orgánica del Ministerio Público y que también es necesario advertir que debe tener un conocimiento básico en temas de informática forense y el tratamiento de la evidencia electrónica y digital.

b) *La interrelación de la prueba electrónica y la informática jurídica.*

En pleno año dos mil veinte a raíz de la coyuntura de la pandemia que el mundo sufre a gran escala se ha visto que diferentes países han implementado estrategias para dotar de justicia en los diferentes casos y ámbitos del Derecho, Guatemala no es la excepción y se ha visto que la Pandemia declarada por la Organización Mundial de

la Salud ocasionada por el COVID-19, siendo esto una enfermedad altamente contagiosa y expandida en todo el mundo. Atendiendo a eso las diferentes naciones del mundo tomaron diferentes estrategias de contención y otros en forma de reacción para atender esta enfermedad. Dentro de estas estrategias se encuentra la cuarenta voluntaria o dependiendo del contexto sanitario se implementó en forma obligatoria, evidentemente tendientes a la limitación al derecho a la locomoción, asociación, entre otras con el objeto de preservar la salud de las personas. Sin embargo, hay circunstancias que no deben obviarse; en el caso de Guatemala debemos hablar sobre el funcionamiento del aparato estatal específicamente en el sector justicia, que en este contexto es diverso, complejo y con protocolos de actuación improvisados y que en el transcurso de la implementación de éstos se llega a un intento de corrección o en otros casos más afortunados, es certero.

En Guatemala las diferentes judicaturas de diversa competencia han tomado algunas medidas como lo es el cierre de los juzgados hasta nuevo aviso, en otros es el trabajo de atención al usuario por turnos; algo que debe llamar la atención es la forma en que se atiende la justicia penal ya que a la fecha se atiende al usuario en los Juzgados de Paz Penal o de Instancia Penal cuando existe un caso en flagrancia o para una primera declaración, consecuentemente el sindicado es puesto a disposición ante la judicatura para que sea escuchada y solvente su situación jurídica. Surge la interrogante entonces: ¿Qué otros mecanismos implementan el Organismo Judicial para atender las audiencias orales en materia penal? Podría sugerir el lector que, dependiendo de la naturaleza y etapa del proceso, podría utilizarse el sistema de videoconferencias, sin embargo, el uso de esta opción se limita a ciertas circunstancias, las cuales veremos más adelante. Es menester entonces conocer cómo se ha implementado la tecnología en los sistemas de audiencias orales en otros países conociendo la diversidad de mecanismos implementados para cumplir los principios generales del derecho y las diferentes garantías del proceso penal.

El sector justicia tiene en un panorama diverso que le presenta una serie de motivaciones para implementar en mayor medida la tecnología para atener los diferentes asuntos tales como acceso e información sobre expedientes, funcionamiento

de la instituciones, análisis de casos, tramitación o diligenciamiento de causas o en forma general propiciar una buena organización del trabajo y aumentar el rendimiento de sus funcionarios con la ayuda de las TIC (Tecnologías de la información y comunicación).

Es evidente que el uso de herramientas tecnológicas propicia un ahorro de tiempo y trabajo, los usuarios también se benefician en el tratamiento de sus casos facilitando el acceso a la justicia favoreciendo a la población especialmente a aquellos sectores más vulnerables. Podemos inferir entonces que la tecnología propicia una mejor gestión y desempeño de las instituciones del sector justicia y además crea un canal de comunicación eficiente entre el sector judicial y otras instituciones. En Latinoamérica se debe propiciar la modernización tecnológica para atender la justicia penal creando otros mecanismos que faciliten la tramitación de las causas penales y con ello el respeto los derechos y garantías de los procesados y víctimas del delito.

Citamos el ejemplo de Finlandia, que posee una base de datos automatizada destacable por sus capacidades de comunicación, que contiene de manera virtual toda la información importante respecto a cada acción o causa ingresada al tribunal, incluyendo las particularidades de las partes, la naturaleza y monto de la demanda, el documento ingresado y el resultado de las audiencias, entre otros. Holanda, país pionero en la adopción de las TIC en su poder judicial y que lo sigue siendo hasta el día de hoy, ha sido un líder tanto en el uso interno de tecnologías para brindar apoyo a la administración del tribunal y a jueces, como en su uso para el intercambio de información entre los tribunales, las partes y el público general. Ambas facetas son parte de un sistema integrado que brinda soporte a un Poder Judicial inalámbrico, donde desde el inicio hasta la decisión del caso, este es manejado a través de sistemas electrónicos

Surge entonces el cuestionamiento si es viable utilizar las videoconferencias en audiencias de diversa naturaleza en un sistema penal acusatorio en donde prevalece la oralidad esto tomando en consideración los principios de inmediación procesal, igualdad de armas, audiencia, tutela judicial efectiva, juez natural, entre otros. Nos enfocaremos en el principio de inmediación que de conformidad a diferentes postulados

debemos analizarlos en las siguientes esferas: proximidad entre juez y las partes procesales, intermediarios y la bilateralidad.

Son relevantes dos tipos de inmediación siendo estas: “la pasiva que supone la posibilidad del juzgador de percibir directamente la pruebas, por ejemplo, la declaración de quien depone en el proceso, pero sin poder intervenir; y la activa, que consiste en la percepción e intervención directa en el conocimiento de las pruebas por parte del juzgador, en especial en la intervención de los sujetos procesales a los fines de interrogarlos, aclarar dudas y conducir el debate.

Es necesario determinar si el hecho de que el declarante se encuentre distante del juzgador, lo cual, por una parte, descarta el requisito de la proximidad, ya que no se rendirá la declaración directamente ante él sino a través de una pantalla y la voz será reproducida mediante un sistema de sonido. Para que exista inmediación es necesario que el juez y quien declara estén ubicados cerca del otro para que la declaración pueda ser percibida por el administrador de justicia directamente y —aquí surge el segundo aspecto— sin intermediarios, de manera que el tribunal pueda formarse una decisión de la observación y escucha del propio declarante, de "primera mano" y no tergiversada por la representación que pudieran efectuar terceras personas o cosas. En consecuencia, se requiere que juez y declarante estén cerca para observar y escuchar directamente lo que sucede, cómo sucede y dónde sucede, pues ésta es la forma habitual como las personas se relacionan, pero ocurre que la misma percepción personal e inmediata puede generarse mediante la videoconferencia. Es decir, si se interpreta el principio la inmediación procesal atendiendo a los avances tecnológicos que se van produciendo, será posible la evacuación probatoria en garantía del referido principio, dado que esta tecnología constituye un medio para acercar en tiempo real a personas alejadas geográficamente y así permitir su interacción audiovisual, que es en definitiva lo que inspira al principio de inmediación. Es necesario emitir un juicio en este sentido toda vez que el tema de proximidad puede evaluarse en forma objetiva y subjetiva en virtud que el medio tecnológico facilita este espacio de interacción, esto queda a un análisis más profundo para el lector. Debemos recordar que en el caso de Guatemala son permitidos los medios audiovisuales de conformidad a la reforma

efectuada por el Decreto 17-2009 del Congreso de la Republica específicamente por el artículo 17.

En Brasil se utiliza la videoconferencia en los procesos penales para el interrogatorio de los procesados privados de libertad. En el caso de España existe una regulación legal que establece e impone a los Juzgados y Tribunales y a las Fiscalías la utilización de cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones, con las únicas limitaciones que procedan de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales y las demás leyes que resulten de aplicación. También se establece la plena validez y eficacia de los documentos originales emitidos por tales medios informáticos o telemáticos, siempre que quede garantizada su autenticidad e integridad y se cumplan los requisitos exigidos por las leyes procesales. También hace alusión al llamado Juez de Instrucción quien refiere en el marco de atribuciones acordar, de oficio o a instancia de parte, que las comparecencias personales que ante él hubieren de realizar investigados o encausados, testigos, peritos o de cualquier otra persona que hubiere de hacerlo en calidad distinta, se lleven a cabo mediante videoconferencia o por cualquier otro sistema similar que garantice la comunicación bidireccional y simultánea de la imagen y el sonido, siempre que concurrieren circunstancias especialmente gravosas o perjudiciales, o se aprecien razones de utilidad, seguridad o de orden público.

El sistema judicial guatemalteco tiene un escenario positivo en plano de las tecnologías de información y comunicación (La Videoconferencia en Guatemala) y que debe aprovecharse para motivar y propiciar la inclusión de modelos de reformas tecnológicos en materia penal, sin embargo debe observarse que debe existir una política integral que incluya, entre otras cosas, una capacitación constante a los diferentes actores del sector justicia a efecto de que estén actualizados, un sistema de seguridad informático fiable que garantice a las diferentes judicaturas que el expediente electrónico y digitalizado no será objeto de manipulación o ataques internos o externos, el uso de un sistema de gestión de casos judiciales, ministeriales o de procedimientos confiable que este adaptado a las necesidades de las judicaturas y esté

estructurado de una forma sencilla, gráfica y con manuales de apoyo al usuario; es importante resalta que el uso de las videoconferencias está regulada en el Código Procesal Penal guatemalteco en el artículo 218 Bis y 218 Ter inclusive. Sin embargo, se enfoca hacia el testigo, perito o colaborador eficaz. Sería interesante evaluar la actuación del Abogado defensor, el Fiscal, Querellante Adhesivo y el sindicado a través de una videoconferencia.

Como se ha apreciado en otras legislaciones el uso de esta tecnología se ha extendido a otros sujetos procesales en virtud que se han superado las condicionantes que limitan la actuación de éstos; por ejemplo, de un Abogado defensor por videoconferencia o una primera declaración de un sindicado que está distante al juzgado que ha emitido una orden de aprehensión o citación o un Fiscal que tenga limitación insuperable para trasladarse de un departamento a otro para evacuar una audiencia. Vemos acá que debe efectuarse la ponderación de los derechos y fundamentalmente la protección a los derechos humanos. Temas de logística e instalaciones, recurso humano, conexión de alta calidad y reformas integrales a nuestra normativa adjetiva pueden ser elementos de un escenario que facilitaría y agilizaría con gran medida la gestión y atención de casos en el organismo judicial y con ello alcanzar la justicia pronta y cumplida.

La democracia política tiene algo esencial, pues se basa en el respeto en el valor de la dignidad de las personas y de los Derechos Humanos, se realiza y se legitima por procurar la participación efectiva todos los ciudadanos a través de todas las organizaciones para crear propuestas públicas, por la búsqueda del debate, la discusión y el consenso en la formación de la voluntad general y por garantizar las libertades, diversidad de opiniones y el consenso.

Una postura interesante que ocurrió en el Derecho comparado fue lo relativo una notificación telemática en el cual refería que debía estar en posesión de los medios telemáticos para recibir dicha notificación y se establecía la presunción de certeza en los servicios de sellado de tiempo electrónico y entrega electrónica certificada generados por Prestadores Cualificados de Servicios de Confianza (QTSP por sus siglas en inglés), herederos del Prestador de Servicios de Certificación. Se advertía que

los sellos cualificados de tiempo electrónicos disfrutarían de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas y que este tipo de sello emitido en un Estado miembro sería reconocido como sello cualificado de tiempo electrónico en todos los Estados miembros.

De la lectura anterior podemos inferir que los datos enviados y recibidos mediante un servicio cualificado de entrega electrónica certificada se visualiza como una base para la presunción de la integridad de los datos.

c) *Ejemplos de valoración de la prueba electrónica en el derecho comparado.*

Definen Ricardo Oliva y Sonsoles Valero en su obra La Prueba Electrónica, Validez y Eficacia Procesal.

> En definitiva, la valoración de la prueba – también en el ámbito digital – es prerrogativa del Juzgador y, por mucho que incomode fuera del sector jurídico, en Derecho dos más dos no siempre suman cuatro. Del mismo modo que un acta notarial de manifestaciones no es prueba plena respecto de la veracidad de los hechos manifestados, no puede pretenderse que la intermediación de terceros de confianza, el informe pericial o el certificado emitido por un QTSP hagan prueba plena de todos los hechos en litigio; y sí y sólo de aquellos sobre los que los terceros, los peritos o los QTSP´s tienen el absoluto control… Fallo condenatorio por amenazas tomando como base la visualización de un WhatsApp en el terminal móvil de la víctima. Sin duda el amable lector, con un alto grado de conocimiento tecnológico, se lleve las manos a la cabeza; y también me las llevaría yo si la visualización de una conversación de WhatsApp fuera el único elemento probatorio tenido en cuenta a la hora de emitir el Fallo. No obstante, si el juzgador, que ha visto y hablado con la víctima de 70 años, llega a la conclusión razonada de que ésta carece de los conocimientos técnicos y/o de la picaresca necesaria para falsear la prueba la cosa cambia. Dicho lo cual ¿que la prueba electrónica es más fácilmente

falseable que la analógica? Probablemente. ¿Que la prueba pericial y/o el testimonio de un tercero de confianza en materia contractual refuerzan la validez de la prueba electrónica? Sin duda. ¿Que la certificación de un Prestador Cualificado de Servicios de Confianza goza de presunción de certeza? Indiscutible. Pero también, que del mismo modo que viene ocurriendo a lo largo de los siglos en el mundo analógico, en el ámbito digital hay sitio para la falsedad y el fraude; y la responsabilidad, en estos casos, es única y exclusivamente del autor del mismo (…) un acta notarial sobre el contenido de una página web en fecha determinada. Con variantes de estilo un acta de estas características podría decir, por ejemplo: "Don Jacinto X Y, se persona en mi notaría y me requiere a mí el notario para que acceda al sitio web http://www.elsitioweb.com y levante acta incorporando el contenido de la misma. Yo el notario accedo a la citada dirección de Internet y realizo 10 impresiones de pantalla con el contenido del sitio web, las cuales incorporo a esta acta en tantos folios de papel notarial, numerados…" Cuando Don Jacinto acuda a los Tribunales con su acta notarial que goza de fe pública pueden ocurrir dos cosas: que el perjudicado por la prueba sepa que es cierta y se allane a la demanda de Don Jacinto. 2ª.- Que el perjudicado por la prueba sepa que NO es cierta y trate de desvirtuar la prueba de Don Jacinto y presente prueba en contrario. En el segundo supuesto el demandado no lo tiene demasiado difícil a partir de prueba pericial especializada, porque el Notario autorizante – que no puede comprobar la veracidad de la información que le muestra su navegador – de lo único que dará fe es de que escribiendo en su navegador la dirección de internet que le ha informado Don Jacinto él ve determinada información, la imprime y la incorpora al acta notarial; pero otra cosa es hablar de veracidad del contenido con exclusión de phishing, man in the middle (…) Porque los seres humanos (y los notarios, hasta donde yo sé, lo son :)) no podemos percibir por nuestros sentidos las transacciones que se producen entre un equipo local y las páginas de Internet. También puede ocurrir que, quien haya de

resolver el litigio entre Don Jacinto y el demandado carezca de los conocimientos informáticos básicos y no confíe en la pericial contradictoria, aferrándose al concepto fe pública como un mantra. Podría haber quien llegados a este punto pudiera pensar que si Don Jacinto, a pesar del acta notarial, no ve reconocidas sus pretensiones tiene una acción de responsabilidad contra el notario. Nada más lejos de la realidad. El notario ha hecho su trabajo (…) sólo que su trabajo no era lo que necesitaba Don Jacinto o sí, si había actuado con picardía. En el ámbito de la prueba digital, como cuando nos referimos a la prueba analógica, los Tribunales entrarán a valorar cualquier prueba válida en Derecho. Es labor de los letrados conocer cuando se precisa cada prueba; sola o en combinación con otros medios probatorios no necesariamente digitales. (Oliva. et al.)

Sigue ilustrándonos de ejemplos los autores antes citados y nos presentan el siguiente ejemplo:

Supongamos que alguien encuentra una vulnerabilidad de tipo XSS (Cross-site scripting) en un periódico digital, por ejemplo, en 'El País'. Este tipo de vulnerabilidades son bastante curiosas y se basan en la posibilidad de abusar de partes en las que el usuario puede insertar contenido y que luego es usado posteriormente para construir una página web. Normalmente la idea del programador es, por ejemplo, poner un apartado de comentarios en una noticia donde espera que la gente escriba texto 'normal'. Pero ¿y si alguien mete contenido HTML? Respuesta: Tenemos un problema, y si encima añade contenido JavaScript, entonces esa vulnerabilidad puede ser abusada para crear una nueva página web que nada tenga que ver con la original. Por poner un ejemplo, hablemos del famoso Mr. Bean en la página web de la presidencia española de la UE. Muchos medios tacharon ese incidente de 'Hackeo' y vendieron el asunto como si hubiese sucedido una intrusión. Pero no era así. Se trataba de una

vulnerabilidad de tipo XSS que nada tiene que ver con una intrusión. Siguiendo con el ejemplo anterior, tenemos un periódico digital y ahora vamos a suponer que alguien encuentra una vulnerabilidad de tipo XSS que le permite crear contenido totalmente ajeno al del periódico usando, por ejemplo, el espacio de comentarios que tiene cada noticia. Y como este atacante tiene mucho sentido del humor, crea una página paralela en la que se da por noticia una supuesta relación sentimental entre Pablo Iglesias y Albert Rivera. Le añade un fotomontaje y la publicita por Twitter con un tweet tal que así: 'Asco de periodismo' http://enlace-que-te-lleva-a-elpais-con-contenido-que-no-es-de-elpais Ese tweet se viraliza y alguien decide tomar cartas en el asunto. Va a un notario y le piden que levante acta de lo que hay ahí. El notario, muy versado en transmisión de patrimonio, pero bastante lego en informática, levanta un acta demoledora. Podemos llevar a juicio a El País por intromisión al honor y el juez, que tiene mucha confianza en el Notario, condena al periódico digital ya que la noticia, según la evidencia, existía y es claramente una falacia. Ahora pensemos en otro escenario diferente. Existe esa acta notarial, pero en paralelo, El País se pone en contacto con nosotros y nos pide que certifiquemos tanto el contenido de la web (el pantallazo) como el código fuente de dicha web. En la evidencia digital que El País tiene en su poder, es perfectamente auditable 'donde está la miga' y deja muy a las claras que nadie en la redacción de dicho medio ha tomado partido directamente en la supuesta noticia. El juez valora el acta del notario, que da fe del contenido, y en paralelo valora la prueba pericial de la que dispone El País que desvela claramente que un usuario malintencionado ha abusado de su web y que en realidad el contenido ofensivo es totalmente ajeno al medio periodístico. El juez absuelve al periódico e inicia diligencias para localizar a la persona para hacerla responsable tanto del daño a los políticos como al medio digital. (Oliva. et al.)

Después de analizar los ejemplos ya citados debemos reflexionar sobre la función que tienen los sujetos procesales en un juicio, recordemos que le Ministerio Público debe realizar su función con objetividad y de conformidad a la ley, misma que le faculta entre otras cosas a aplicar el principio de oportunidad, además de implementar otro tipo de procedimiento dependiendo de la gravedad del delito y no obstante no pudiese aplicarse algún beneficio o darle una salida procesal al asunto, en juicio debe ponerse en práctica el principio de proporcionalidad de la penas en caso sea sentencia y sea cosa juzgada el caso de una persona ya enjuiciada. No está por demás apuntar que el juez debe emitir una sentencia de conformidad a la sana crítica razonada y fundamentada. Recordemos además que existen ciertas exigencias legales que condicionan la actuación de los sujetos procesales y que limitan la validez y la eficacia probatoria de los medios de prueba aportados y esto se encuentra regulado del artículo 181 al 186 del Código Procesal Penal de Guatemala.

Siguen aportando Ricardo Oliva y Sonsoles Valero en su obra La Prueba Electrónica, Validez y Eficacia Procesal más ejemplos reales que nos ilustran como funciona en la práctica la valoración de la prueba electrónica, indicando que:

> 1. El marido, con el fin de acreditar la relación adúltera que su mujer mantenía con otro hombre, aportó como medios de prueba mensajes de SMS intercambiados por su mujer con su amante desde el teléfono móvil de aquélla, y fotografías y mensajes de textos obtenidos de la red social Facebook. Tales mensajes, inequívocamente, acreditaban diálogos e intercambios de afectuosidad, palabras amorosas y claras referencias a una común sexualidad entre dos personas entre las que había una relación íntima en curso. La mujer cuestionó la licitud de tales medios de prueba alegando que habían sido obtenidos vulnerando su derecho fundamental a la privacidad. El Tribunal italiano dio la razón al hombre indicando que no puede considerarse ilícito el descubrimiento casual del contenido de los SMS, aunque sean personales, fácilmente legibles en un teléfono móvil dejado en un espacio común de la casa familiar.

2. Un trabajador utiliza el correo corporativo de su empresa para revelar y filtrar a terceros datos empresariales reservados. Posteriormente, el empresario accede a la cuenta de correo del trabajador a través del ordenador que utilizaba en el centro de trabajo, descubre la revelación no autorizada de secretos empresariales, y procede a despedir al trabajador. Si consideramos que la intervención del ordenador del trabajador por parte del empresario constituye un caso de intromisión ilegítima en el ámbito de protección del derecho fundamental a la intimidad (…) la aportación del correo electrónico no debería ser admitida por como prueba válida ante un tribunal (ya que, por haberse obtenido vulnerando el derecho a la intimidad del trabajador, se consideraría una prueba ilícita). Los casos mencionados aluden o se refieren a la doctrina denominada teoría de los frutos del árbol envenenado que sostiene que todo resultado probatorio generado a partir de un medio de prueba ilícito -porque vulnera derechos y libertados fundamentales, o porque implica la realización de una actividad prohibida por la ley- adolece de nulidad insalvable y afecta a todos aquellos medios de prueba relacionados y derivados a partir de dicho medio de prueba. (Oliva. et al.)

d) *Consideraciones para el tratamiento y valoración de la prueba electrónica. (Los pantallazos o captura de pantalla)*

Siguen aportando Ricardo Oliva y Sonsoles Valero en su obra La Prueba Electrónica, Validez y Eficacia Procesal, algunas consideraciones importantes:

Por tanto, a la prueba electrónica le serán aplicables las reglas procesales generales sobre actividad probatoria, medios de prueba y resultado probatorio (…) El tiempo establecido para la proposición y aportación de la prueba electrónica debería ser el más temprano posible a fin de asegurar la cadena de custodia, vale decir, a fin de garantizar la autenticidad, inalterabilidad e indemnidad de la prueba electrónica. La admisibilidad de la prueba electrónica debe cumplir los requisitos exigidos a cualquier otro medio de

> prueba: pertinencia, utilidad y licitud. Respecto de esta última la prueba lícita serás aquella que se obtiene sin violar derechos y libertades fundamentales (…) Debido a la facilidad de manipulación de la prueba electrónica, la dificultad de la visualización o escucha de material intangible, y la dificultad para distinguir entre el original y la copia; la intervención de un perito informático para elaborar el correspondiente dictamen pericial puede ser muchas veces necesario y hasta determinante (…) La prueba electrónica aportada debe analizarse, como cualquier medio probatorio ordinario o convencional, bajo los principios de oralidad, contradicción, concentración, publicidad e inmediación (…) El sistema de valoración aplicable a la prueba electrónica, como regla general, es el de la libre valoración de la prueba bajo las reglas de la sana crítica (…) El juez siempre puede contar con el auxilio de un perito informático que le ayude a esclarecer si ha habido o no manipulación de un medio de prueba electrónico, y con el apoyo de un prestador de servicios de certificación que le ayude a determinar la integridad de los datos y la corrección del origen de los mismos. (Oliva. et al.)

Nos hemos referido en forma general al tratamiento de la prueba electrónica y debemos apuntar que en el medio forense encontramos algo que es muy común encontrar es lo relativo a los pantallazos, captura de pantalla o screenshot y es que debemos recordar que la prueba electrónica o en su caso la digital deben estar contenidos en un dispositivo electrónico ya sea que el dispositivo sea el analizado o la información que se encuentra en éste sea la que se analice, en uno u otro caso la identificación y análisis debería ser en forma autónoma verificando para el efecto la fecha de creación del análisis forense, se advierte que si se presenta una captura de pantalla impresa en papel y se presenta ante juez competente esto creará duda en el juzgador y por lo tanto no le dará un valor probatorio autónomo.

Citan los autores Ricardo Oliva y Sonsoles Valero en su obra La Prueba Electrónica, Validez y Eficacia Procesal el caso Tuenti sucedido en donde se enjuició la

validez y autenticidad de unos pantallazos extraídos de la red social Tuenti en un caso de acoso sexual, describiendo lo siguiente:

> El Alto Tribunal concluyó que si bien la valoración de la prueba en estos casos de mensajería instantánea "debe ser abordada con todas las cautelas" por la posibilidad real de manipulación, en este caso se debía valorar otras 93 pruebas circunstanciales como el hecho de que la propia víctima hubiera puesto a disposición del Juez de Instrucción su contraseña de Tuenti con el fin de se pudiera solicitar un informe pericial, que hubiera obtenido los pantallazos también en presencia de la guardia civil (…) En este caso el trabajo del perito informático consistirá principalmente en el desarrollo de procedimientos encaminados a "preservar" las evidencias digitales que se puedan derivar del contenido electrónico que se pretenda aportar en juicio. Esta preservación se obtiene a través de la realización de copias forenses "exactas" de la información digital almacenada dando lugar a un código alfanumérico de dicha información (código hash). Dicha copia se realiza por duplicado, depositando una de ellas ante Notario, y quedando la segunda copia en poder del perito para su posterior análisis técnico. Las técnicas utilizadas en este análisis suelen ser de carácter selectivo, es decir, sólo se busca aquella información que resulte necesaria para la investigación, a través, por ejemplo, de búsquedas "ciegas", evitando con ello posibles injerencias en datos o informaciones de carácter íntimo o privado del trabajador investigado. Finalmente, los resultados de la investigación se trasladarán a un informe pericial técnico que será el que se aporte en juicio. Es frecuente en la práctica que acuda el perito el día del juicio para ratificar el informe evitando con ello posibles impugnaciones de la parte contraria. La finalidad de la aportación de pruebas electrónicas mediante informe pericial informático es garantizar en el proceso judicial la originalidad, autenticidad e integridad de la información digital que se presente como prueba digital. Por lo tanto, esta opción será útil en aquellos casos en los que exista un gran volumen de datos e información a analizar, como puede

ser el disco duro de un ordenador, o bien cuando la prueba electrónica es la principal, o incluso la única disponible, y existen facilidades (y dudas) de manipulación, como pueden ser los mensajes de aplicaciones móviles.(Oliva. et al.)

En conclusión, no es válido aportar como medios de prueba una captura de pantalla de un mensaje de cualquier red de mensajería en virtud que es manipulable y no da ningún tipo de certeza jurídica, hoy en día podemos encontrar varias aplicaciones y programas que simulan una conversación, pregunto al lector, ¿Conoce usted de algún caso en donde se haya emitido una sentencia en donde se le haya dado valor probatorio a una captura de pantalla?

8.5. La prueba digital.

En el apartado anterior describimos extremos útiles y relevantes en relación la prueba electrónica, que iba encaminado a todo el procedimiento para identificar, obtener, analizar, documentar y presentarla ante juez competente, resaltando que este tipo de procedimiento es sobre dispositivos electrónicos o hardware. Ahora corresponde describir algunos extremos importantes sobre la prueba digital, recordando que, así como en la prueba electrónica, debemos advertir que una regla general para la valoración de la prueba debe también basarse en la sana critica razonada del juez, antes de entrar en detalle sobre el sistema de valoración conoceremos en las siguientes líneas algunas consideraciones generales.

La prueba digital se refiere toda la información contenida en un dispositivo electrónico o que transmite por el referido medio, esto incluye a los metadatos, logs y toda aquella información que se encuentra almacenada y que en algún determinado momento nos ayudará para acreditar determinados hechos. Es importante resultar que la información que se pudiera encontrar en un escenario criminal podría ser utilizada para acreditar la comisión de un acto ilícito ya sea de los tipos penales comunes o algún delito informático.

Como hemos ya apuntado en otros apartados de este texto, la tecnología sigue avanzando en forma rápida y con ello surgen cada día diferentes tipos de dispositivos y aparatos que ayudan las tareas del hombre, consecuentemente cada uno de ellos lleva consigo la producción y transmisión de información, hablar de un teléfono celular, un dron, inteligencia artificial, robótica, nubes de información, servidores o estaciones inteligentes, automóviles inteligentes, internet de las cosas, entre otros nos da la pauta de un sinnúmero de actividades

Debemos analizar que cuando nos referimos a la prueba digital es posible que nos encontremos con dispositivos electrónicos, sistemas informáticos o medios de almacenamiento que serán susceptibles de análisis forense consecuentemente podremos obtener la evidencia digital que nos servirá para nuestra investigación, sin embargo también podría existir otro escenario y es cuando la información se transmite por diferentes plataformas o redes de comunicación entre ellas podemos mencionar la telefonía fija y móvil. En el caso de Guatemala podemos citar como ejemplo la información obtenida a raíz de una interceptación telefónica que está regulada del artículo 48 al 71 del Decreto 21-2006 del Congreso de la República “Ley contra la Delincuencia Organizada” en el cual se intercepta, graba y reproducen las comunicaciones que ahí se describen.

Otro caso interesante es la información obtenida de las redes sociales cuando de las comunicaciones existentes entre dos o más personas se obtiene información relevante, sin embargo en Guatemala aún existe una mala práctica en cuanto a tomar una captura de pantalla de las comunicaciones para luego ser presentada como prueba ante juez, esto a todas luces es antitécnico, inviable y viciado toda vez que debe seguirse un procedimiento establecido para acreditar aquellos extremos como prueba, iniciando con una certificación digital de las comunicaciones, cadena de custodia física y digital, entre otros pasos que se describieron en el apartado de protocolos forenses.

Es menester señalar que el procedimiento que implica el adecuado tratamiento de la prueba digital corresponde a las mismas fases que se aplican en la prueba electrónica, recordando que estas fases atienden también a la ciencia de la informática forense siendo ellas: la identificación, obtención o recopilación, traslado, análisis y

presentación de resultados; además es necesario mencionar que esta prueba debe ser licita, pertinente, necesaria, auténtica e integra.

Un aspecto que no debemos obviar es que se deben respetar los derechos fundamentales de las personas, en un ejemplo claro es cuando se encuentran diferentes dispositivos electrónicos en el escenario criminal, sabemos que en este caso la evidencia electrónica y digital que se identifica y obtiene deben de observarse y cumplirse los principios constitucionales, siendo entonces que previamente debe existir una autorización judicial para llevar a cabo esta diligencia de investigación como por ejemplo un allanamiento en donde el fiscal solicita al juez que en ésta diligencia se practique la inspección, secuestro y registro de un inmueble a efecto de recopilar evidencia o rastros del delito o en su caso para hacer efectiva una orden de aprehensión, sin embargo cuando nos trasladamos al plano de la evidencia electrónica y digital el fiscal debe solicitar además del secuestro, la autorización para la extracción de la información y la revisión de la información obtenida.

Existen varias posturas al respecto en el sentido que muchos estudiosos del derecho apuntan a que después de secuestrar los dispositivos electrónicos no es necesaria la autorización de la extracción y análisis de la información ahí contenida, sin embargo se estima que si se autoriza el secuestro de evidencia electrónica y digital es necesario que el juez valide la extracción y análisis de información atendiendo al principio del contradictorio y legalidad en virtud que si solo se autoriza el secuestro de la evidencia y tácitamente se desea extraer y analizar la información sin necesidad de autorización correspondiente se estaría vulnerando el derecho a la intimidad y privacidad de la persona, invito al lector para que en forma crítica analice el articulo doscientos del Código Procesal Penal de Guatemala y efectúe una integración con el contenido que se presenta en este trabajo.

Además de lo descrito en el párrafo anterior, puede ocurrir que una persona se aprehendida en flagrancia o cuasi flagrancia por las autoridades correspondientes y se le incaute al aprehendido algún dispositivo electrónico en cuyo caso es necesario también aplicar los protocolos y estándares en materia de recolección de evidencia electrónica y digital, cuyos aspectos relevantes son iniciar la cadena de custodia física

y digital manteniendo la evidencia en forma íntegra y que no se dude de su autenticidad, esto de conformidad al protocolo específico del dispositivo electrónico objeto de análisis.

Es importante mencionar la forma en que se puede obtener la evidencia electrónica y digital en forma lícita. Cabe entonces preguntarnos qué procedimiento aplica el Ministerio Público en Guatemala para acceder a la información o datos producidos o almacenados en un dispositivo electrónico, o en su caso de que dichos datos sean transmitidos en forma electrónica a través de redes de comunicación tales como Internet o redes de telefonía. Y más aún que deben se practica un anticipo de prueba según lo establece el artículo 317 del Decreto número 51-92 del Congreso de la República en materia de evidencia electrónica y digital. Otro escenario polémico y recurrente es cuando una persona es aprehendida con algún dispositivo electrónico y cabe acertadamente entonces preguntarnos qué procedimiento se utiliza para embalar la evidencia y obtener la información que nos servirá para el proceso.

En la práctica forense también es muy común que las víctimas del delito aporten información como prueba pretendiendo ser evidencia electrónica y digital sin embargo es un error muy común y que atenta contra los protocolos y principios en relación a la informática forense, toda vez que a todas luces esa incorporación carece de autenticidad e integridad.

La prueba que se incorpora al proceso debe ser legal y legítima evitando crear mecanismos fraudulentos para su obtención e incorporación, esto lo menciono porque en otros países no se le da valor probatorio a la prueba digital cuando se emplean técnicas de fuerza bruta, hacking, ataques de denegación de servicios, virus y muchos más, usadas para obtener información sin embargo éstas y muchas prácticas similares encajan en la teoría de los frutos del árbol envenenado porque la prueba no es obtiene de una forma legítima, evidentemente el juez debe tener un conocimiento previo para saber cómo resolver este tipo de asuntos y es acá donde juega un rol importante el Perito Forense Digital tanto como experto que ha efectuado el peritaje o en su caso para efectuar un contra peritaje bajo la figura del Consultor Técnico que de conformidad

al artículo 141 del Código Procesal Penal de Guatemala se faculta para actuar en casos que se considere necesario la asistencia.

Como lo mencionaba anteriormente en la labor de obtener la evidencia digital existe una línea delgada que si se cumplen los protocolos forenses determinados se logrará presentar al juez la prueba digital que sirva para esclarecer el hecho que se investiga pero si se realiza en forma incorrecta entraremos a la esfera de la vulneración a los derechos fundamentales de las personas tales como la privacidad, el secreto de las comunicaciones, vulneración de la protección de información sensible de las personas y en muchas ocasiones contra el honor. .

Debemos apuntar y recordar que uno de los elementos fundamentales de la prueba *strictu sensu* es que sea pertinente, útil, legal y legítima y en este caso agregaría que también ser relevante. En ese sentido la prueba digital debe tener una relación clara y precisa con el hecho que se investiga con el objeto de conocer la verdad histórica de los hechos en su caso verdad probada en juicio, todo esto para esclarecer los hechos controvertidos de la acusación y sometidos al contradictorio de la etapa de juicio.

La prueba digital debe también someterse a un interrogatorio por parte de los sujetos procesales, al peritaje y contra peritaje, relevante resulta que en los alegatos de apertura y en las conclusiones de los sujetos procesales se determine fehacientemente y con claridad la importancia que aporta al juicio la prueba digital encontrada.

En el medio forense y practica tribunalicia a diario existen diversidad de casos en los cuales se maneja prueba digital sin embargo ésta es tratada como prueba documental o prueba material aplicando metodologías de interpretación erróneas y que la gran mayoría de veces ésta prueba no es valorada por los jueces de forma correcta y apegado a los protocolos forenses digitales y esto es ocasionado porque el juez evita resolver basado en la prueba digital ya sea por desconocimiento o por confusión según lo visto en juicio.

Citemos algunos ejemplos interesantes: cuando se aporta un teléfono celular en cuyo contenido aparece una conversación de la plataforma WhatsApp y junto al

teléfono celular se adjunta una impresión o transcripción escrita de la misma en donde se solicita el cotejo de esa impresión y el contenido de la conversación de WhatsApp; cuando se presentan registros de actividades o sucesos de un cajero automático, plantas telefónicas, en cuyo caso en muchas ocasiones es posible que solo se presente una inspección ocular de estos dispositivos, historial de uso, etc., cuyo aspecto relevante en este caso es establecer el funcionamiento correcto de estos dispositivos en el momento en que ocurrieron los hechos.

Un aspecto que se discute frecuentemente es sobre la forma correcta de incorporar al proceso penal específicamente en la audiencia de ofrecimiento de prueba y en el debate oral y público los soportes electrónicos que contienen información sobre los informes de la extracción y análisis de información ya que muchas veces se confunde con la prueba digital misma; una y otra son diferentes en virtud que los soportes que contienen información sobre el análisis pericial realizado pueden presentarse en forma escaneada o digitalizada mediante algún dispositivo de almacenamiento ya sea una memoria USB o un disco compacto toda vez que solo contiene el informe que también se presentará en forma escrita y que en etapa de juicio se ratificará por parte del Perito Forense Digital que haya realizado la expertiz, asimismo el referido informe se presentará como prueba documental que se pondrá a la vista del Perito para que lo reconozca y efectúe la ratificación, ampliación o modificación según sea el caso.

En el caso de la prueba digital es importante resaltar que no puede debe guardarse en una memoria USB o similar toda vez que debe tomarse en cuenta la volatilidad de la información; es necesario comentar brevemente al lector que cuando se obtiene la evidencia digital debe de efectuarse una clonación de la información del dispositivo y luego se procede a la extracción de la información in situ si es posible y si no fuera así se envía al laboratorio forense para su análisis forense digital, el dispositivo original se embala y se inicia la cadena de custodia física y digital y la información clonada o también llamada imagen forense obtenida de ese dispositivo electrónico debe almacenarse en un disco de blue-ray o DVD que garanticen que no se regrabará o modificará la información clonada, ésta será nuestra evidencia digital

original y además se generarán copias de ésta imagen forense que serán entregadas a los sujetos procesales según corresponda para analizarlo y efectuar la defensa o acusación según corresponda; el disco de blue-ray o DVD original se convertirán en la evidencia digital sujeta a análisis y de ella debe garantizarse la integridad tanto en el embalaje, cadena de custodia física y digital. Ya en la etapa de juicio se presentará como prueba material electrónica el dispositivo de donde se extrajo la información y como prueba digital la información que está contenida en la imagen forense y del análisis realizado se presentará el informe de resultados con las conclusiones o dictámenes correspondientes misma que será prueba documental y el Perito Forense Digital o Experto será quién ratificará, ampliará o modificará el informe según corresponda.

Siguiendo el procedimiento anterior garantiza que los sujetos procesales puedan examinar en juicio la prueba electrónica y digital con las garantías del debido proceso. Recordemos que lo que hemos detallado en este capítulo se refiere a las pericias informática que se realizan en el ámbito público es decir la que será útil en un proceso penal sin embargo también este tipo de pericias es aplicable para otras ramas de derecho y ser utilizado en los diferentes procesos ya sea civil, laboral, administrativo, entre otras; además éstas pericias también son requeridas en el ámbito privado por parte de empresas que en varios países del mundo es algún muy recurrente, en virtud que muchas veces se necesita para acreditar conductas de un trabajador, utilización de información de clientes o de la empresa, uso de software original o malicioso y que al final si existen anomalías en las auditorías realizadas podría ser utilizada como prueba electrónica y digital en un proceso judicial.

La prueba digital como dijimos anteriormente, cuando es presentada ante un juez, debe ser mediante un informe. Estos informes podríamos clasificarlos así: a) Técnico: cuyo contenido se refiere a el procedimiento empleado para la extracción y análisis forense es decir contendrá todo el idioma técnico y metodológico empleado. b) Ejecutivo: cuyo contenido debe ser en un lenguaje entendible para los sujetos procesales para que pueda ser interpretado y utilizado en el proceso, por lo regular la

terminología técnica es limitada pero muy enriquecedor en los resultados obtenidos. c) Mixto: es la mezcla del informe técnico y ejecutivo.

Resumiendo lo relativo a la prueba electrónica diremos entonces que las fases del análisis forense digital están: la preservación, adquisición, análisis, documentación y presentación. De igual forma podemos indicar que en un proceso de análisis forense digital se inicia así: a) Identificación y obtención de la información ya se evidencia electrónica o digital. b) Procedimiento para crear la imagen forense mediante un clonado de información con la respectiva cadena de custodia física y digital (algoritmo hash) c) Análisis forense digital y su posterior elaboración del informe o dictamen pericial. d) Valoración por parte del Tribunal de Sentencia Penal ya sea en forma colegiada o Unipersonal según sea el tipo de delito que se esté conociendo.

Invito al lector a considerar lo relativo a la función del juez sentenciador que emite el fallo en el cual absuelve o condena al acusado y es que no debemos olvidar que acá entran en juego las reglas de la sana crítica razonada que deben ser empleadas por el juzgador para la apreciación de la prueba, excluyendo así la discrecionalidad absoluta, siendo entonces relevante la lógica, la psicología y la experiencia principios fundamentales que pesar que parecieran obvias mencionar es necesario que no pasen por alto en el momento de apreciar la prueba electrónica y digital, debiendo procurar que la resolución del juez esté fundamentada e indique el motivo del por qué le da o no credibilidad a un medio probatorio a efecto de preservar el principio de legalidad, presunción de inocencia sin olvidar que se debe tutelar porque los principios de inmediación, contradicción, publicidad, igualdad y proporcionalidad deben haberse observado a lo largo el desarrollo del debate oral y público.

Es importante señalar lo que dice María Cristina González en su obra “El Valor de la Prueba Electrónica en el Proceso Penal Español” quien afirma:

> La doctrina define a la sana crítica como el buen arte de juzgar, que tiene por objetivo alcanzar y establecer, con expresión motivada, la certeza sobre la prueba que se produce en el proceso…Se trata de una valoración racional de la prueba, como una especie de estándar jurídico, que ofrece soluciones flexibles al caso pero que no se

originan en la inventiva personal ni en la caprichosa interpretación del juez. La expresión "sana crítica" se ha considerado sinónimo de "sana filosofía" o "crítica racional". Así, por ejemplo, se trata de poder valorar datos como puedan ser la moralidad de un testigo, la relación del testimonio con el hecho, el grado de implicación con la otra parte, etc. Puesto que no debe tratarse de una interpretación arbitraria por parte del Juez, se considera que la sana crítica comporta una serie de razonamientos que deben expresarse en forma de motivación. Así, deben contemplarse el principio de razón suficiente; ningún hecho puede ser verdadero o existente, y ninguna enunciación verdadera, sin que haya una razón suficiente para que sea así y no de otro modo, el principio de contradicción; una cosa no puede ser y no ser al mismo tiempo, el principio de identidad; una cosa sólo puede ser lo que es y no otra, y el principio del tercero excluido; entre dos proporciones de las cuales una afirma y otra niega, una de ellas debe ser la verdadera (…) La experiencia está asociada al sentido común, el hombre medio actúa en base a la experiencia que le es conocida, acumulando datos, conocimientos, cultura, que relaciona y por los que toma unas determinadas decisiones (…) Por ello, resulta importante para el Juez, como encargado de interpretar la prueba, la experiencia que éste tiene para ayudar a realizar la tarea que le es encomendada de valorar hechos, situaciones y las pruebas aportadas. Es importante no confundir la experiencia con el conocimiento científico o las leyes de la naturaleza, las cuales son verdades axiomáticas, sino que la experiencia es relativa, puede aproximarse a la verdad, pero no tiene porqué ser así. C) Certidumbre razonable: Si bien la prueba es un medio que se utiliza para establecer la verdad de un hecho, el juicio valorativo emitido por el Juez, discurre entre la probabilidad y la certeza jurídica, teniendo puntos de conexión con la verdad. Se defiende una certeza que excluya toda duda fundada y razonable puesto que es lo necesario y justo para poder pronunciar una sentencia de forma adecuada. Esa certeza no es una convicción íntima válida del juzgador, sino que

trata de excluir toda probabilidad de una solución contraria a la que se adopta. Es un tema complejo puesto que, pese a lo dicho anteriormente, en el fondo no es algo objetivo: la verdad está en los hechos, mientras que la certeza está en las personas, en el grado de convicción alcanzado por el destinatario de la prueba que viene obligado a su valoración. Certeza es ausencia de duda o dudas razonables y de peso, incompatibles con lo que se cree. Es por ello que no puede existir una hipótesis alternativa, puesto que implicaría la existencia de una duda razonable respecto de que otra postura pudiera ser la correcta. Así, a través de la sana crítica, del buen sentido, de la experiencia y de la capacidad lógica de razonar se puede llegar a una elección que resulta más probable en el caso, alcanzando una "certeza razonable". (González Bedmar, 2015)

En relación a la prueba electrónica y digital la autora aludida ya en el párrafo anterior nos da su postura afirmando que:

En la prueba electrónica, por sus características propias, existe una especialidad que no se puede encontrar en el resto de pruebas: el soporte en el que se encuentran. Este tipo de pruebas se contienen en soportes tales como disquetes, ordenadores, tarjetas de memoria, Smartphone, etc. Por tanto, existen dos elementos a analizar: uno técnico y externo llamado hardware y otro lógico e interno que recibe el nombre de software. En cuanto al primero, hardware, es necesario comprobar las posibles incidencias en su etapa de elaboración, fabricación, funcionamiento o transmisión tales como fallos de los programas, humedad, disfunciones por temperaturas extremas, acumulación desordenada de información proveniente de distintas terminales de entrada, etc. Mientras que respecto al segundo, el software, es necesario comprobar aspectos relativos a la averiguación de quién confeccionó el programa, si intervino persona no autorizada, alguien diferente al que aparece como autor, si se empleó su clave por un

> tercero, etc…el conocimiento de la prueba contenida en soporte electrónico puede conducirse por diversas vías (a través de su lectura, imprimiendo los datos, reproduciéndolo en pantalla, etc.) pero siempre ha de asegurarse que el órgano juzgador tenga acceso y se entere de tal contenido para poder valorar el material que le ha de informar para tomar su decisión. Es en este punto en el que los Jueces deben dar un paso más con respecto al resto de pruebas, por tener las electrónicas unas características inherentes, el órgano juzgador debe motivar su resolución a través de lo que algunos autores han calificado como "sana crítica especialísima" entendiendo que no sólo deben basarse en la lógica y sentido común del hombre medio, sino que deben de pasar a un nivel superior que es el que requieren las nuevas tecnologías, haciendo un esfuerzo añadido que en la mayoría de ocasiones se materializa con el auxilio de profesionales, expertos y peritos informáticos. Por tanto, se entra en el plano de una libre valoración siempre guiada por las reglas de la lógica, la argumentación racional, la técnica y el estado de la ciencia. (González Bedmar, 2015)

Siguiendo con el texto de la autora González Bedmar sobre la concurrencia de las pruebas y la pericia informática indica que:

> La prueba electrónica no representa en sí una superioridad probatoria, sino que requiere del complemento o refuerzo de otras pruebas tradicionales, para realizar un ejercicio de valoración global y así acceder a un resultado determinado. Es por ello necesario y frecuente la denominada concurrencia de pruebas, el conocimiento privado del Juez respecto a las nuevas tecnologías no va ser en todos los casos el más alto ni el más idóneo, sino que el órgano juzgador puede desconocer por completo las distintas formas electrónicas y medios informáticos que se van desarrollando en la sociedad. Pese a ello, no es posible que tal desconocimiento impida una tutela judicial efectiva que se haga depender de que el órgano juzgador sepa más o menos sobre las nuevas tecnologías.

> En esta línea, algunos autores defienden como inexcusables dos puntos: la práctica en todos los casos de la pericia informática y que el lenguaje expositivo y las conclusiones sean de la máxima claridad. De esta forma, se introduce objetividad y transparencia para suplir al desconocimiento, la subjetividad o el oscurantismo. Solamente disponiendo de todo ese material, de los conocimientos personales suficientes (como son las expresiones técnicas del caso) y de la pericia judicial o informes de las partes, que especifiquen lo sucedido y ofrezcan conclusiones claras y científicamente avaladas, podrá estarse en las condiciones idóneas de efectuar una adecuada valoración de esos concretos medios de prueba electrónicos. (González Bedmar, 2015)

Por último, puntualizo en que el Perito Forense Digital es quien aporta al Juez los conocimientos científicos y máximas de la experiencia de la tecnología que en Guatemala me atrevo a decir que por parte del Organismo Judicial aún persiste el reto para guiar e informar a los jueces sobre la forma en que se da el tratamiento de la prueba electrónica y digital. No es aventurado indicar que el Perito Forense Digital debe tomar un papel preponderante en esta área y lo afirmo en virtud que en Guatemala se tiene una mala práctica en delegar este tipo de labor forense a Ingenieros en Sistemas o en computación quienes, a pesar de su elevado conocimiento en temas tecnológicos, no poseen el perfil idóneo para examinar y presentar la prueba electrónica y digital.

8.6. La prueba digital en medios de comunicación y aplicaciones de mensajería instantánea.

Hoy en día existen una gran variedad de plataformas de comunicación tales como Instagram, Facebook, Twitter, Skype, YouTube, etc y aplicaciones mensajería instantánea como Messenger, WhatsApp, Signal, Telegram, Line, Viber, etc.; éstas se han convertido en esenciales y parte de nuestra comunicación e información diaria y que en muchas ocasiones son útiles transformándose también en material probatorio en las diferentes judicaturas del país sin embargo nuestro ordenamiento jurídico no responde a las necesidades el mundo globalizado en el tratamiento de la prueba electrónica y digital generando con ello un panorama de inseguridad jurídica causando

un gran perjuicio a los sujetos procesales ya sea porque no se le da o no el valor probatorio aplicando basándose en posturas y afirmaciones errónea. En otras palabras, afirmamos que nos encontramos ante una regulación procesal limitada o es que escasa para la prueba electrónica y digital, en virtud que cuando es presentada la prueba digital no se sabe con certeza si ha sido objeto de manipulación o modificación.

Las plataformas de mensajería como por ejemplo WhatsApp son utilizadas para la comisión de diferentes actos ilícitos dentro de ellos los llamados ciberdelitos que ya fueron descriptos en el capítulo correspondiente, no obstante que estas plataformas son muy comunes y usadas para estos fines, Guatemala aun no cuenta con la regulación legal pertinente que responda a las necesidades de la población en materia de justicia. Los cibercriminales y criminales comunes utilizan diferentes mecanismos para llevar a cabo sus fines como ejemplo el uso de VPN cuyo uso es evitar que una dirección IP sea vista o ubicada, también es usado el navegador Tor en la internet profunda cuyos mecanismos de encriptación son más avanzados y prácticamente difíciles de perseguir penalmente.

Para comprender de mejor forma la percepción que tienen varios juristas en cuanto a la prueba digital específicamente de las aplicaciones de mensajería citaremos lo que dice José Sánchez en su texto “Estudio de la Prueba Electrónica en el Proceso Penal” indicando que:

> lo cierto es que la naturaleza jurídica de la prueba electrónica plantea problemas teóricos (que alcanzan más tarde a la práctica profesional), hasta tal punto de que son varias las teorías que han nacido al respecto tales como: a) Teoría analógica: aunque minoritaria, esta primera tesis, encabezada por Illan Fernández, defiende que existen ciertas similitudes entre la prueba electrónica y la documental (…) b) Teoría autónoma: esta segunda tesis, la más mayoritaria, considera que la prueba electrónica es independiente de la documental (…) Y es que si tenemos en cuenta que la prueba electrónica es un elemento que se pretende hacer valer en un proceso, necesita no solo de la licitud en su obtención, sino de la posterior verificación o autenticación de la

> autoría y de las afirmaciones formuladas (…c) Teoría de la equivalencia funcional: finalmente, esta tesis entiende que «el contenido de un documento electrónico surte los mismos efectos que el contenido de un documento en soporte papel…en otras palabras, la equivalencia funcional implica «aplicar a los mensajes de datos un principio de no discriminación respecto a las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas; en este sentido los efectos jurídicos deseados por el emisor de la declaración deben producirse con independencia del soporte en papel electrónico donde conste la declaración. (Sánchez Hérnadez, 2016)

Del análisis de lo vertido por el autor nos inclinamos por la teoría autónoma en virtud de las características propias de la prueba digital y con ello afirmamos que es un error que en las judicaturas de Guatemala se aporte el llamado pantallazo o screenshot de una conversación de una aplicación de mensajería instantánea pretendiendo aportarlo como prueba digital o simplemente como documental, toda vez que ésta práctica a todas luces es ilegítima y no reviste de ningún tipo de elemento de certeza jurídica en virtud de la facilidad con que puede manipularse o crearse una conversación de una aplicación de mensajería en virtud que en el internet existen una gran cantidad de sitios que simulan este tipo de actos.

8.7. La prueba electrónica y digital en el proceso penal del derecho comparado.

A. México.

Afirma la autora Anselam Vicente en su obran “La prueba digital en la automatización de los procesos jurisdiccionales” que, de las reformas y adiciones del Código Civil Federal, del Código Federal de Procedimientos Civiles y del Código de Comercio:

> el consentimiento puede presentarse por medios electrónicos, ópticos o por cualquier otra tecnología, y la comunicación generada, enviada, recibida, archivada o comunicada

a la que se llama mensaje de datos se reconoce como prueba. La forma escrita y la firma se tendrán por otorgadas con el “mensaje de datos… siempre que éste sea atribuible a las personas obligadas y accesible para ulterior consulta” (…) Propongo que de la fusión del derecho procesal, las telecomunicaciones, computación, la economía del conocimiento y la automatización de los procesos jurisdiccionales, surja una nueva parcela jurídica: el derecho procesal informático, que se ocupa de la interrelación entre el ciberespacio y las relaciones humanas, así como los conflictos que se generen con motivo de ellas. El ciberespacio está conformado por tres pilares: la digitalización de las relaciones sociales, hechos o actos jurídicos informáticos; las redes de comunicación, Internet, Intranet, Extranet, telefonía, mensajería, agendas electrónicas; la convergencia tecnológica, que es la fusión de la radio, la televisión, la telefonía e Internet. Asimismo, propongo una discutible definición de derecho procesal informático: conjunto de actos provenientes del Estado que regulan las pruebas digitales que aportan las partes y terceros ajenos a juicio, a fin de demostrar los hechos controvertidos en el mismo y la verdad material (…) La firma digital garantiza la autenticidad e integridad del documento, así como la posibilidad de detectar cualquier cambio o alteración del documento digital. Sellos de tiempo es otra actividad relacionada con la prueba, en el caso de emisión del documento digital…El sistema de sellos digitales de tiempo deberá cumplir, en todo momento, por lo menos, con el estándar internacional Internet X.509 “Public Key Infraestructure Time Stamp” y considerar los RFC, 3161 y 3628 o los que lo suplan, previo aviso que la Secretaría haga por escrito a los Prestadores de Servicios de Certificación. El sellado de tiempo timestamping es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Un sello de tiempo es una información relativa al momento de la acción de firma electrónica, obteniendo el dato de tiempo de una fuente fiable y objetiva…Hoy en día muchos dudan sobre la validez de utilizar documentos

digitales como medio de prueba y, lo que es más grave, en ocasiones son los mismos jueces quienes se cuestionan la validez probatoria de los acuerdos y demás documentos que no constan en papel, o documentos digitales. ¿Cómo verificar si el documento electrónico es verdadero o no lo es? En México, la Secretaría de Economía tiene certificadores de servicios, que son los que brindan la emisión de certificados digitales, que es el elemento con el que se firma prácticamente en todo el mundo. Por otra parte, la norma oficial mexicana NOM151 dispone perfeccionar el método de almacenamiento y establece requisitos para la conservación de mensajes de datos. Las reformas al Código de Comercio de mayo de 2000 le dan fuerza probatoria cuando el documento es firmado con la firma electrónica avanzada (…) El caso de la prueba pericial en informática es el equivalente a tener a los peritos en grafología; es decir, se pone en duda una firma electrónica se tendrá que recurrir a los especialistas en informática para su perfeccionamiento (…) El especialista también se refiere al aseguramiento de la evidencia. Al respecto, señala que una vez que se ha cumplido apropiadamente, y el congelar la evidencia y generar la imagen digital, se deberá asegurar la evidencia, según sea el caso, para que la información no pueda ser manipulada. (Vicente Martínez, 2016)

B. España.

La autora María González en su obra “El valor de la prueba electrónica en el proceso penal español” explica que:

La prueba electrónica es un medio de prueba autónomo, distinto del resto de medios de prueba, nacido por el avance de la tecnología en el ámbito de la información y comunicación, que es reconocido como tal dentro del procedimiento civil pero no en el proceso penal, que como hemos subrayado carece de regulación específica en relación a la obtención, incorporación y valoración probatoria de este tipo de pruebas. De

conformidad con lo dispuesto en el art. 4 CC la legislación civil será de aplicación analógica en lo no previsto por las leyes penales. Por ello, se ha de tener presente el artículo 299.2 LEC, el cual reconoce como verdaderas fuentes de prueba los "medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase", estas fuentes de prueba dan lugar al medio de prueba que se denomina "de la reproducción de la palabra, el sonido y la imagen y los instrumentos que permiten archivar y conocer datos relevantes para el proceso (…) Se implanta a través de esa redacción un numerus apertus en esta materia que da cabida a la utilización de los medios electrónicos como pruebas dentro del proceso judicial (…) En nuestro ámbito comunitario coexisten dos modelos en relación con los requisitos que deben reunir las pruebas para su admisibilidad, por un lado, los que siguen un criterio muy amplio y que se basan en la libre consideración del juez para admitir o no la prueba electrónica, como son Austria, Dinamarca, Suecia, y Finlandia; y por otro lado, los países que tienen un criterio más restrictivo y que se remiten a los requisitos exigidos para los medios de prueba clásicos o tradicionales como son España, Francia e Italia…..Después de que España ratificara el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2011 14 ,es precisa la introducción en la Ley de Enjuiciamiento Criminal de una regulación específica acerca del acceso y obtención de la información contenida en dispositivos electrónicos así como su incorporación y resulta aplicable a los denominados delitos informáticos, así como a "la obtención de pruebas electrónicas de cualquier delito" de acuerdo con su art. 14.2 sobre la valoración en el proceso penal, para asegurar un procedimiento con pleno respeto a las garantías del proceso. (González, 2015)

C. Argentina

En la obra “El Rastro Digital del Delito” escrita por Di Lorio y demás autores explican el contexto de las instituciones encargadas de la investigación criminal detallando lo siguiente:

> El Instituto de Ciencias Forenses Sur (con sede Mar del Plata), de reciente inauguración, se especializa en Medicina Forense, Balística y Análisis de Comunicaciones. Los distintos esquemas actualmente existentes no contemplan la disciplina de la Informática Forense de forma integral, siendo abordada en ocasiones a través de otras oficinas con especialidades diversas que realizan algún tipo de examen pericial informático, sin cubrir todo el campo que esta nueva disciplina tiene para aportar a los procesos judiciales. Los especialistas en el manejo de la evidencia digital deberían trabajar en conjunto y de forma coordinada, bajo la forma de un Laboratorio Forense Judicial, integrando una Asesoría Pericial Departamental o bien un Instituto de Investigación Criminal y Ciencias Forenses. (Di lorio. et al.)

De igual forma Mercedes Rivolta en su blog titulado “Medios de prueba electrónicos: estado de avance en la legislación argentina (sic)” refiere lo siguiente:

> La Argentina no dispone de normas específicas en materia de procedimiento judicial digital, al modo de Brasil con su Ley Nro. 11.419 del 2006 que establece el proceso telemático para la Justicia. Algunos pocos códigos procesales admiten explícitamente el uso de medios de prueba electrónicos. También, la posibilidad de realizar notificaciones electrónicas, comunicaciones y exhortos. Solamente la Ciudad de Buenos Aires y la Provincia de Chubut cuentan con ordenamientos jurídicos procesales avanzados que contemplan el uso de medios digitales en la administración de justicia. El recientemente aprobado Código Procesal Penal de la provincia de Entre Ríos, admite para algunas medidas probatorias específicas el uso de medios electrónicos: reconocimiento de voz,

reconocimiento por imágenes, testimonial especial filmada, y el principio general establecido en el artículo 300 que admite la filmación de otros actos procesales. (2) En la Ciudad Autónoma de Buenos Aires, el Reglamento General de Organización y Funcionamiento del Poder Judicial de la Ciudad dedica, en el artículo 1.12 sobre "expedientes", varios incisos al tema. En síntesis, admite que la totalidad de los juicios se instrumenten en formato digital, la producción de prueba en dicho formato y el acceso a la información. Asimismo, admite las comunicaciones entre magistrados por medios telemáticos, y el uso de video conferencias para recibir declaraciones o testimonios. En los juicios orales, habilita el uso de herramientas tecnológicas para producir imágenes, sonidos o texto. Hasta el momento, no se ha puesto en funcionamiento. La provincia de Chubut cuenta con un moderno Código Procesal Penal que contempla el uso de medios electrónicos. (3) Admite el expediente electrónico, la presentación y producción de prueba mediante evidencia digital, y las comunicaciones y notificaciones electrónicas. Dicha provincia patagónica, ha instrumentado un sistema de notificaciones electrónicas que se realiza a través del servidor de correo electrónico del Poder Judicial, y utiliza certificados de clave pública emitidos por una Autoridad Certificante propia. (Rivolta, Saij, 2007)

D. Colombia

Juvencio Galvis en su blog “Abogado en la Web” explica los detalles de “La Prueba Electrónica en Colombia” específicamente en la legislación afirmando que:

la prueba electrónica en Colombia se encuentra en la ley 527 de 1999, Artículo 5 en la siguiente expresión: ARTICULO 5o. RECONOCIMIENTO JURÍDICO DE LOS MENSAJES DE DATOS. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos. La expresión Mensaje de Datos lógicamente hace alusión a la prueba electrónica ya que

esta ley es la que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y establece las entidades de certificación y dicta otras disposiciones relacionadas con el Comercio electrónico. ARTICULO 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.(Galvis Feria)

Por último, señala el autor Fernando Morales en su obra “Validez de la Prueba Electrónica que “una de las funciones de la firma digital es la utilización de técnicas de encriptación y cifrado, que presta la entidad certificadora, con el fin de proteger la integridad de la información y asegurar la autoría por medio de una clave, así mismo el destinatario cuenta con una clave que le permite accesar la información y garantizar la integridad y autoría, ya que el documento al ser enviado estuvo expuesto en la red pública de datos, esta certificación es suficiente para acreditar la veracidad de un documento electrónico.” (Morales Sánchez)

8.8. Ley para el reconocimiento de las comunicaciones y firma electrónica.

Cuando se desarrolla el tema de informática forense y dentro de ello los puntos específicos sobre la prueba electrónica y digital nos encontramos con que muchos juristas refieren que en Guatemala no existe a la fecha una ley que regule de alguna forma esto y simplemente hacen referencia a que en el ámbito del Derecho Penal existe un catálogo de tipos penales de tipo informático, opinión polémica toda vez que por una lado los tipos penales que están regulados en el Código Penal no cumplen con la expectativa a nivel mundial sobre delitos informáticos ya sea como medio u objeto, además desde otro punto de vista el tener o no una ley que regule los ciberdelitos es

solo una pequeña parte que estudia el Derecho Informático, advirtiendo entonces que la opinión es limitada y poco congruente con la realidad de las Tecnologías de la Información y Comunicación.

En Guatemala es vigente y positivo el Decreto número 47-2008 Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas en cuyos considerandos fundamentan la creación de esta ley por la proliferación y masificación de la tecnología en la sociedad a efecto de adaptarnos al mundo digital, enfocado al comercio electrónico creando para el efecto herramientas que faciliten y viabilicen las operaciones comerciales más allá de las fronteras de Guatemala propiciando nuevas prácticas de comercio mediante la implementación objetiva de instrumentos técnicos y legales que responden al contexto internacional, incluyendo lo relativo a las firmas electrónicas, contratos electrónicos, fuerza probatoria de las comunicaciones electrónicas y los proveedores de servicios digitales (certificadores)

Desde una percepción mercantil diremos que esta normativa jurídica es un conjunto de datos que se adjuntan a un mensaje o documento electrónico, que tiene como principal objetivo identificar al firmante de éste como su autor único y verificar que el mensaje no haya sido modificado, creándose para ello un certificado digital, que no es más que un archivo digital que contiene la información y los datos de la persona que firma electrónicamente. Vemos entonces que en principio esta ley se enfoca al comercio y con ello a la implementación de todos aquellos mecanismos digitales para que exista un buen flujo de información y operaciones comerciales, sin embargo, haremos un análisis desde la percepción de la informática forense y la prueba electrónica y digital, en los siguientes artículos:

I) "Artículo 1. Ámbito de aplicación. La presente ley será aplicable a todo tipo de comunicación electrónica, transacción o acto jurídico, público o privado, nacional o internacional… Las disposiciones contenidas en esta ley se aplicarán sin perjuicio de las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos".

Esta norma jurídica se analiza en su conjunto sin embargo me permito resaltar y parafrasear este artículo: "*aplicable a todo tipo de acto jurídico público o privado nacional o internacional…se aplicarán sin perjuicio de las normas relativas a la celebración formalización y validez de otros actos jurídicos*.". Esto nos da la pauta que es posible aplicar la normativa no solo en el ámbito de las relaciones bilaterales de tipo comercial, sino que también a otros actos jurídicos en otras ramas del derecho.

II) "Articulo 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".

Esta norma jurídica se analiza en su conjunto sin embargo me permito resaltar y parafrasear este artículo: *"No se negará efecto jurídico, validez o fuerza probatoria solo por ser comunicación electrónica".* Esto nos da la pauta que en las judicaturas deben apreciar la prueba digital y no deben desecharla o no valorarla solo por ser electrónica o digital, en el entendido que cuando se refiere a comunicación electrónica nos indica que es toda aquella información que está contenida o transmitida en los dispositivos electrónicos por eso es totalmente válido indicar que la comunicación electrónica es la evidencia o prueba digital.

III) "**Artículo 10. Integridad de una comunicación electrónica.** Para efectos del artículo 9 anterior, se considerará que la información consignada en una comunicación electrónica es íntegra, si atiende a los criterios siguientes: a) Ésta se ha mantenido completa y sin alteraciones que no sean la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, archivo o presentación; y b) El grado de fiabilidad requerido se determinará teniendo en cuenta la finalidad para la que se generó la información, así como todas las circunstancias del caso".

Esta norma jurídica se analiza en su conjunto sin embargo me permito resaltar y parafrasear este artículo: "*Una comunicación electrónica es integra si se ha mantenido completa y sin alteraciones o adiciones o algún cambio que haya surgido en su transmisión, archivo o presentación*" Esto nos da la pauta que la prueba digital será

integra si no se ha modificado, alterado o se le ha adicionado algo desde su obtención, recopilación, preservación, análisis o presentación.

IV) "**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".

Esta norma jurídica se analiza en su conjunto sin embargo me permito resaltar y parafrasear este artículo: *"las comunicaciones electrónicas serán admisibles como medios de prueba y no se negará eficacia, validez o fuerza probatoria en toda actuación judicial solo por ser comunicación electrónica o que no se haya presentado en original".* Esto nos da la pauta que la prueba digital tiene eficacia, validez y fuerza probatoria ante un juez, autoridad administrativa y también para uso en el ámbito privado.

V) "**Articulo 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".

Esta norma jurídica se analiza en su conjunto sin embargo me permito resaltar y parafrasear este artículo: "*toda comunicación electrónica gozará de fuerza probatoria según los criterios para la apreciación de la prueba y que cuando se refiera a la fuerza probatoria de un mensaje de datos se debe tomar en cuenta su credibilidad según como se haya generado, archivado, enviado y conservado la integridad de la información y así mismo se identifique quien lo inició y otros factores adecuados u*

oportunos para entender su credibilidad." Esto nos da la pauta nuevamente que la prueba digital para asegurar que reviste de seguridad y certeza jurídica debe analizarse cada uno de los pasos de la informática forense en cuanto al tratamiento de la evidencia digital es decir debe ponerse mucha atención a la generación, archivo, envío y conservación de la información se han seguido los protocolos forenses de cada caso concreto, de lo contrario no se considerará fiable ni muchos menos legitima ni legal. También hace mención a que debe identificarse el origen de la información y que todo factor que ayude a entender su credibilidad o certeza jurídica se tomará en cuenta para valorar dicha información en forma integral.

VI) Artículo 13. Conservación de las comunicaciones electrónicas. Cuando cualquier norma jurídica requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de las comunicaciones electrónicas, siempre que se cumplan las condiciones siguientes: a) Que la información que contengan sea accesible para su posterior consulta; b) Que la comunicación electrónica sea conservada en el formato en que se haya generado, enviado o recibido o con algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida; y, c) Que se conserve, de haber alguna, toda información o dato que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido. No estarán sujetos a la obligación de conservación, los documentos, registros o informaciones que tenga por única finalidad facilitar el envío o recepción de la comunicación electrónica. Los libros y papeles podrán ser conservados en cualquier medio tecnológico que garantice su reproducción exacta.

Esta norma jurídica se analiza en su conjunto sin embargo me permito resaltar y parafrasear este artículo: "*las comunicaciones electrónicas según lo exija la ley pueden ser conservadas para su posterior consulta, con formato en que se haya generado, enviado o recibido o algún formato que pueda demostrar la exactitud de la información generada o recibida, además, que al momento de conservar se pueda determinar el origen, destino, fecha y hora del mensaje enviado o recibido. Los libros y papeles también pueden ser conservados en cualquier medio tecnológico que garantice su*

reproducción integra". Esto nos da la pauta que después que extraiga la información de un dispositivo electrónico ésta debe ser posible revisarla de ahí que es importante la obtención de una imagen forense o clonado de información que nos garantizan la integridad de la información de su original ya que entre muchas cosas al realizar el análisis forense podremos observar los resultados de los hallazgos encontrados en la información analizada y dentro de ello determinar el origen, destino, fecha y hora de los datos generados o almacenados todo esto sin alterar la información original que previamente se encuentra embalado y con la cadena de custodia física y digital correspondiente, éste último con la generación del algoritmo hash correspondiente. Por último, también nos da la pauta de poder guardar la información en dispositivos de almacenamiento que no sean volátiles y que garanticen la integridad de la información tales como un disco de Blu-ray o DVD

Es importante mencionar que el Acuerdo Gubernativo 135-2008 Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firma Electrónica se enfoca más en regular lo relativo a la certificación de la firma electrónica y los proveedores de servicios, es decir se dirige más a la instrumentalización de los medios electrónicos para proveer esos servicios.

Es importante tomar en cuenta lo que en este tema se ha tratado en virtud que ésta normativa es fundamental para realizar un tratamiento idóneo y legal de la prueba electrónica y digital en el Derecho Penal y Procesal Penal de Guatemala.

8.9. Iniciativas de ley para regular el fenómeno social de la ciberdelincuencia.

A. Iniciativa de Ley 5254 (Ley contra la ciberdelincuencia)

Esta fue una iniciativa fue presentada el pleno del Congreso el 09 de marzo de 2017 nominada como Ley contra la Ciberdelincuencia cuyos aspectos interesantes y que sobresalen en la exposición de motivo es que pone en contexto que las relaciones sociales y actividades cotidianas son influenciadas de gran forma por las tecnologías de la información y comunicación y que derivado de ello el tráfico comercial y de comunicación a través del internet se desarrolla e incrementa al paso de los días y que sabiendo esto los ciberdelincuentes se aprovechan de ello para realizar ataques que

ocasionan un perjuicio directo e indirecto y que esto trasciende también a que en las redes digitales de comunicación se hace presente la delincuencia organizada que actúan a nivel transnacional. En esta iniciativa se contempla la protección a diferentes bienes jurídicos tales como los datos personales, intimidad informática, la indemnidad sexual de los menores. En cuanto a los datos se enfoca a la integridad, confidencialidad y disponibilidad de la información y la forma de asegurar las comunicaciones electrónicas. Implementa también un equipo de respuesta a incidentes de seguridad informática llamados CERT, que de conformidad a esta iniciativa está nominado como Centro de Seguridad Interinstitucional de Respuesta Técnico-jurídica de incidentes informáticos de Guatemala. En uno de sus capítulos define un catálogo de ciberdelitos unos que tutelan la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos tales como el acceso ilícito, la interceptación ilícita, ataque a la integridad de los datos y el ataque a la integridad del sistema; además se contempla a los delitos informáticos propiamente dicho tales como la falsificación informática, apropiación de identidad ajena, abuso de dispositivos, fraude informático. En lo relativo a los ciberdelitos contra las personas se encuentra la pornografía infantil, acoso por medios cibernéticos, delitos contra la integridad sexual de una menor o contacto a menor con fines sexuales a través de las TIC y por último lo relativo a la propiedad intelectual.

Es menester indicar que esta iniciativa fue asesorada por mucho tiempo por el Observatorio Guatemalteco de Delitos Informáticos dirigido por su fundador José Leonett quien a lo largo de muchos años ha trabajado en temas de informática forense para el país y creado e implementado temáticas de enseñanza para que el sector justicia conozca a detalle la forma en que deben tratarse los diferentes contenidos que estructuran a la informática forense y lo menciono toda vez que un logro reflejado, entre muchos, fue la implementación del llamado CERT Guatemala que da un aporte al país en tema de seguridad informática en el área de respuesta a incidentes.

Al hacer el análisis de esta propuesta de ley es necesario advertir que si bien es cierto contempla instituciones novedosas competencia del Derecho Informático e Informática Forense, hace falta la propuesta de regulación sobre algunos principios

procesales, la jerarquía normativa y sanciones más drásticas en los tipos penales que se proponen y la necesidad imperante que Guatemala se adhiera al Convenio de Budapest. Esta iniciativa fue reemplazada por la iniciativa 5601 que analizaremos a continuación.

B. Iniciativa de Ley 5601 (Ley de Prevención y Protección contra la Ciberdelincuencia).

Esta iniciativa de ley fue presentada recientemente el 18 de noviembre de 2019 al pleno del Congreso de la República y llama la atención que dentro de su exposición de motivos refiere que es necesario regular la conducta humana en la protección de derechos fundamentales regulados en la Constitución Política de la República de Guatemala, en virtud que existe un ecosistema criminal en donde existen una diversidad de conductas humanas que se pueden tipificar como antijurídicas y que lesionan a diferentes bienes jurídicos, denominada delincuencia informática. También resalta que Guatemala no es parte del Convenio sobre la Ciberdelincuencia suscrito en Budapest el veintitrés de noviembre de dos mil uno y que tampoco es parte de ninguna convención en materia de protección de datos haciendo referencia además a que tampoco existe algún convenio internacional sobre obtención de datos sobre el tráfico e interceptación de comunicaciones, derecho a la intimidad y confidencialidad de datos. De igual forma en la exposición sobre el impacto de la ley puntualiza sobre el actuar de la ciberdelincuencia que actúa en escenarios favorables sobre equipos informáticos en donde es utilizado el internet y que cualquier persona que esté conectada a internet a través de cualquier dispositivo puede ser víctima de un ciberdelincuente.

Es importante resaltar que esta iniciativa reemplaza a la iniciativa 5254 y prácticamente la estructura es similar, sin embargo, se nota que se adhiere y regulan más aspecto en protección de la dignidad y el honor. Además, agrega en uno de sus preceptos legales lo siguiente:

> Artículo 29. Registro y secuestro de medios digitales o electrónicos. El juez podrá ordenar a requerimiento del fiscal, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos, electrónicos o de la

comunicación, con el objeto de: Secuestrar los dispositivos con sus componentes físicos y digitales, que integren o no un sistema informático; b) Obtener copia de los datos en un soporte autónomo; o c) Preservar por medios tecnológicos o bloquear el acceso a los datos de interés para la investigación. Regirán en cuanto sean aplicables las normas generales y las mismas limitaciones dispuestas para el secuestro de documentos y correspondencia epistolar. En los supuestos en los que, durante la ejecución de una medida de secuestro de datos de un Sistema Informático, previstos en el párrafo anterior, surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema Informático al que se tiene acceso lícito desde el dispositivo o sistema inicial; el órgano investigador que lleva adelante la medida podrán extenderla o ampliar el registro al otro sistema, siempre que medie orden del órgano judicial. La ampliación del registro a los fines de la incautación deberá ser autorizada por el juez salvo que estuviera prevista en la orden original. (Comisión de Asuntos de Seguridad Nacional del Cong, 2019)

De la lectura de este articulo vemos con satisfacción que con esta propuesta de regulación legal se da la pauta para que la evidencia electrónica y digital se maneje en forma adecuada en virtud que acá se resume el contenido de los protocolos forenses sobre el tratamiento de la evidencia electrónica y digital.

De conformidad a la Estrategia Nacional de Seguridad Cibernética del Ministerio de Gobernación en su informe detalla que:

En términos de capacitación para la investigación de delitos cibernéticos, se destaca la falta de conocimiento de las autoridades sobre la aplicación de la ley acerca de una prueba digital, así como de la cadena de custodia digital, el traslado y la sustracción de la evidencia sobre el ISO 27037. De igual manera, las salas de audiencia no están equipadas para recibir evidencia digital, y hace falta también instrumentos para la adecuada recolección, preservación, transporte y análisis de la evidencia digital (ej.

bolsas de Faraday utilizadas para preservar dispositivos móviles como evidencia). Actualmente, existe una unidad en la Policía Nacional Civil (PNC) encargada de la investigación de delitos cibernéticos que es necesario reforzar e impulsar al igual que la Unidad Científica de Peritaje Forense del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF). Sin embargo, el Ministerio Público aún no cuenta con una Unidad de Delitos Cibernéticos, la cual deberá ser creada y reforzada para trabajar en conjunto con las demás unidades relacionadas al tema. Se remarcó la disposición de instituciones que pueden facilitar la capacitación de las autoridades en delitos relacionados con la informática y en el manejo de evidencias electrónicas, como la Red Latinoamericana de Informática Forense y la consultoría INFOGTM. Asimismo, se discutió la importancia de ofrecer capacitaciones a los profesionales del derecho, no sólo a las autoridades. (Ministerio de Gobernación, 2018)

CAPITULO IX

Delincuencia Organizada y el Uso de las Nuevas Tecnologías de la Información y Comunicación.

9.1. Generalidades del crimen organizado.

Adentrarnos en conocer la forma en que el crimen organizado se ha desarrollado y evolucionado a través de la historia es importante para conocer la forma en que operan actualmente no solo en el ámbito espacial sino también en el ciberespacio, para ello debemos analizar las características propias de cada contexto social y asimismo al interpretar que este flagelo es necesario considerar en primera instancia que esto corresponde a un problema de carácter estructural y que a pesar de los esfuerzos por parte de los estados en erradicarlos ha sido una tarea ardua y que hasta la fecha se sigue realizando.

Los grupos criminales tienen un antecedente legal y esto se encuentra en el Código de Napoleón lo largo de la historia en el mundo se han manifestado diferentes grupos que se han organizado para cometer actos ilícitos o que en plenos roles facultativos han abusado de su status para aprovecharse de grupos o sectores más débiles. Tonemos a diferentes sociedades de crimen organizado que en su momento proliferaron en diferentes partes del mundo tales como los Triadas Chinas, La Mafia Japonesa, La Mafia Rusa, Los Yacuza, La Mafia Italiana, La Mafia Turca, La Mafia Albanesa y que según muchos estudios se considera al grupo llamado “gabellotti” como un antecedente de la Mafia.

En el texto “Crimen Organizado” de la Doctora Sandra Acán explica lo relativo a las mafias y grupos organizados en el siglo XX y XXI, indicando que “durante la edad de oro del crimen organizado se mantuvo hasta la época de 1950…a principios de la década de 1920 la mafia norteamericana estuvo presente en todo tipo de negocios tale como el: el contrabando, prostitución, corrupción sindical, juegos, usura, extorsión, chantaje, etc…Los rasgos que han permitido la sobrevivencia de la mafia Siciliana se ha debido al hecho de que castas políticas enteras hayan hecho uso de bandas

mafiosas para su protección y con fines de control político y social…Hoy el día el poder de la mafia es ejercido por una mafia burguesa, una casta de directivos, profesionales contables, abogados, políticos e ingenieros, ninguno de ellos dispuesto a usar armas, estos están ingresando a la mafia en negocios globalizados". (Acán Guerrero, 2015)

Debemos tener claro que a lo largo de la historia han existido varios grupos delincuenciales que se han organizado para llevar a cabo sus fines. En el crimen organizado existen estructuras en cuya parte estructural están bien definidas las funciones o roles y que se rigen en base a reglas o códigos internos de actuación que guían su proceder. Estos grupos regularmente dentro de sus funciones se incluye la influencia en otros grupos sociales para conseguir favores a cambio de un soborno, dadivas o coimas, es decir existe un tráfico de influencias bien marcado.

Evidentemente hablamos de una esfera de corrupción en donde se realizan diferentes actos ilícitos e ilegítimos cuyo trasfondo es un beneficio para estos sectores criminales, actos en los cuales podemos mencionar desvío de fondos públicos, lavado de dinero u otros activos, simulación de contratos administrativos, compra de productos o servicios en forma sobrevalorada, influencia de jueces y fiscales en procesos judiciales, financiamiento de campañas electorales con recursos económicos obtenidos en forma ilícita, etc.

9.2. Características y fines de la delincuencia organizada.

Dentro de la estructura de la delincuencia organizada es menester indicar que en la mayoría de casos están organizados en forma piramidal es decir hay una persona quien tiene el rol de líder y es quien dirige todos los operativos criminales del resto de integrantes; asimismo existen otros grupos criminales que actúan en forma horizontal y uno de sus aspectos interesante es que del producto de las ganancias o riquezas obtenidas se distribuyen en forma equitativa.

De conformidad a la Convención de Palermo o Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, define a la delincuencia organizada como: "Un grupo estructurado de tres o más personas que exista durante

cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material" (Naciones Unidas, 2000).

Es necesario apuntar entonces que un grupo delincuencial organizado está estructurado con un grupo de tres o más personas en forma jerárquica lo cual le ayuda a la consecución de sus fines, además existe una auto renovación con el ánimo de garantizar la permanencia usando la violencia y las influencias sociales a efecto de alcanzar sus objetivos criminales.

Es necesario indicar que dentro de los mecanismos que actualmente usan estas estructuras criminales es el uso de la tecnología mismo que abordaremos más adelante. Es importante señalar la diferencia entre estructura criminal y red criminal, en virtud que la primera está estructurada en forma piramidal u horizontal y en cambio la segunda está conformada por pequeños grupos que se encuentran dispersos pero vinculados entre sí para llevar a cabo sus actos ilícitos, algo así como una red de telaraña con diferentes puntos de conexión y afines.

Dentro de los fines que persigue la delincuencia organizada es la obtención ilícita de un beneficio económico o ganancias económicas significativas, pero a esto hay que agregarle que se busca que sea en tiempo reducido, sin esfuerzo, burocracia ni obstáculos. Paralelo a esto, la delincuencia organizada busca mantener el poder en las diferentes esferas de la sociedad para que puedan mantenerse sus intereses económicos, políticos o sociales, este aspecto se relaciona mucho con los denominados delitos de cuello blanco.

9.3. Actividades criminales de la delincuencia organizada en el ciberespacio.

Hemos mencionado a lo largo de todos estos capítulos y subtemas que componen este trabajo de investigación, la informática y las nuevas tecnologías de la información y comunicación han influido en cambios significativos en la sociedad de hoy en día y los conceptos de redes de comunicación y la globalización digital ha creado que los diferentes sectores económicos, sociales y culturales acoplen sus

mecanismos de funcionamiento para atender sus necesidades. Un ejemplo de ello es la forma en que el comercio y las negociaciones electrónicas en los últimos años han tenido un repunte en su dinámica contractual en virtud que empresas de toda magnitud se han lanzado al mercado nacional e internacional para comercializar sus servicios.

Actualmente el internet tiene una dinámica constante en el que todo tipo de personas interactúan como por ejemplo al conversar por medio de las redes sociales, subir una foto o video y mostrar las acciones del día, vender productos y servicios, buscar información, estudiar y prepararnos académica y profesionalmente, es decir en las redes sociales y de comunicación podemos encontrar el resumen de vida de mucha gente, la información que se tiene obtiene de las personas es pública y en la mayoría de ocasiones no nos damos cuenta de eso hasta que nuestra información confidencial o privada es expuesta y nos vemos en la necesidad de tomar acciones para restaurar de alguna forma nuestra privacidad.

En el texto denominado “Ciberespacio y el crimen organizado” de Juan Salom Clotet expone lo siguiente:

> Ese mundo virtual basado en la tecnología digital, se ha convertido en un reto intelectual para unos y una barrera para otros. La complejidad técnica de los sistemas informáticos y del diseño de las redes, y los protocolos de comunicaciones que se utilizan, generan indudablemente diferencias de conocimiento entre los usuarios de la Red, que sin duda son aprovechados por unos pocos para hacer prevalecer sus intereses (…) Internet se revela como un mundo virtual donde no existen los mismos patrones sociales del mundo real, un mundo al que nos asomamos ocultos tras la pantalla, creyendo ser anónimos y asumiendo nuevos roles. Donde la protección que ofrece la facilidad de crear identidades ficticias, supone un acicate o desinhibidor de nuestros temores frente a las barreras sociales, impulsándonos a veces a superar la legalidad establecida. A la incultura digital, al escaso rechazo social de las conductas desviadas en la red, al vacío

> legal y al anonimato de la red, que ya de por sí son estímulos para el delincuente, se suma el rechazo social a cualquier. (Salom Clotet, 2011)

Debemos reflexionar que nuestra sociedad actualmente tiene un alto grado de inseguridad informática y digital y tengo esta postura en virtud que dentro del mundo digital existen, entre otras cosas, dispositivos electrónicos los cuales los poseen las personas sin embargo estos no son manejados en forma responsable, prudente y con las medidas de seguridad respectiva, esto ocasiona que exista una navegación y exploración a través de nuestros dispositivos electrónicos en forma insegura y con mucho riesgo de que seamos víctima de los ciberdelincuentes que se manifiestan de diferentes formas desde robar nuestros datos privados para comercializarlos hasta poner en riesgo nuestra vida.

Dentro de las actividades que realiza la delincuencia organizada se encuentran la obtención de bienes en forma ilícita, tráfico de armas y drogas, trata de personas, tráfico de inmigrantes ilegales, venta de animales exóticos, venta de obras de arte en el mercado negro, materiales nucleares, lavado de dinero a través de las redes criminales convencionales, tráfico de órganos y menores de edad, todo lo anterior en forma convencional, sin embargo hoy es más recurrente encontrar este tipo de actividades en la internet profunda –deep web-. La delincuencia o crimen organizado ha evolucionado y es por ello que ahora utilizan el ciberespacio para cometer actos ilícitos en virtud que emplean diferentes mecanismos para dejar el menor rastro o huella digital sobre los actos que cometen.

En la revista El Fisco de Benjamín Blanco escribió el artículo “El crimen organizado y las nuevas tecnologías” resulta importante destacar lo que literalmente dice:

> La Tecnología permite seguir cometiendo delitos tradicionales de forma no tradicional, desde cualquier parte del mundo y en cualquier momento. Al igual que en el delito tradicional, el fraude a través de Internet se caracteriza por su constante evolución. Y el fraude electrónico, no iba a ser menos, continúa desarrollándose y ganando en

sofisticación a la vez que avanzan y progresan las Nuevas Tecnologías y aparecen nuevas herramientas más sofisticadas; pero, paralelamente, los usuarios (domésticos, empresas y administraciones) al igual que en el mundo físico, resultan menos vulnerables gracias a mejores hábitos de utilización de la Red y a una mayor protección de los equipos, y sobre todo a una mayor información sobre el manejo de las mismas y sus vulnerabilidades. El delito informático produce un impacto económico negativo: no solo el daño directo para el que sufre o asume la estafa, sino también las pérdidas derivadas de la erosión de la imagen del suplantado; ambas provocan un impacto social, que se traduce en un freno al desarrollo de la Sociedad de la Información (…) El spam o mensajes de correo electrónico no solicitados que son enviados en cantidades masivas a un número muy amplio de usuarios suponen, en muchos casos, la cabeza de puente para la comisión de un fraude electrónico (phishing, scam, “cartas nigerianas”, bulos, etc. Por lo tanto, hemos de tener presente que todos los usuarios de Internet somos víctimas potenciales del cibercrimen, de la misma forma que en la vida real lo podemos ser de cualquier delito. Las nuevas tecnologías, al configurarse como nuevo paradigma que invade todos los ámbitos de la actividad humana, no podían por menos de incidir también en el lado oscuro de dicha actividad: la conducta delictiva o criminal de los individuos de los grupos organizados (…) Por ello, conocer sus procedimientos y técnicas resulta fundamental para mantener nuestros sistemas a buen recaudo y estar bien protegidos, y policialmente supone abrir vías o caminos para la investigación. En los últimos tiempos la ciberdelincuencia ha evolucionado considerablemente en complejidad y alcance: programas espía, troyanos, ataques de denegación de servicio o phishing, entre muchos otros, son algunos de los métodos más utilizados hoy en día, para llevar a cabo estos ataques y cada vez con técnicas más sofisticadas. A medida que prolifera el uso de Internet como medio para realizar transacciones on-line en las que los usuarios deben indicar datos personales, los ciberdelincuentes buscan la forma

> de acceder a esa información con el objetivo de utilizarla posteriormente con fines lucrativos (Blanco, s/f)

Para nadie es un secreto que al navegar en el ciberespacio podemos encontrarnos con muchos sitios de interés sin embargo también hay otros que son peligrosos no solo para nuestros dispositivos electrónicos e información sino también ponen en riesgo nuestro patrimonio y vida, es menester indicar que esto podemos encontrarlo en sitios web que no se encuentran indexados para su búsqueda y que no aparecen en los exploradores o navegadores tradicionales y de uso doméstico, comercial o académico.

Como lo apuntaba, la web profunda tiene innumerable información que nos ayuda a conocer diferentes temas de interés, sin embargo, también podemos encontrar diferentes sitios en donde hay información ilegal. En otro nivel mucho más pequeño y de complejidad para su acceso encontramos la web oscura que es ahí donde encontramos información extremadamente confidencial y con niveles altos de inseguridad e ilegalidad, es en estos niveles de navegación en el ciberespacio en donde la delincuencia organizada se aloja en un gran porcentaje para desarrollar sus planes delictivos. Además, es importante señalar que las estructuras criminales hoy en día invierten grandes cantidades de dinero para reclutar o contratar a piratas informáticos, hackers de sombrero negro, crackers, entre otros para manipular los sistemas informáticos y así fortalecer su estructura criminal.

Nuevamente citamos a Benjamín Blanco que redactó el artículo “El crimen organizado y las nuevas tecnologías” en donde cita algunos ejemplos y aspectos interesantes explicando que:

> Las mafias virtuales pueden conseguir hasta 4,130 millones de euros de beneficios, en un ataque phishing. El producto más valorado por las redes de delincuentes son los datos asociados a tarjetas de crédito, clave para obtener un beneficio mayor. El precio por cada dato de una tarjeta o cuenta bancaria oscila entre los 0,79 y 19,5 euros, dependiendo del volumen de la cctta cctte, y la cantidad que un delincuente obtendría

de ella puede alcanzar hasta los 31.100 euros. Un ordenador infectado se cotiza en el mercado negro por entre 2 y 3 céntimos; una red de 5.500 equipos se alquila por 350 dólares. Las últimas investigaciones, han demostrado que las Organizaciones Criminales de los Países del Este dedicadas a la comisión de delitos a través de las Nuevas Tecnologías, captan a los cerebros en convenciones, foros y eventos cibernéticos, organizados expresamente para identificar, localizar y convencer a los nuevos genios de la Informática, ofreciéndoles un buen trabajo, que les proporcionará grandes beneficios. Ellos se creen que han conseguido un "gran empleo", bien remunerado, en una Empresa legal, y sin saberlo están contribuyendo a la creación software y programas, que, sin ellos aprobarlo, serán utilizados para la ejecución y comisión de diversos delitos que se realizaran a través de la red. Las Nuevas Tecnologías, con Internet a la cabeza, se han revelado como una herramienta sumamente eficaz para que el dinero sucio, que puede proceder de las drogas, pero también de actividades terroristas y delitos tradicionales como el robo, el secuestro, la extorsión y la evasión de impuestos, borre su oscuro origen y no deje ningún rastro. No es que con Internet hayan surgido más casos de blanqueo de dinero, sino que la Red ha aumentado la velocidad de las transacciones. Las nuevas tecnologías permiten una tremenda movilidad del capital procedente del delito hasta que se esfuma su procedencia, y además ha puesto herramientas en manos de los delincuentes para la ocultación del rastro de las transacciones y movilidad del dinero. Una transferencia "online", se lleva a cabo en fracción de segundos y en fracción de segundos el dinero ha desparecido de un lugar o país y aparecido en otro, sin dejar rastro aparente y sin ningún tipo de control. Cabe mencionar que el surgimiento de "posadas cibernéticas", en las que el dinero sucio pasa unos minutos y va tejiendo un recorrido laberíntico de país a país, a través de Internet, que hace tremendamente difícil su rastreo. Casinos virtuales, inversión en línea, cuentas bancarias en la red, etc. (Blanco, s/f).

Actualmente existen otro tipo de actividades criminales que desarrolla la delincuencia organizada a través del ciberespacio como por ejemplo el espionaje a empresas, venta de información confidencial o datos personales y sensibles número de cuentas y tarjetas de crédito causando un grave problema al patrimonio de las personas, además de poner en riesgo los datos personales de las personas.

Seguimos citando al autor Benjamín Blanco en la obra ya indicada, ahora nos explica cómo opera una organización criminal en el mundo digital:

> Primeramente, explicaremos la estructura básica de cualquier organización dedicada, por ejemplo, al phishing. Ella se compone desde la cabeza a la cola de: la dirección, phishers, spamers o especialistas para el diseño e implantación de troyanos en páginas o correos, mulas de recepción de dinero, mulas de cuentas de primera transferencia, victimas. El primer paso es la obtención de correos electrónicos, las compran en la red misma, o bien las obtiene del famoso spam. Seguidamente los cerebros lanzan la campaña contra los usuarios de Internet, a ver quién pica. Para ello disponen de hackers profesionales a su servicio (…) En ocasiones las organizaciones disponen de los muleros del país, que se desplazan a otros países y llegan con diversas documentaciones falsas, abriendo cuentas bancarias en casi todas las entidades. En dichas cuentas reciben el dinero, que posteriormente sacan y envían a la Organización (…) A los muleros de otros países, los captan con ofertas de trabajo (Scam), o bien en foros, chats, anuncios, páginas web, etc. Y a las víctimas, las consiguen utilizando cualquier método de ingeniería social, o bien a través de troyanos instalados en páginas web, de forma que cuando la víctima entra en cualquiera de ellas, sin saberlo se le instala un troyano, específicamente diseñado, para que cuando el usuario, acceda a la banca on line, los datos sean captados y enviados a la Organización. Las mulas pueden llegar a ganar varios miles de euros en un mes, completamente ilegales, blanqueando el dinero de otros. Los últimos informes están señalando que el conseguir dinero por este

medio se está convirtiendo en una actividad en desarrollo en la Red (…) Los proxenetas de la red han puesto de moda el cibersexo online, consistente en video conferencia en tiempo real, y que se paga mediante la inevitable tarjeta de crédito. Invitaciones a canales privados, para entablar conversaciones privadas es común, donde el tema estrella es el sexo. Y lo más sobresaliente es que las mujeres han pasado a tomar la iniciativa, algo que en la vida real raramente harían. La pornografía infantil corre pasos similares a la prostitución organizada, pues en el momento en que se abusa de un menor y se obtiene una fotografía o video, es cuando el dinero empieza a tener un papel importante Hemos de tener en cuenta que en Internet hay más de 4.000.000 de sitios web que contienen imágenes, archivos, fotos videos de contenido sexual, y cada día se crean unos 500 sitios nuevos. Estas páginas reciben unos 2.000.000 de visitas anuales. Teniendo en cuenta que el 60 % de los sitios es de pago, se calculan, que este mercado mueve unos 950.000.000 de euros. Con el intercambio de fotografías y videos comienza la distribución y emerge el ánimo de lucro. Pero detrás de cada foto hay un criminal sexual, que consigue que a cambio de una cantidad de dinero que el menor realice ciertos actos obscenos. Hay que tener en cuenta que el 60 % de estos sitios es de pago. Por lo tanto, ni que decir tiene que Los Grupos de Crimen Organizado, controlan este tipo de páginas, unas ofrecen material erótico o pornográfico, y otras conversaciones, videos, fotos, videoconferencias. Con triple finalidad: cobran por mirar, te roban los datos bancarios, y encima utilizan tu ordenador para otras operaciones (es decir matan tres pájaros de un tiro, con unos beneficios económicos excepcionales. En resumen, un pastel demasiado apetitoso, como para renunciar a él. En general en el mercado del sexo virtual, no solo obtienen enormes beneficios las bandas del Crimen Organizado, sino que también ganan dinero, administradores de portales de Internet, propietarios de páginas web, proveedores de lugares, mediadores de contactos, productores, distribuidores, vendedores, publicistas, etc. (Blanco, s/f).

Después de leer algunos ejemplos sobre la actividad criminal de los ciberdelincuentes en el ciberespacio podemos inferir que estamos expuestos de muchas formas a ser víctimas por parte de estos criminales, además no debemos olvidar que la esfera en la que actúa la delincuencia organizada muta periódicamente y pone en un plano complicado de investigación y persecución penal a las autoridades de cada estado, no olvidemos que acciones como los fraudes en la red, phishing, ilícitos en contra de la propiedad intelectual e industrial, robo de identidad, clonación de tarjetas de crédito y/o Carding, ciberacoso, sabotaje informático, etc; son actividades que son recurrentes en la red y que a diario hay miles de víctimas a nivel mundial. Todo esto nos deja como tarea mejorar nuestra privacidad en los sitios web que visitamos, además debemos usar dispositivos electrónicos que sean seguros con un antivirus y con los firewall necesarios y activos y sobre todo tener conciencia que estamos en un inminente riesgo de ser víctimas por parte de la delincuencia común y organizada que interactúa en el ciberespacio.

9.4. Aspectos legales sobre la delincuencia organizada en Guatemala.

En los subtemas anteriores hemos destacado aspectos relevantes sobre la forma en que la delincuencia organizada actúa en el ciberespacio sin embargo no debemos olvidar que la delincuencia organizada se manifiesta de diversas formas y es que el presente capítulo se pretende que el lector conozca y analice la forma en que las estructuras criminales han actuado en su modus operandi en su forma convencional y su dinámica criminal en el ciberespacio. Cuando escuchamos sobre delincuencia organizada nos imaginamos a un grupo de personas que se reúnen para cometer diferentes actos ilícitos y donde su objetivo final es conseguir algún beneficio, ya sea de carácter económico o patrimonial y en otras para cumplir deseos o cubrir intereses de las diferentes élites del poder.

A nivel mundial escuchamos el termino de blanqueo de capitales como una forma a través de la cual se implementan mecanismos o estrategias para convertir una ganancia que se ha adquirido en forma ilegal e ilegítima como si fuera algo legal y legítimo es decir se intenta dar la apariencia de legalidad a actos en donde se han

obtenido ganancias cuando en realidad no ha sido así. Es menester apuntar que existen muchas actividades ilícitas que generan muchas ganancias y que los criminales necesitan darle apariencia de legalidad y legitimidad para que puedan usarse en la economía nacional sin mayores problemas, estas actividades pueden ser originadas por el narcotráfico, venta de armas y órganos, contrabando y defraudación tributaria, pago de coimas a funcionarios públicos, juegos de azar, delitos informáticos, delitos de telemarketing, extorsión, lavado de dinero digital a través de ataques a los juegos en línea, etc.

En Guatemala existen diferentes instrumentos legales que tienen por objeto prevenir controlar vigilar y sancionar las actividades de la delincuencia organizada tales como el Decreto 21-2006 del Congreso de la República (Ley contra la Delincuencia Organizada), Ley contra la Narcoactividad, Ley contra el Lavado de Dinero u otros activos, Ley de Migración, Ley para Prevenir y Reprimir el Financiamiento del Terrorismo, Ley contra la Corrupción, Ley contra la Defraudación y el Contrabando Aduanero, Ley de Armas y Municiones, la Ley de Extinción de Dominio, todas las anteriores con su reglamento respectivo y por último el Código Penal. Estas normativas jurídicas tienen particularidades en cada caso y que en su conjunto están creadas en forma armónica para el combate a la actividad criminal de la delincuencia en especial a la delincuencia organizada que se manifiesta de muchas formas, como ya lo comentamos anteriormente.

El autor Julio Rivera Clavería en su texto “El Crimen Organizado” realiza un análisis sobre las características del crimen organizado en Guatemala, indicando que:

> Investigar las causas que dieron origen a la criminalidad organizada en Guatemala es una tarea compleja, sin embargo, existen algunos hechos claves en la historia reciente del país que podrían explicar el fenómeno criminal, siendo estos: 1. La guerra civil que se libró en Guatemala durante 36 años evitó que el crimen organizado pudiera articularse y expandirse en el país, por lo que, con el advenimiento de la nueva era democrática como sistema político y con el final del conflicto armado, así como con la

> desestructuración operativa de los grupos antagónicos que en el conflicto intervinieron, se favorece la criminalidad organizada. 2. La debilidad del Estado guatemalteco es una realidad innegable, así mismo lo es la fragilidad de sus instituciones para atender no sólo las demandas de la población sino para ejercer su autoridad y el monopolio de la fuerza en todo el territorio nacional. 3. Factores externos como el fenómeno de la globalización económica, tecnológica y de las comunicaciones igualmente hicieron posible la globalización de la criminalidad, por lo cual surgen nuevos actores, nuevas amenazas y, sobre todo, se consolida y expande el crimen organizado local y se vincula a la transnacional. (Rivera Clavería, 2011)

El autor citado menciona también las principales actividades del crimen organizado en Guatemala, explicando:

> Existe una fuerte tendencia en el país por parte de las organizaciones criminales a la especialización del delito por lo que, independientemente de que las organizaciones criminales puedan mutar a otros delitos dependiendo de las circunstancias del momento, su especialidad las hace mucho más efectivas en la realización de su accionar ilegal y como resultado, sus ganancias económicas se incrementan. Para el caso de Guatemala se identifican las siguientes amenazas: 1. La Narcoactividad 2. El tráfico ilegal de migrantes y personas 3. El lavado de activos 4. Tráfico de armas de fuego de tipo defensivo 5. Extorsiones 6. Secuestros 7. Robo de vehículos 8. Sicariato y otros. (Rivera Clavería, 2011)

Con base a lo anterior podemos asegurar que el crimen organizado transnacional seguirá aumentando y en el caso de Guatemala a pesar que existe legislación para contrarrestar la dinámica criminal organizada, ésta no es suficiente en virtud que los cambios tecnológicos y la globalización digital traen consigo modelos de cooperación y ayuda mutua entre las organizaciones criminales a nivel mundial y tal como lo apunte, la delincuencia organizada invierte mucho en recurso humano

preparado en el manejo de las TIC y asimismo en inteligencia similar a la militar en el entendido que se efectúa una contrainteligencia por parte de estas estructuras criminales que les ayuda a tener el dominio y el poder no solo en un territorio sino también en el ciberespacio.

9.5. Mecanismos de investigación para combatir la delincuencia organizada.

En los capítulos anteriores hemos observado y conocido la importancia del conocimiento sobre derecho informático, protección jurídica de los datos, delitos informáticos, informática jurídica, la cadena de custodia digital, los protocolos aplicados en la informática forense, el perito forense digital, la prueba electrónica y digital y ahora sobre la delincuencia organizada, todo esto nos lleva ahora a unificar todos esos conceptos y conocimientos para armar esos mecanismos de investigación que nos ayudarán para contrarrestar la actividad ilegal de la delincuencia o crimen organizado. Guatemala cuenta con una amplia normativa al respecto, sin embargo, también hay que tomar en cuenta que existen otros tratados o instrumentos internacionales que también coadyuvan a esta labor tales como los suscritos en la Convención de Palermo, Convenio de las Naciones Unidas contra la Delincuencia Organizada Transnacional, Convención de las Naciones Unidas contra la Corrupción, entre otros. Tanto en la normativa jurídica tanto de carácter interno como internacional persigue el objetivo de descubrir y sancionar aquellas conductas y patrones ilícitos que día a día mutan y tienen una conversión constante cuya característica es que se agencian de mecanismos más y más complejos que hace una tarea ardua para las autoridades en cuanto a la persecución penal correspondiente. Importante resulta la función de las autoridades policiales que en el caso de Guatemala resulta relevante mencionar a la Unidad de Delitos Informáticos, la División de Información Policial (INTERPOL), División de Policía Internacional, la Subdirección General de Investigación Criminal, Gabinete Criminalístico, el Centro de Recopilación análisis y difusión de información criminal (CRADIC), entre muchas más que son parte esencial en el área de inteligencia y estrategia policial en materia de investigación y que junto al Ministerio de Gobernación deben dar una respuesta para contrarrestar el flagelo de la proliferación de la delincuencia organizada en Guatemala.

Extorsiones, asesinatos, robo de vehículos, narcotráfico, ingreso y tráfico ilegal de personas, secuestro, lavado de dinero, tráfico ilegal de armas, malversación, fraude, asociación ilícita, cohecho, lavado de dinero u otros activos, intermediación financiera, financiamiento del terrorismo, obstrucción extorsiva de tránsito, entre muchos más tipos penales en relación a la delincuencia organizada y que están regulados en la legislación guatemalteca deben tener un mecanismo efectivo para su investigación, persecución y sanción y aunado a la proliferación de los delitos informáticos y la actividad criminal de los ciberdelincuentes en el mundo digital, crea un gran reto para los actores del sector justicia a efecto de combatir de manera eficaz y eficiente este flagelo. No podemos pensar en una investigación eficiente si se utilizan los medios de investigación convencionales, por lo que el Estado debe implementar mecanismos innovadores acorde a la dinámica criminal organizada. El Estado debe responder a esa necesidad de proveer justicia a sus ciudadanos, es decir debe ir un paso por delante a la delincuencia organizada. Aspectos como la impunidad y la corrupción afectan gravemente la imparcialidad, objetividad y avance de una investigación, sin embargo, hay que resaltar que la cooperación internacional es importante en la investigación de estructuras criminales transnacionales y que esto también es parte de estudio del derecho informático en el área de Ciberespacio y flujo de datos fronterizos.

En Guatemala se encuentra vigente y positiva la Ley contra la Delincuencia Organizada cuya estructura en sus aspectos relevantes se encuentra lo relativo a: a) Los Medios para investigar grupos delictivos organizados y delitos de grave impacto social. b) Métodos especiales de investigación. Es muy interesante la forma en que se utilizan los medios especiales de investigación en Guatemala tales como: las operaciones encubiertas (Art 21-34) las entregadas vigiladas (Art 35-47) y las interceptaciones telefónicas y otros medios de comunicación (Art 48-71), toda vez que actualmente el Ministerio Público las utiliza para la persecución penal y han resultado efectivas, sin embargo, hay algunos vacíos técnicos que mencionaremos más adelante. También resulta relevante la implementación del Derecho Penal Premial a través de la regulación legal del colaborador eficaz (Art 90-104) que en muchos casos es clave para la desarticulación de estructuras criminales.

El autor Julio Rivera Clavería nuevamente en su texto “El Crimen Organizado” simplifica la forma en que funciona cada uno de estos métodos especiales de investigación y refiere que:

> a) Los Agentes Encubiertos: Son los funcionarios policiales especiales que voluntariamente, a solicitud del Ministerio Público, se les designa una función con la finalidad de obtener evidencias o información que permitan descubrir y procesar a los miembros de grupos delictivos organizados. Los agentes encubiertos podrán asumir transitoriamente identidades y roles ficticios, actuar de modo secreto y omitir la realización de los procedimientos normales de su cargo ante la comisión de delitos, para optimizar las investigaciones y el procesamiento de los integrantes de las organizaciones (…) b) Las Entregas Vigiladas: Consiste en el método de investigación que permite el transporte y tránsito de remesas ilícitas o sospechosas, así como de drogas o estupefacientes y otras sustancias, materiales u objetos prohibidos o de ilícito comercio, que ingresen, circulen o salgan del país, bajo la estricta vigilancia o seguimiento de autoridades. Se utiliza para descubrir las vías de tránsito, el modo de entrada y salida del país, el sistema de distribución y comercialización, la obtención de elementos probatorios, la identificación y procesamiento de los organizadores, transportadores, compradores, protectores y demás partícipes de las actividades ilegales (…) c) Las Interceptaciones Telefónicas y otros medios de comunicación: Consiste en la intercepción, grabación y reproducción con autorización judicial de las comunicaciones orales, escritas, telefónicas, radiotelefónicas, informáticas y similares que utilicen el espectro electromagnético, así como de cualesquiera de otra naturaleza que en el futuro existan cuando sea necesario evitar, interrumpir o investigar la comisión de los delitos regulados en la Ley Contra la Delincuencia Organizada. (Rivera Clavería, 2011)

En el caso del agente encubierto está regulado en la Ley contra la Delincuencia Organizada como “Operaciones Encubiertas” y es menester apuntar que acá es relevante la infiltración policial que realiza dentro de las estructuras criminales para saber el modo de operar de la organización criminal sin embargo debemos diferenciar los conceptos de infiltración policial y un agente encubierto en virtud que el primero es la técnica o estrategia a través de la cual se planifica que un agente encubierto ingrese a la estructura criminal mientras que el segundo es la persona que realiza todas las acciones necesarias para conocer el modus operandi de la organización criminal es decir se convierte en un órgano de investigación.

En el caso de las entregas vigiladas se ha utilizado principalmente para conocer la ruta en el trasiego de droga o estupefacientes en los diferentes Estados, consecuentemente esta técnica de investigación es susceptible de ser utilizado en el ámbito internacional, sin embargo, en el caso de Guatemala se utiliza para la investigación de varios tipos de casos como por ejemplo en el caso de extorsiones, plagio o secuestro. Instrumentos internacionales que regulan esta técnica de investigación es lo contenido en la Convención de las Naciones Unidas contra el Tráfico ilícito de estupefacientes y sustancias psicotrópicas y en la Convención de Viena. Esta forma de investigación es importante para adquirir evidencia y que posteriormente se presentará como prueba ante un juez competente.

Nos corresponde ahora analizar lo relativo a las interceptaciones telefónicas y otros medios de comunicación y es que de conformidad a lo regulado en el artículo 49 de la Ley contra la Delincuencia Organizada y según la Instrucción General del fiscal general y jefe del Ministerio Público número 06-2011 corresponde al fiscal solicitar la autorización de la interceptación de las comunicaciones. En la práctica la unidad encargada de solicitar las interceptaciones telefónicas es la Unidad de Métodos Especiales de Investigación del Ministerio Público quien a requerimiento del fiscal encargado del caso debe justificar ante el Juez contralor la necesidad e idoneidad de ese método de investigación para recabar más indicios que fortalezcan el requerimiento fiscal que en su momento procesal se presentare. Para salvaguardar los derechos fundamentales de las personas sujetas a investigación es necesario que atender lo que

regula el artículo 24 de la Constitución Política de la República de Guatemala, articulo 12 de la Declaración Universal de los Derechos Humanos, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, artículo 11.2 de la Convención Americana de Derecho Humanos que se refieren al derecho a la privacidad e intimidad de las personas en sus medios de comunicación salvo resolución por juez competente en los casos que determine la ley. Es muy importante mencionar que el Ministerio Público debe contar con los equipos informáticos adecuados para monitorear el flujo de información que surge de las comunicaciones interceptadas, consecuentemente la información que surja y se considere que servirá como evidencia debe almacenarse en discos compactos embalados en una bolsas especiales o Faraday conjuntamente con el inicio de la cadena de custodia. Las grabaciones son transcritas en acta y se pueden entregar en forma diaria, semanal, quincenal o mensual según sea el requerimiento del caso, asimismo la información puede ser grabada en esa misma mecánica.

9.6. La valoración de la prueba electrónica y digital en casos de delincuencia organizada.

En este capítulo hemos desarrollado aspectos interesantes sobre la delincuencia organizada y los métodos especiales de investigación, sin embargo debemos enfatizar que a nivel mundial las estructuras criminales tienen una capacidad impresionante para adaptarse a cada contexto económico y geopolítico creando alianzas con otras organizaciones criminales, consecuentemente se hace necesario conocer como las autoridades estatales y específicamente los actores del sector justicia responden al flagelo de la delincuencia organizada transnacional no solo en su forma de operar convencional sino también en el ciberespacio y el mundo digital propiamente dicho; en este espacio nos referiremos a analizar sobre la forma en idealmente puede valorarse la prueba electrónica y digital en casos de delincuencia organizada en Guatemala.

Es menester indicar que los ciberdelincuentes frecuentemente cambian sus patrones de conducta y la forma de comportarse en el ciberespacio y es por ello que se rompe el esquema convencional o tradicional de la delincuencia común en cuanto a la consumación de los delitos es decir los ciberdelincuentes tienen una gran variedad de opciones en la red para cometer actos ilícitos aprovechando todos los recursos que

existen, consecuentemente estos actos ilegales tienen la particularidad que trascienden fronteras y es ahí donde la persecución penal es compleja en virtud de las legislaciones de cada Estado que en muchos cosas no están en una misma sintonía para la acción y persecución penal especialísima relativa a la actividad ilegal de los ciberdelincuentes que por ende los Estados no tienen más que adaptar de manera apresurada y hasta arbitraria procedimientos e institutos procesales para conocer y juzgar hechos en donde existen cibercriminales, evidencia electrónica y digital, etc. Es por ello que se escucha ahora del término “Ecosistema Digital Criminal” que una forma de cooperación entre autoridades nacionales e internacionales para crear estrategias eficientes de acción para combatir los delitos informáticos. Para nadie es un secreto que las organizaciones criminales a nivel transfronterizo actúan en forma coordinada y estructurada de tal forma que en diferentes plataformas sociales de la red oscura y red profunda se comparten ideas, estrategias, acciones y propuestas para mejorar la efectividad de sus actividades ilícitas es decir actualmente existe esa contrainteligencia digital en la cual los ciberdelincuentes van un paso delante de las autoridades.

a) De la afectación a diferentes bienes jurídicos tutelados: A título personal se considera que en Guatemala existen muchas formas en que la delincuencia organizada actúa y atenta contra diferentes bienes jurídicos tutelados, menciono algunos a continuación:

i. Uso de Phishing para sustraer datos como correo electrónico, usuario y contraseña con el objeto de atacar la banca electrónica de los usuarios consecuentemente se consuman los delitos de hurto, robo y casos especiales de estafa. (Arts. 246, 251, 264 del Código Penal)
ii. Ataques de servidores de información, equipos de cómputo, bases de datos y páginas web con gusanos, virus o malware a efecto de borrar, sustraer o modificar información tipificando estos hechos en los tipos penales de: Destrucción de registros informáticos, alteración de programas, manipulación de información, uso de información y programas destructivos. (Arts. 274 “A”, 274 “B”, 274 “D”, 274 “E”, 274 “F” del Código Penal)

iii. Intimidación a las personas utilizando diferentes plataformas digitales de comunicación o redes sociales, que de conformidad a nuestra legislación podría considerarse como una calumnia, injuria, difamación y publicación de ofensas coacción, amenaza, coacción contra la libertad política (Arts. 159, 161, 164, 165, 214, 215, 216 del Código Penal).

iv. Creación, difusión y promoción de la pornografía a través de diferentes plataformas digitales utilizando una diversidad de dispositivos electrónicos que de conformidad a nuestra legislación podría considerarse su encuadramiento en los tipos penales que regula la Ley contra la Violencia Sexual, Explotación y Trata de Personas en su Título IV, que reforma varios artículos del Código Penal.

v. En el delito de Lavado de Dinero u otros activos la delincuencia organizada en Guatemala ha implementado diferentes mecanismos para consumar actos ilícitos tales como: El desvío de recursos del Estado utilizando sociedades o empresas de “cartón” o fachada en que se simula la prestación de servicios, apertura de cuentas bancarias utilizando documentos falsos o documentos que han recopilado a través de redes sociales con la supuesta justificación de un ofrecimiento de trabajo y que finalmente las referidas cuentas sirven para el cobro de extorsiones, siendo estos solo algunos casos y que de conformidad a nuestra legislación podría considerarse su encuadramiento en los tipos penales que regula el Decreto 67-2001 Ley contra el Lavado de Dinero u otros activos. Además es importante mencionar que un mecanismo que han implementado para el lavado de dinero es el uso de las criptomonedas en diversas modalidades tales como la promesa de ganancias sobre inversiones simuladas en criptomonedas y en otros casos el criptolavado en el que se compran fuertes sumas de bitcoins, como ejemplo, en un país determinado para luego ser trasladados a otros países y ser canjeados en el sistema financiero del país de destino sin ningún tipo de problemas y que posteriormente son utilizadas para comprar armas, drogas, etc. Por ejemplo, en el mercado negro de la “red oscura”

la mayoría de transacciones y negocios se realiza mediante el uso de criptomonedas.

b) De las conductas no reguladas en nuestra legislación: Existen algunas conductas ilícitas que expresamente no están reguladas en nuestra legislación sin embargo es necesario considerarse a efecto de prevenir la comisión del delito, estas son las siguientes:

i. Clonación de tarjetas de crédito y uso del skimmer para obtener la información electrónica sobre los datos del cuentahabiente.
ii. Conductas ilícitas de la delincuencia organizada referida a las nuevas tecnologías de la información.
iii. Las acciones en donde son utilizadas las llamadas “botnets” cuya dinámica es que a través de un Phishing se estafa a cientos de personas al mismo tiempo, pero en ubicaciones diferentes y distantes y que consecuentemente los depósitos bancarios o transferencias bancarias irán a un país diferente o paraíso fiscal con otro tipo de regulaciones jurídicas.
iv. La propagación de fotos y videos con contenido pornográfico en las redes sociales y que después de haber juzgado a los responsables y haber resarcido a la víctima, ese material que afecta la indemnidad sexual aún se encuentra alojada en servidores de otros países y que una orden judicial de Guatemala no es suficiente para obligar a que se elimine de un determinado sitio web.
v. Uso de hacking para obtener información personal y sensible de las personas.
vi. Descubrimiento y revelación de secretos informáticos tanto en el ámbito privado como público.
vii. Vulneración a la protección de datos personales mediante ataques informáticos.
viii. Regulación del hacking ético como medida preventiva o demostrativa sobre ataques realizados en contra de sistemas informáticos, bases de datos o personas.
ix. Regulación legal para el combate en la proliferación del Carding y skimming.

x. Estafas informáticas, cuya dinámica se caracteriza por la regulación legal de aquellas conductas en que el apoderamiento ilícito se realiza mediante el uso de la tecnología.

xi. Regulación legal de la denegación de servicios en donde se crean daños a sistemas de información o sitios web.

xii. Reforma a la Ley de Derechos de Autor y Derechos Conexos y la Ley de Propiedad Industrial relativo a la sanción punible de aquellos actos en donde se efectúa plagios de las invenciones e innovaciones del titular del derecho.

xiii. Ciberterrorismo digital o informático.

xiv. Regulación legal de la información que almacenan y procesan los dispositivos electrónicos en relación al internet de las cosas.

c) Consideraciones para abordar y valorar la prueba electrónica y digital.

Actualmente existe el Convenio de Cibercriminalidad de Budapest elaborado por el Consejo de Europa y acordado en Hungría el veintitrés de noviembre de dos mil uno, es interesante analizar que diferentes países se adhirieron a este instrumento internacional cuyo objeto era crear los cimientos necesarios en relación a las políticas internas para la persecución penal de los ciberdelitos, es decir, la creación de una legislación para cada uno de los Estados firmantes encaminados a la cooperación mutua para la persecución penal de esas conductas típicas y lesivas para ser investigadas, no sólo en el estado miembro sino también crear los mecanismos necesarios para la persecución penal y estratégica en diferentes estados a través de la cooperación internacional a efecto de proteger intereses legítimos de cada Estado en relación a las tecnologías de la información y comunicación. Se debe considerar que en este convenio se adoptaron estrategias y medidas para que los procedimientos pudieran ser eficientes.

Es menester conocer como el Derecho Informático contribuye y se relaciona con el Derecho Penal; en un primer escenario debemos recordar que este último en un sentido amplio comprende tres áreas de estudio: la parte sustantiva, la adjetiva y de ejecución y que específicamente en la parte sustantiva en su parte especial se encuentra el catálogo de tipos penales y sus respectivas sanciones y que en el caso

que nos amerita en el presente artículo, tendríamos que encontrar todo aquellos supuestos que regulen las conductas ilícitas que constituyan una vulneración al uso incorrecto de la tecnológica, sin embargo Guatemala no cuenta con un catálogo amplio y contextualizado en esta materia.

A) En el ámbito de la identificación, obtención y recolección de evidencia electrónica y digital actual la Dirección de Investigación Criminalística del Ministerio Público y debemos preguntarnos:

a. ¿Son Peritos Forenses Digitales, E-Discovery, ¿primer respondiente o alguna especialización?
b. ¿Son capaces de discriminar la evidencia electrónica y digital del resto de evidencia?
c. ¿Utilizan bolsas de Faraday e inician una custodia de cadena digital junto a la física?
d. ¿Utilizan la clonación de imágenes forenses in situ?

B) En el ámbito de preservación de la evidencia electrónica y digital cuestionemos:

a. ¿En qué dispositivos de almacenamiento se guarda la información recolectada en un escenario criminal digital?
b. ¿En dónde se almacenan los dispositivos electrónicos objetos a posterior análisis?

C) En el ámbito del análisis de la evidencia electrónica y digital cuestionemos:

a. ¿Qué protocolos de análisis se utilizan?
b. ¿Qué calidades ostentan las personas encargadas de efectuar el análisis?

D) por último en el ámbito de la presentación de resultados:

a. ¿Cuándo se presentan los resultados ante juez competente, qué tipo de informes son entregados?
b. ¿Se utiliza la cadena de custodia digital en el Juicio Oral y Público?

Derivado de estos cuestionamientos debemos analizar los que regula la norma y para ello citamos lo que refiere el artículo 226 del Decreto 51-92 del Congreso de la República referente a la calidad de los Peritos y es que en textualmente hay un apartado que refiere (…) “Si por obstáculo insuperable no se pudiera contar en el lugar del procedimiento con un perito habilitado, se designará a una persona de idoneidad manifiesta” En el ámbito forense actual se toma como valido el informe rendido por personal del Instituto de Nacional de Ciencias Forenses en materia de evidencia electrónica y digital, en casos determinado, sin embargo debemos advertir que cada uno de los técnicos que ahí labora tienen una especialización determinada o forman su propia preparación, sin embargo cuestionemos: ¿Cuántos técnicos del Instituto Nacional de Ciencias Forenses son Peritos Forenses Digitales o tienen expertiz para manejar las áreas de la informática forense? En la práctica a pedido de parte se llama bajo la figura del Consultor Técnico a un Ingeniero en Sistemas, Licenciado en Informática, Ingeniero en Telecomunicaciones, entre otros, para debatir o efectuar aclaraciones sobre un dictamen de peritos de INACIF, sin embargo tanto en Peritos como en Consultores Técnicos se adolece de un criterio definido sobre su idoneidad en virtud que en el campo de la informática forense las competencias y habilidades que se deben poseer son especializadas y que ya apuntamos anteriormente; debemos advertir que en muchas ocasiones a pesar que se tiene un título académico que en documentos acredita la idoneidad esto no significa que automáticamente se tenga la habilidad para efectuar un contraperitaje tecnológico y actuar en el ámbito de la informática forense debatiendo y argumentando sobre prueba electrónica y digital.

Por último, mencionaremos aspectos importantes que a criterio del autor deben tomarse en cuenta en la etapa de juicio oral en el proceso penal, se mencionan las siguientes:

1. En el debate oral y público debe comprobarse o desvirtuarse, según sea el caso, el desarrollo de la acción y la participación de cada uno de los acusados en circunstancias de modo, tiempo y lugar de conformidad al rol que desempeñaron en la manipulación de los dispositivos electrónicos.

2. En el debate oral y público debe comprobarse o desvirtuarse, según sea el caso, el rastro digital que incrimina a los acusados en circunstancias de modo, tiempo y lugar y que pueda acreditarse mediante los informes periciales que presente el experto pertinente.

3. Se acrediten fehacientemente las agravantes que sustentan la culpabilidad de los acusados, discriminando cada acción y cada rol que realizaron los enjuiciados dentro de la organización criminal.

4. En el caso de las actas, discos y prueba originada por una interceptación telefónica y otros medios de comunicación, debe asegurarse la cadena de custodia física y digital, asimismo evitar que el fiscal a cargo de la investigación incurra en realizar inspección ocular del disco que contiene las grabaciones originales de las interceptaciones, es decir que se realice en forma unipersonal sin autorización de juez y sin presencia de los demás sujetos procesales.

5. No confundir la prueba de análisis forense de audios con el análisis forense de voces que son dos pericias totalmente diferentes y que tienen por efecto acreditar diferentes extremos; en el caso del primero nos servirá para acreditar que los audios no han sido dañados, alterados o modificados mientras que el segundo nos ayudará a encontrar coincidencias o diferencias entre las voces una dubitada y otra indubitada.

6. Valorar la prueba digital que se extraiga del internet de las cosas, de las redes eléctricas inteligentes y de infraestructuras críticas. (Electrodomésticos, domótica, sistemas de control de información, sistemas de salud y transporte, etc)

En virtud de lo anterior es necesario mencionar algunos aspectos finales a los estimados lectores para que puedan sacarle provecho a este tipo de pruebas que más adelante en debate oral y público podrán hacerla valer como prueba legítima y legal:

1. Un pantallazo o captura de pantalla impresa en papel no es prueba digital, si ve esto en un ofrecimiento de prueba debe argumentar su invalidez notoria.

2. Si la información es generada, enviada, recibida, almacenada o transmitida por algún dispositivo electrónico, se considera prueba digital, previo cumplimiento de todas las fases de la actividad probatoria.

3. Si se obtiene información que deriva de un mensaje de datos, este debe ser integro de conformidad a la Cadena de Custodia Digital y la certificación digital correspondiente.

4. No hay equivalencia de condiciones en la apreciación y valoración de una prueba digital y prueba documental, es decir no puede tratarse con la misma técnica ni emitirse un juicio de valor sin conocer los protocolos y normas procedimentales específicas para evaluar la legalidad de esta prueba.

5. De conformidad a la teoría de la prueba ésta es autónoma de la prueba documental y pericial en cuanto a los mecanismos e inserción para su validez legal.

6. El profesional competente el tratamiento de la evidencia digital es el Digital Computer Forensic o Perito Forense Digital y se debe restar credibilidad a la supuesta prueba digital cuando es manipulada y presentada por un Técnico en Escena del Crimen, analista criminal, agente policial o perito si este no tiene acreditada sus facultades para practicar la pericia y si tampoco se ajusta a la norma ISO/IEC 27037:2012, es decir quedaría sin valor probatorio la evidencia obtenida o en debate quedaría desechada la prueba electrónica o digital.

CAPITULO X

Presentación de Resultados.

En el presente capítulo se presentan los resultados del trabajo documental y de campo que se efectuaron, explicando la forma en que se aplicaron las técnicas de investigación utilizadas, así también, los resultados que se obtuvieron del muestreo utilizando los dos instrumentos de recopilación de información siendo ellos la entrevista y la encuesta, por último, se detalla la interpretación de los resultados cuantitativos y un análisis de los resultados cualitativos.

10.1. Contexto.

La presente investigación se desarrolló a consecuencia del siguiente cuestionamiento:

1. ¿Existe seguridad jurídica y legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada?

Tomando en consideración la problematización del objeto que es tema de estudio, se definió la siguiente hipótesis:

2. No existe seguridad jurídica ni legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada dentro del proceso penal guatemalteco, como consecuencia de la inexistencia de procedimientos uniformes y reglamentados, poco conocimiento y uso escaso de los procedimientos adecuados para la obtención, recuperación, reproducción, conservación, análisis e incorporación de la información.

Después de efectuar la investigación se descubrió que el problema de estudio tiene matices más específicos en su campo de aplicación y que se vio reflejada en la operacionalización de la segunda variable independiente, sufriendo una ampliación,

quedando así de la siguiente forma:

3. No existe seguridad jurídica ni legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada dentro del proceso penal guatemalteco, como consecuencia de la inexistencia de procedimientos uniformes y reglamentados, poco conocimiento y uso escaso de los procedimientos adecuados para la identificación, recopilación, recuperación, reproducción, análisis, preservación, y presentación de la información.

La investigación tuvo como fin de conocer diferentes extremos siendo los siguientes:

1. El estado actual de la forma en que es utilizada y valorada la prueba electrónica y prueba digital en el proceso penal guatemalteco con ocasión que los actores responden al ámbito de la delincuencia organizada y en algunos casos corresponden a la competencia de mayor riesgo.

2. Se estudió desde el punto de vista de la norma jurídica vigente la legalidad de los procedimientos utilizados por el Ministerio Publico para recabar la evidencia electrónica y digital en el escenario criminal y su posterior ofrecimiento de prueba en el momento procesal correspondiente.

3. Además, se estudió la posterior valoración judicial que se le dan a estas pruebas por los diferentes órganos jurisdiccionales que conocen casos relacionados a delincuencia organizada y en otros de delincuencia común; estudiando la postura y argumentos de los fiscales y abogados litigantes para sostener sus argumentos, en donde se diligencian pruebas digitales y electrónicas,

4. Se analizó de esa misma cuenta el grado de efectividad que se le otorga a este tipo de prueba y la forma en que los jueces le otorgan valor probatorio

influyendo en la resolución de una sentencia condenatoria o absolutoria.

5. Se estudiaron diferentes escenarios jurídicos y que aunado a la recopilación de datos se pudo conocer la postura y conocimiento que tienen abogados litigantes, fiscales y jueces sobre el derecho informático, informática forense que va íntimamente ligado con el tratamiento de la prueba electrónica y digital.

6. Se analizaron las consecuencias jurídicas se tienen implícitas en la correcta o errónea aplicación de procedimientos o protocolos de seguridad para diligenciar la prueba electrónica y prueba digital para darle certeza jurídica. Además,

7. Se efectuó un análisis de diferentes instituciones internacionales y entes estatales que auxilian al Ministerio Público en la obtención de la prueba digital y electrónica, observándose los diferentes peritajes que pueden aplicarse a este tipo de pruebas.

8. Se realizó un estudio del derecho comparado con el objeto de analizar los diferentes procedimientos y protocolos que se utilizan dentro del derecho procesal penal de algunos países en donde se tiene un avance en materia de derecho informático en donde se tienen normativas jurídicas sólidas, claras y aplicables que coadyuvan al buen desenvolvimiento y diligenciamiento de la prueba electrónica y digital que de esa misma cuenta se hacen valer los diferentes agentes e interactúan en el sistema de justicia para hacer valer su postura y sostener su hipótesis, respetándose con ello los principios de igualdad de las partes procesales, derecho defensa, debido proceso y legalidad de la prueba.

La investigación de campo se dirigió a abogados litigantes, fiscales y jueces del departamento de Quetzaltenango y otros profesionales que no obstante siendo originarios de otros departamentos tales como Guatemala, Huehuetenango, San Marcos, Totonicapán, Retalhuleu, Suchitepéquez desarrollan sus labores profesionales en el departamento de Quetzaltenango.

Actualmente el departamento de Quetzaltenango cuenta con un Centro Regional de Justicia ubicado en la Diagonal 10 0-34 de la zona 6 de la ciudad de Quetzaltenango, cuenta con tres edificios uno que donde se encuentran las judicaturas en materia civil, familia y laboral, en otro se desarrollan las funciones administrativas y en otro se localizan diferentes judicaturas con competencia en casos penales y que conformidad a su organización interna y ampliación de cobertura actualmente se rige por el Acuerdo 11-2015 de la Corte Suprema de Justicia que regula el funcionamiento y competencia del Juzgado de Primera Instancia Penal Narcoactividad y Delitos contra el Ambiente de departamento de Quetzaltenango que actualmente funciona bajo la modalidad de siete turnos y el personal administrativo correspondiente. Actualmente, también se encuentra en funciones el Juzgado de Primera Instancia Penal Narcoactividad y Delitos contra el Ambiente en procesos de Mayor Riesgo con sede en el municipio y departamento de Quetzaltenango según el Acuerdo de creación 26-2016 de la Corte Suprema de Justicia que conoce competencia a razón de territorio casos provenientes de los departamentos de Suchitepéquez, Retalhuleu, San Marcos, Huehuetenango, Totonicapán, Quiché, Sololá y Quetzaltenango y que a razón de materia conocen casos según lo regula la Ley de Competencia Penal en Procesos de Mayor Riesgo Decreto 21-2009 del Congreso de la República y reforma según Decreto número 35-2009 de Congreso de la República los casos que resuelva Cámara Penal respecto a los requerimientos que le fueran planteados.

Para el efecto se procedió a encuestar y entrevistar a abogados litigantes, fiscales y personal de la Dirección de Investigaciones Criminalísticas del Ministerio Público y jueces en el Centro Regional de Justicia y oficinas jurídicas y sedes fiscales, mismos que desarrolla sus funciones en el ámbito penal.

10.2. Técnicas de investigación utilizadas.

Las técnicas de investigación cuantitativas utilizadas fueron, la encuesta y la estadística y el instrumento de investigación de recopilación de información cualitativa fue la entrevista. La encuesta fue dirigida a una determinada muestra de abogados

litigantes, fiscales para conocer sobre el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada y de esa misma cuenta se utilizó la estadística para conocer con datos numéricos y porcentuales sobre el objeto de estudio en el departamento de Quetzaltenango y la entrevista fue dirigida a jueces, fiscales y abogados litigantes determinados por la posición o cargo que ostentan o en su defecto por el conocimiento previo de abogados litigantes que se dedican al litigio penal.

El universo y el muestreo de la presente investigación se determinó tomando en cuenta en primera instancia por el número de fiscalías especializadas que conocen casos de delincuencia organizada en Quetzaltenango, la cantidad de abogados que están asociados en el departamento, la cantidad de jueces en materia penal en rol de turnos y la cantidad de jueces de mayor riesgo que desempeñan funciones en Quetzaltenango. Los datos cuantitativos fueron recabados de conformidad a fuentes abiertas de información que se encuentran en páginas de redes sociales de Asociaciones de Abogados y Notarios de Quetzaltenango, Tribunal Electoral y Registro de Ciudadanos de Quetzaltenango, tomando como referencia la última elección para elegir a miembros de Junta Directiva del Colegio de Abogados y Notarios de Guatemala, obteniendo para el efecto solo datos numéricos mas no datos sensibles y personales en virtud que estos no se encuentran en estas fuentes de información.

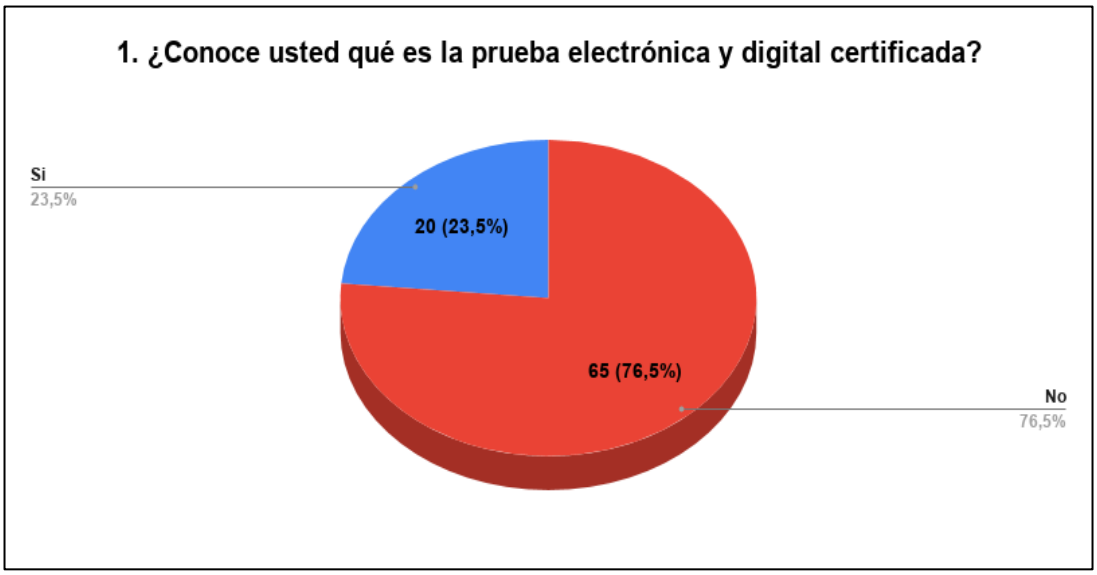
Son un total de 835 abogados y se consideró una muestra de 10% que es suficiente para reflejar representatividad dando como resultado 83.5, sin embargo, fueron encuestados 85 abogados, para ello se empleó un muestreo aleatorio simple.

En cuanto a las entrevistas se decidió entrevistar a un total de cuatro jueces de primera instancia penal, un juez de instancia penal en procesos de mayor riesgo, un fiscal especial y dos abogados litigantes, siendo un total de ocho profesionales del derecho. Se efectuó ese filtro de conformidad a la técnica del muestreo por juicio en virtud que existe un número restringido de profesionales del derecho que poseen determinadas cualidades en función del puesto que ostentan y desarrollan, además de la experiencia que poseen, considerándose idóneas para contestar las interrogantes que conformaron la guía de entrevista.

10.3. Encuesta

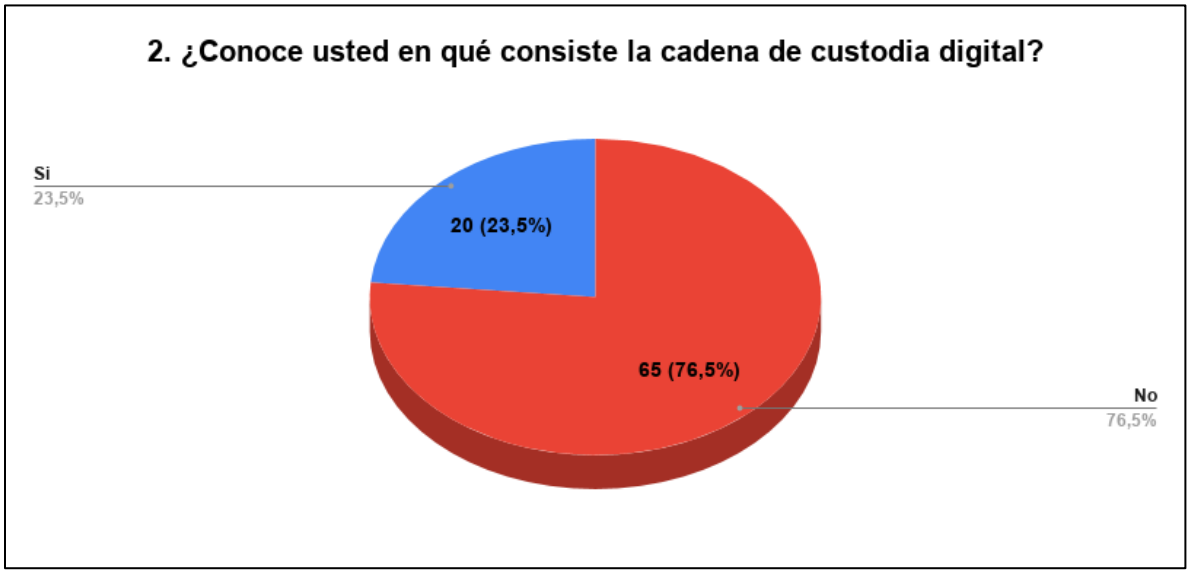
A continuación, se describe cada uno de los cuestionamientos, su representación en forma gráfica circular, además se realiza un Resultado de las respuestas.

- **Cuestionamiento No. 1. (Gráfica No.1)**



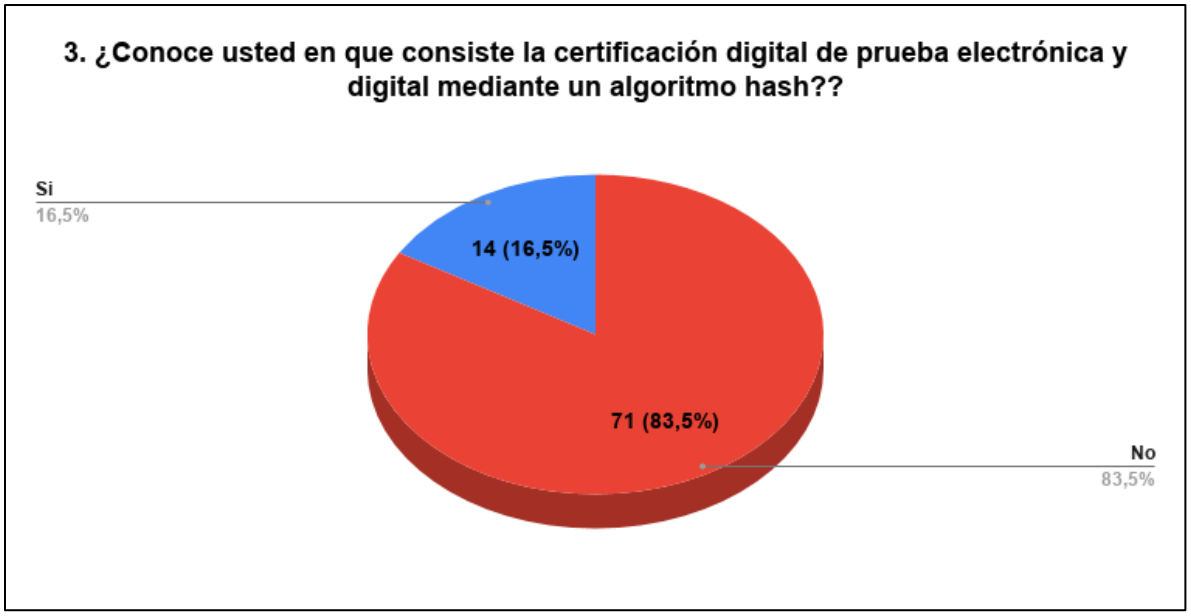
- **Resultado (1):** Del total de personas encuestadas, 20 respondieron “Si”, lo cual representa un 23.5% y 65 personas respondieron “No”, lo cual representa el 76.5%. Dentro de la explicación que los encuestados señalan manifiestan que: se enfocan a que la prueba electrónica y digital son las que se den en plataformas digitales, que es prestablecida, se firman con equipos especializados, se obtienen de correos electrónicos, las que son incluidas en medios electrónicos, las obtenidas de videoconferencias, son palabras, imágenes y sonidos que son recogidos en medios digitales y otros indican que son similares; sin embargo de todas las respuestas se observa que no hacen una diferenciación clara y no es muy limitada su definición y tienden a su confusión. Se comprueba que el mayor porcentaje de encuestados no conoce lo que es la prueba electrónica y digital certificada.

- **Cuestionamiento No. 2. (Gráfica No.2)**



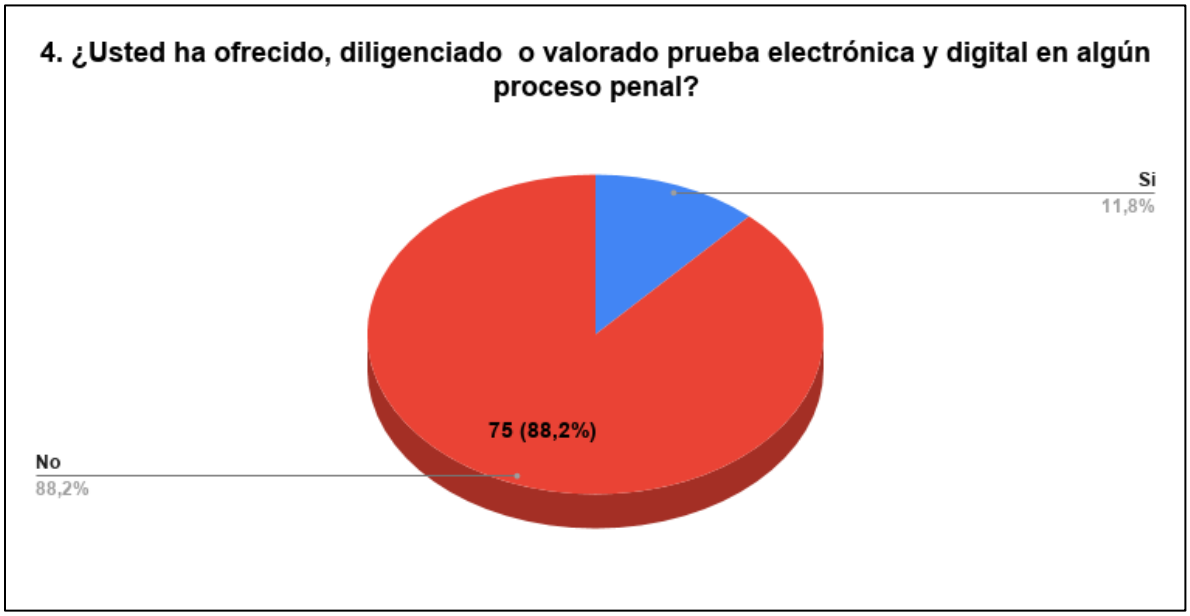
- **Resultado (2):** Del total de personas encuestadas, 20 respondieron “Si”, lo cual representa un 23.5% y 65 personas respondieron “No”, lo cual representa el 76.5%. De la explicación que realizan los encuestados resalta lo siguiente: que es guardar con cuidado y vigilancia los medios electrónicos, supervisión realizada por un Perito Forense Digital, sirve para garantizar la autenticidad de los medios de prueba, que es un documento, son firmas plasmadas en un documento, son pautas de extracción y protección de los medios de prueba, preservación y almacenamiento inalterable de archivos digitales, que se llena en Word y se envía por correo electrónico, es poner en contexto las evidencias digitales, que es un mecanismos administrativo para garantizar la legitimidad de la prueba. De las respuestas analizadas se observa que se tiene un conocimiento básico sobre cadena de custodia digital sin embargo se confunde con los presupuestos y requisitos de una cadena de custodia física. Se afirma que el mayor porcentaje de encuestados no conoce en qué consiste la cadena de custodia digital.

- **Cuestionamiento No. 3. (Gráfica No.3)**



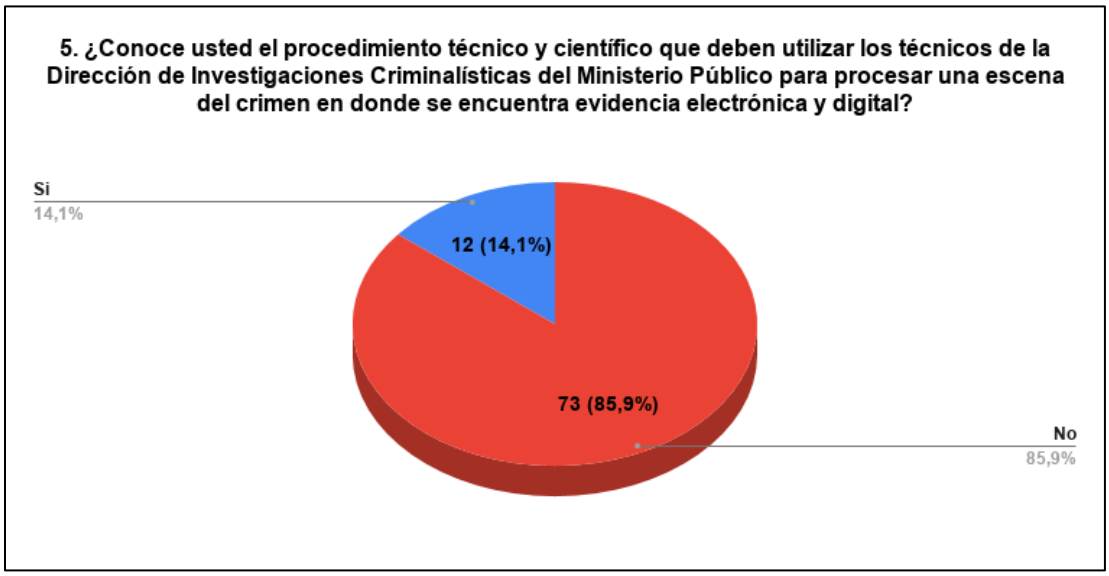
- **Resultado (3):** Del total de personas encuestadas, 14 respondieron “Si”, lo cual representa un 16.5% y 71 personas respondieron “No”, lo cual representa el 83.5%. Se comprueba que el mayor porcentaje de encuestados no conoce en qué consiste la certificación digital de prueba electrónica y digital mediante un algoritmo hash.

- **Cuestionamiento No. 4. (Gráfica No.4)**



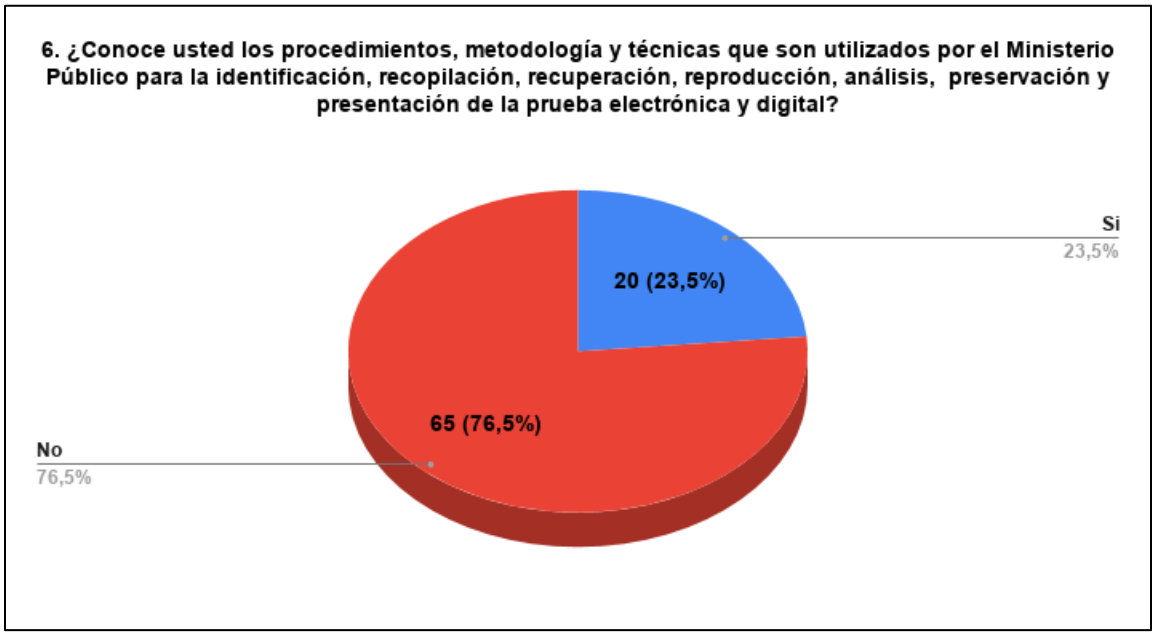
- **Resultado (4):** Del total de personas encuestadas, 10 respondieron “Si”, lo cual representa un 11.8% y 75 personas respondieron “No”, lo cual representa el 88.2%. Se comprueba que el mayor porcentaje de encuestados no ha ofrecido, diligenciado o valorado prueba electrónica y digital en algún proceso penal.

- **Cuestionamiento No. 5. (Gráfica No.5)**



- **Resultado (5):** Del total de personas encuestadas, 12 respondieron “Si”, lo cual representa un 14.1% y 73 personas respondieron “No”, lo cual representa el 85.9%. Dentro de las ampliaciones de las respuestas se describen algunos aspectos, siendo los siguientes: que el procedimiento de marras se en cuenta en el Manual de normas y procedimientos para el procesamiento de escena del crimen del Ministerio Público, que no se cuenta con un procedimiento especifico, que hay un personal idóneo, que se embala y se envía al departamento técnico para extraer la información, se usa un sistema UFED y se lleva a la fiscalía para extraer la información. De las respuestas analizadas se observa que no se hace mención de algún protocolo determinado ni un procedimiento concreto, en virtud que el manual al que hace alusión en las respuestas, de conformidad a la investigación, se estableció que no existe un procedimiento estandarizado o que se guie mediante una instrucción a lo interno del Ministerio Público y el trabajo es empírico. Se comprueba que el mayor porcentaje de encuestados no conoce el procedimiento técnico y científico que deben utilizar los técnicos de la Dirección de Investigaciones Criminalísticas del Ministerio Público para procesar una escena del crimen endone se encuentra evidencia electrónica y digital.

- **Cuestionamiento No. 6. (Gráfica No.6)**

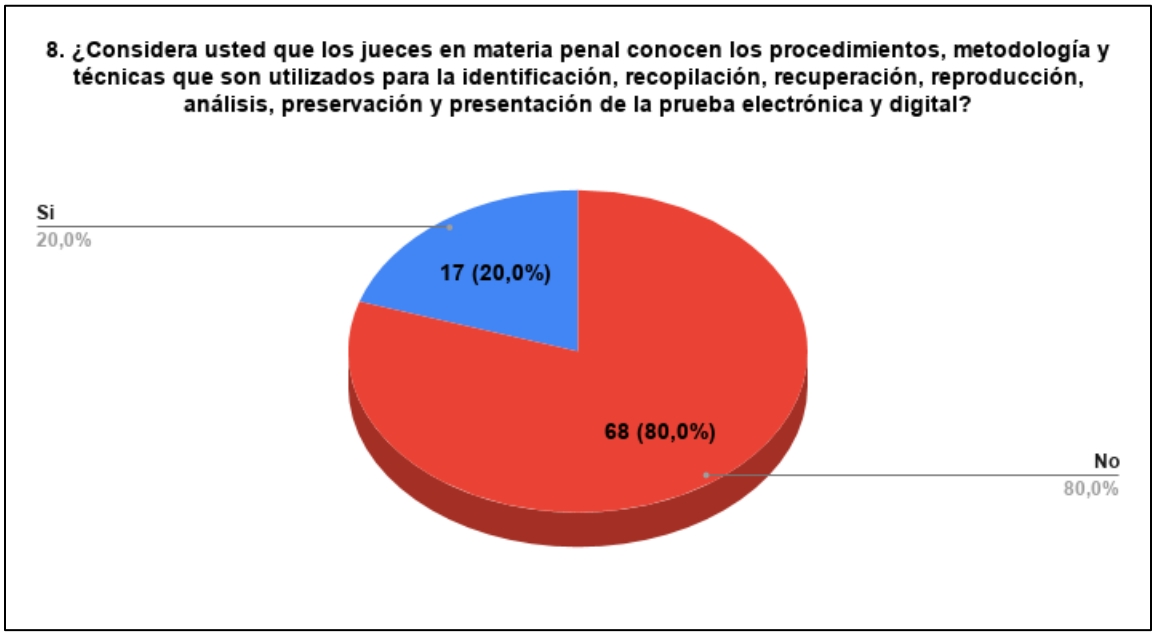


- **Resultado (6):** Del total de personas encuestadas, 20 respondieron “Si”, lo cual representa un 23.5% y 65 personas respondieron “No”, lo cual representa el 76.5%. Se comprueba que el mayor porcentaje de encuestados no conoce los procedimientos, metodología y técnicas que son utilizados por el Ministerio Público para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital.

- **Cuestionamiento No. 7. (Gráfica No.7)**

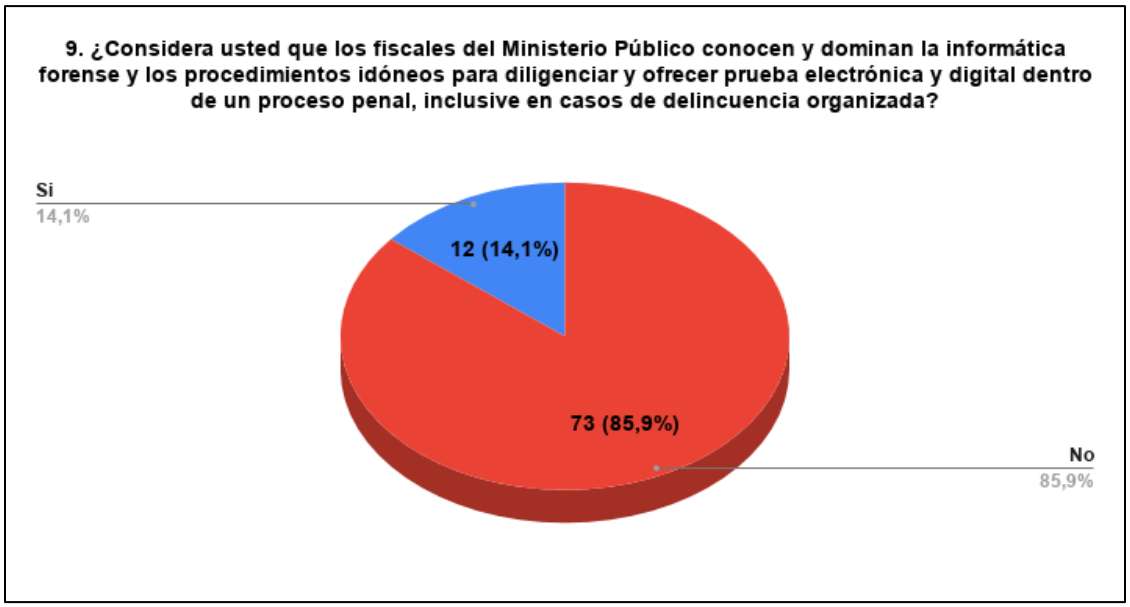
- **Resultado (7):** Del total de personas encuestadas, 1 respondió “Si”, lo cual representa un 1.2% y 84 personas respondieron “No”, lo cual representa el 98.8%. Se comprueba que el mayor porcentaje de encuestados considera que los abogados litigantes no conocen los procedimientos, metodología y técnicas que son utilizados en el proceso penal para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital.

- **Cuestionamiento No. 8. (Gráfica No.8)**



- **Resultado (8):** Del total de personas encuestadas, 17 respondieron “Si”, lo cual representa un 20% y 68 personas respondieron “No”, lo cual representa el 80%. Se comprueba que el mayor porcentaje de encuestados considera que los jueces en materia penal no conocen los procedimientos, metodología y técnicas que son utilizados para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital.

- **Cuestionamiento No. 9. (Gráfica No.9)**



- **Resultado (9):** Del total de personas encuestadas, 12 respondieron “Si”, lo cual representa un 14.1% y 73 personas respondieron “No”, lo cual representa el 85.9%. En la ampliación de respuestas se destaca que los encuestados indican que: algunos fiscales conocen la informático pero que son especializados, por el cargo que desempeña deberían saber, que los fiscales manipulan los equipos electrónicos al encontrarlos en la escena del crimen, que el ochenta por ciento de fiscales no tiene el conocimiento adecuado para trabajar delitos informáticos, que por falta de conocimiento causan que el caso se pierda y se contamine la prueba, no cumplen con el protocolo de evidencia, falta capacitación, falta de recursos en el Ministerio Público. Lo que se evidencia con estas respuestas es que a criterio de los encuestados los fiscales en su gran mayoría no conocen el tema objeto de cuestionamiento. Se comprueba, entonces, que el mayor porcentaje de encuestados considera que los fiscales del Ministerio Público no conocen y dominan la informática forense y los procedimientos idóneos para diligenciar y ofrecer prueba electrónica y digital dentro de un proceso penal, inclusive en casos de delincuencia organizada.

- **Cuestionamiento No. 10. (Gráfica No.10)**

- **Resultado (10):** Del total de personas encuestadas, 3 respondieron “Si”, lo cual representa un 3.5% y 82 personas respondieron “No”, lo cual representa el 96.5%. En la ampliación de respuestas se destaca que los encuestados indican que: es por falta de conocimiento, hay muy pocos, no revisan y no comprenden el procedimiento de extracción de información, poca capacitación, por la poca utilización de los métodos especiales de investigación, es una técnica relativamente nueva, no hay conocimiento de la práctica de estos temas, que debe ser socializado a profundidad porque no todos los abogados conocen de esto. Se comprueba que el mayor porcentaje de encuestados considera que los abogados litigantes no conocen y dominan la informática forense y los procedimientos idóneos para diligenciar y ofrecer prueba electrónica y digital dentro de un proceso penal, inclusive en casos de delincuencia organizada.

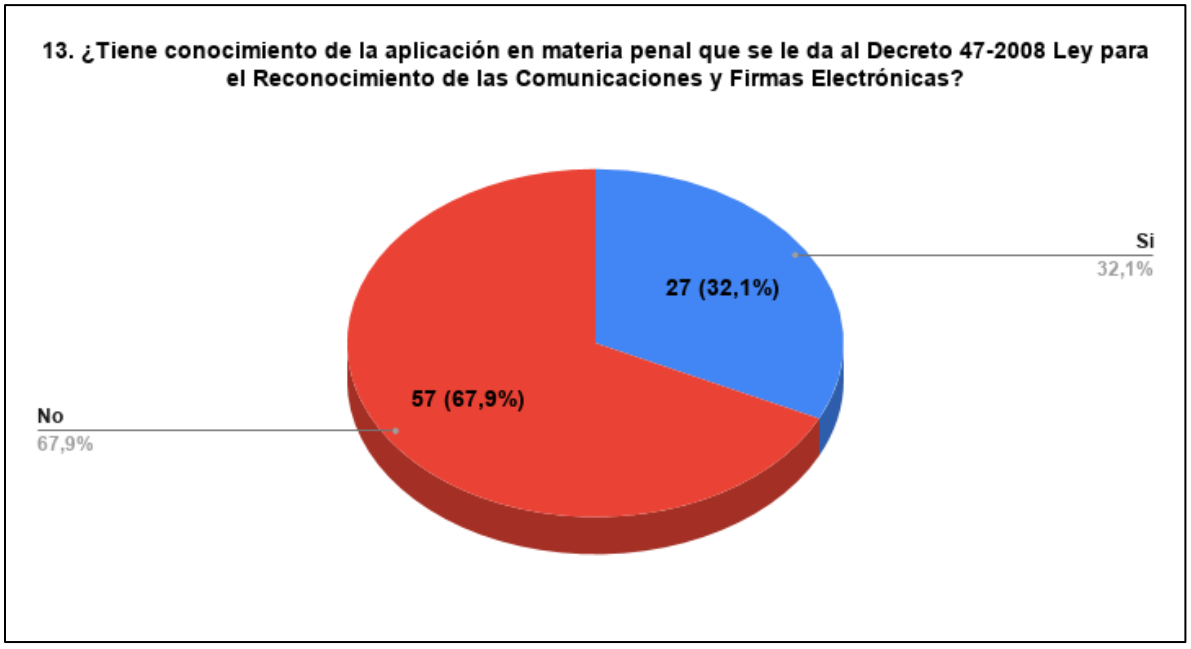
- **Cuestionamiento No. 11. (Gráfica No.11)**

- **Resultado (11):** Del total de personas encuestadas, 10 respondieron “Si”, lo cual representa un 11.8% y 75 personas respondieron “No”, lo cual representa el 88.2%. En la ampliación de respuestas se destaca que los encuestados indican que: es por falta de conocimiento, que los jueces por estar designados en cada judicatura entonces deberían tener el conocimiento, que no es expertiz, la capacitación en ese campo es limitado, que los jueces comunes no conocen salvo que sean de mayor riesgo, la mayoría no domina el tema, no saben utilizar la tecnología, falta de legislación, se limitan al sustento de evidencias puestas a la vista, falta de manuales nacionales. Se comprueba que el mayor porcentaje de encuestados considera que los jueces no conocen y dominan la informática forense y los procedimientos idóneos para valorar prueba electrónica y digital dentro de un proceso penal, inclusive en casos de delincuencia organizada.

- **Cuestionamiento No. 12. (Gráfica No.12)**

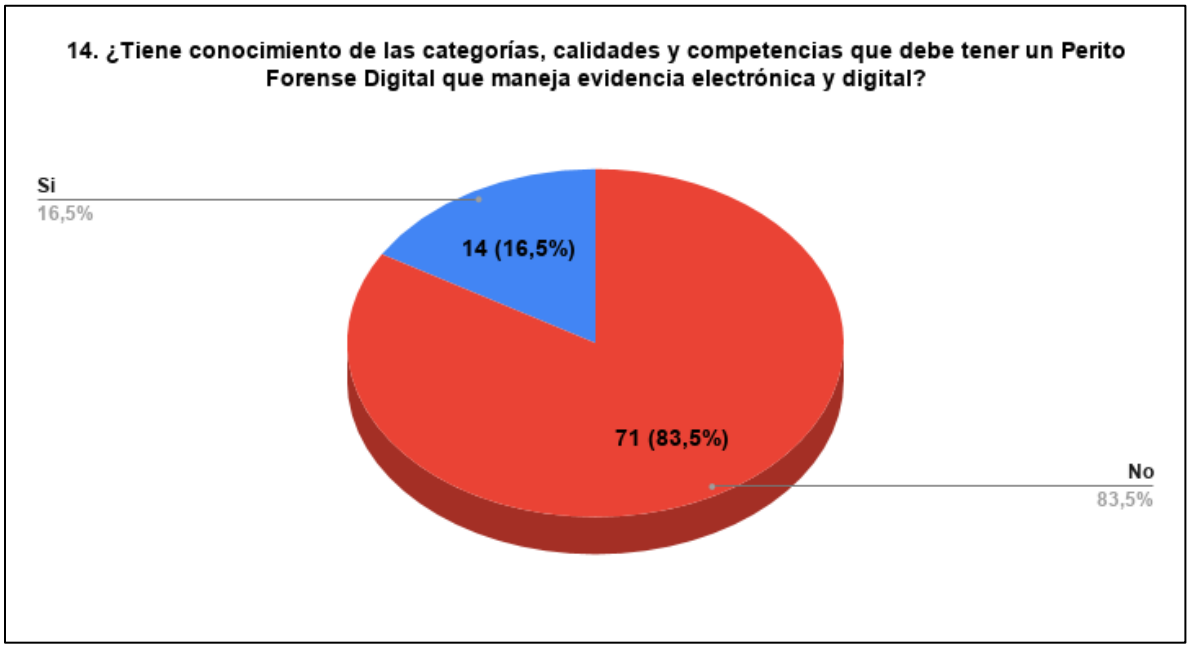
- **Resultado (12):** Del total de personas encuestadas, 5 respondieron “Si”, lo cual representa un 5.9% y 80 personas respondieron “No”, lo cual representa el 94.1%. Se comprueba que el mayor porcentaje de encuestados considera que no conocen el uso que se le da en el proceso penal a las normativas ISO/IEC 27037:2012, ISO/IEC 27042.

- **Cuestionamiento No. 13. (Gráfica No.13)**



- **Resultado (13):** Del total de personas encuestadas, 27 respondieron “Si”, lo cual representa un 32.1% y 57 personas respondieron “No”, lo cual representa el 67.9%. Se comprueba que el mayor porcentaje de encuestados considera que no tienen conocimiento de la aplicación en materia penal que se le da al Decreto 47-2008 Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

- **Cuestionamiento No. 14. (Gráfica No.14)**

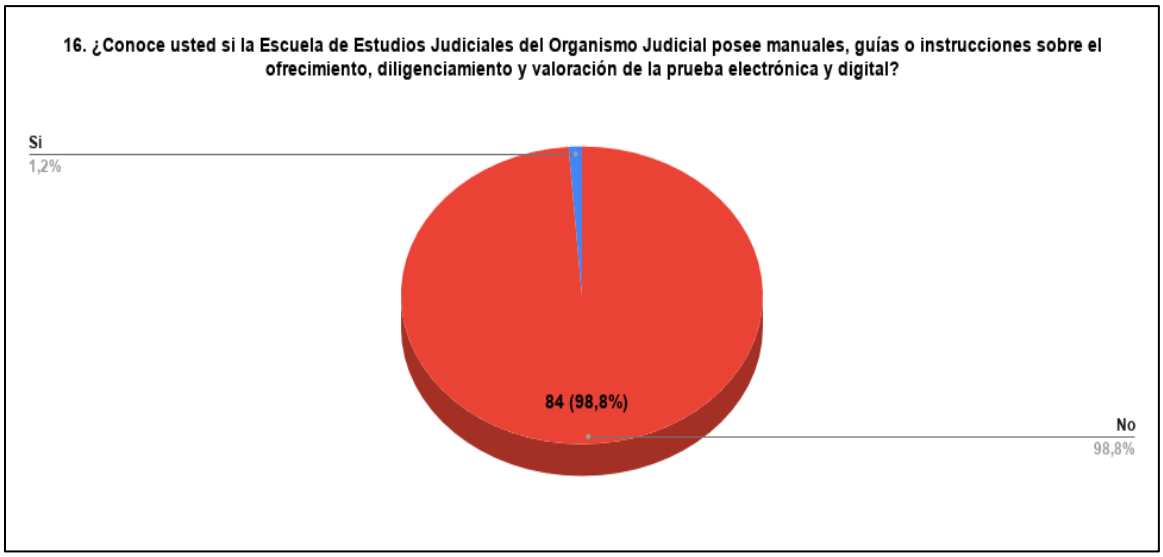


- **Resutado (14):** Del total de personas encuestadas, 14 respondieron “Si”, lo cual representa un 16.5% y 71 personas respondieron “No”, lo cual representa el 83.5%. Se comprueba que el mayor porcentaje de encuestados considera que no tienen conocimiento de las categorías, calidades y competencias que debe tener un Perito Forense Digital que maneja evidencia electrónica y digital.

- **Cuestionamiento No. 15. (Gráfica No.15)**

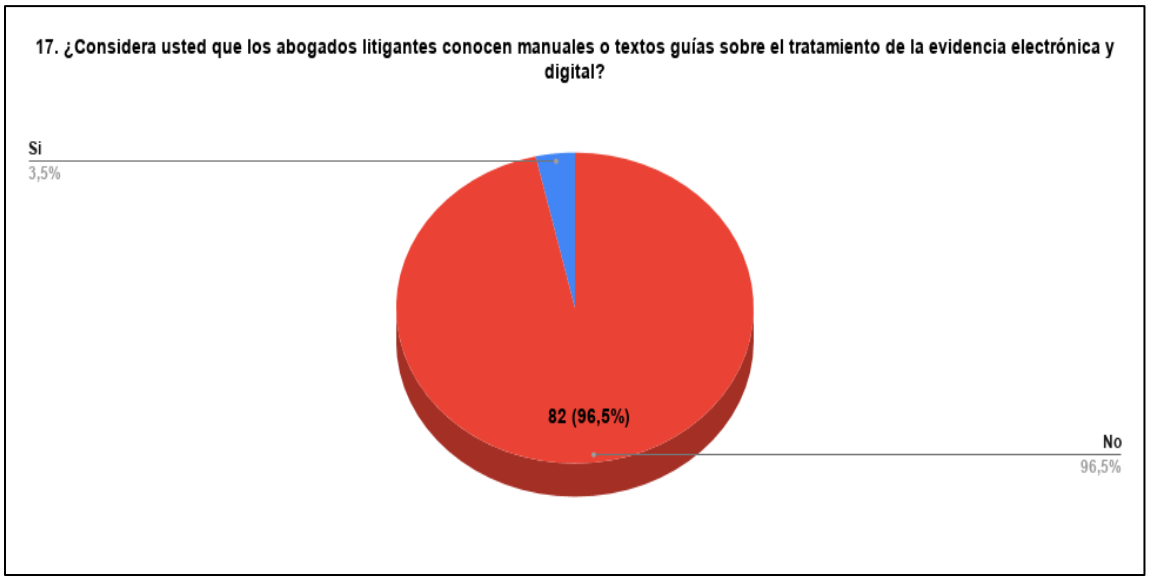
- **Resultado (15):** Del total de personas encuestadas, 6 respondieron “Si”, lo cual representa un 7.1% y 79 personas respondieron “No”, lo cual representa el 92.9%. En la ampliación de respuestas se destaca que los encuestados indican que posiblemente se encuentran en el manual de normas y procedimientos para el procesamiento de la escena del crimen, en la Ley del Ministerio Público (sic) y en algunos acuerdos internos, sin embargo, es menester indicar que de conformidad la investigación realizada se pudo determinar que no existen este tipo de manuales o instrucciones a lo interno del Ministerio Público. Se comprueba que el mayor porcentaje de encuestados considera que no conoce si la Unidad de Capacitación del Ministerio Público posee manuales o instrucciones sobre el tratamiento de la evidencia electrónica y digital.

- **Cuestionamiento No. 16. (Gráfica No.16)**



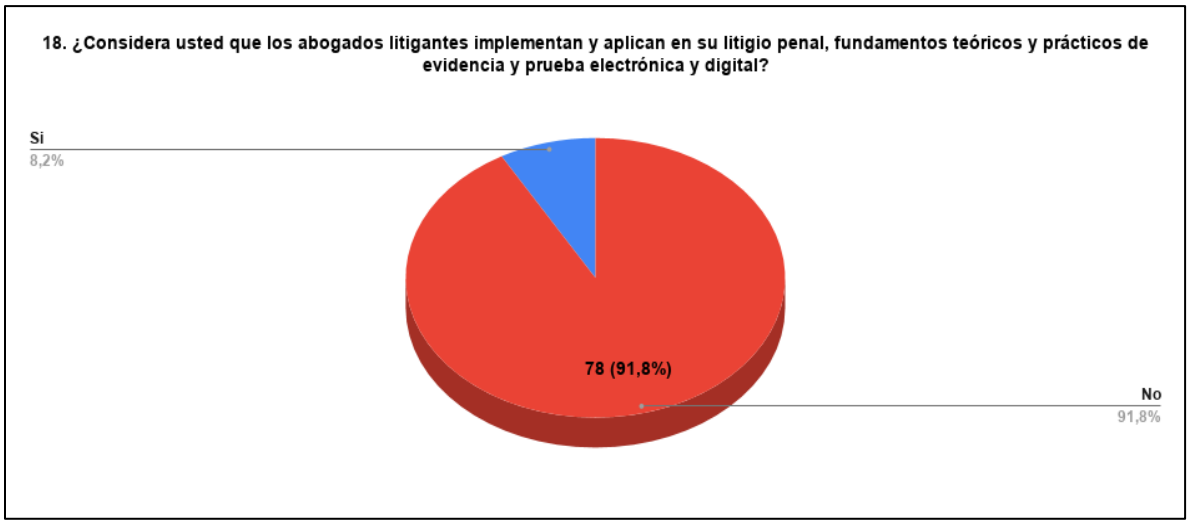
- **Resultado (16):** Del total de personas encuestadas, 1 respondió “Si”, lo cual representa un 1.2% y 84 personas respondieron “No”, lo cual representa el 98.8%. No hubo ampliación de respuestas por parte de los encuestados. Se comprueba que el mayor porcentaje de encuestados no conoce si la Escuela de Estudios Judiciales del Organismo Judicial posee manuales o instrucciones sobre el tratamiento de la evidencia electrónica y digital.

- **Cuestionamiento No. 17. (Gráfica No.17)**



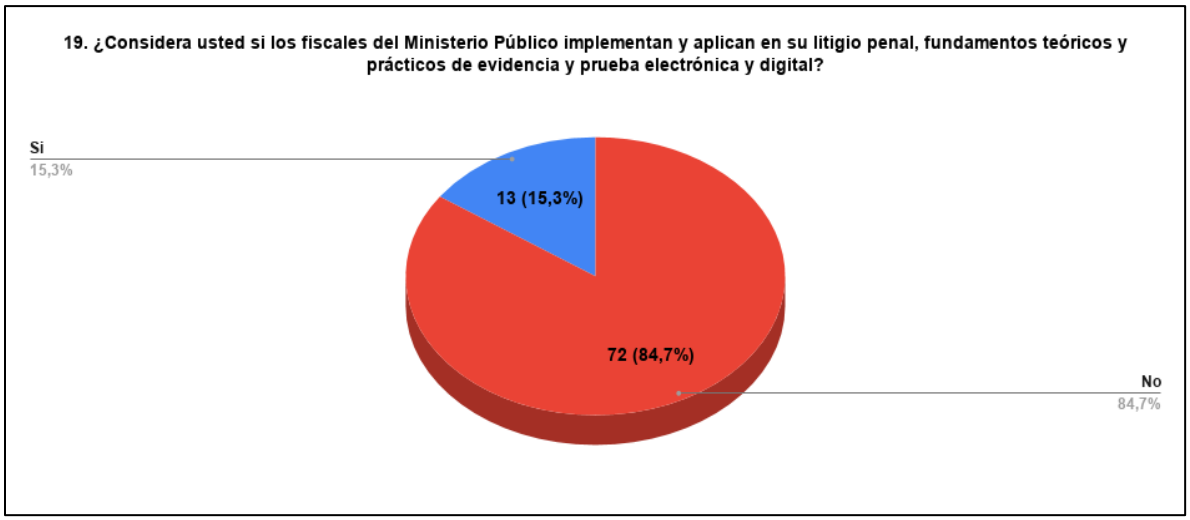
- **Resultado (17):** Del total de personas encuestadas, 3 respondieron “Si”, lo cual representa un 3.5% y 82 personas respondieron “No”, lo cual representa el 96.5%. En la ampliación de respuestas se destaca que algunos de los encuestados indican que algunos se publican, pero son muy generales y que dada la capacitación y exigencia del caso que le pone en su conocimiento el abogado debería tener ese tipo de material para desempeñar su trabajo de mejor forma. Se comprueba que el mayor porcentaje de encuestados considera que los abogados litigantes no conocen manuales o textos guías sobre el tratamiento de la evidencia electrónica y digital.

- **Cuestionamiento No. 18. (Gráfica No.18)**



- **Resultado (18):** Del total de personas encuestadas, 7 respondieron “Si”, lo cual representa un 8.2% y 78 personas respondieron “No”, lo cual representa el 91.8%. Se comprueba que el mayor porcentaje de encuestados considera que los abogados litigantes no implementan y aplican en su litigio penal, fundamentos teóricos y prácticos de evidencia y prueba electrónica y digital.

- **Cuestionamiento No. 19. (Gráfica No.19)**

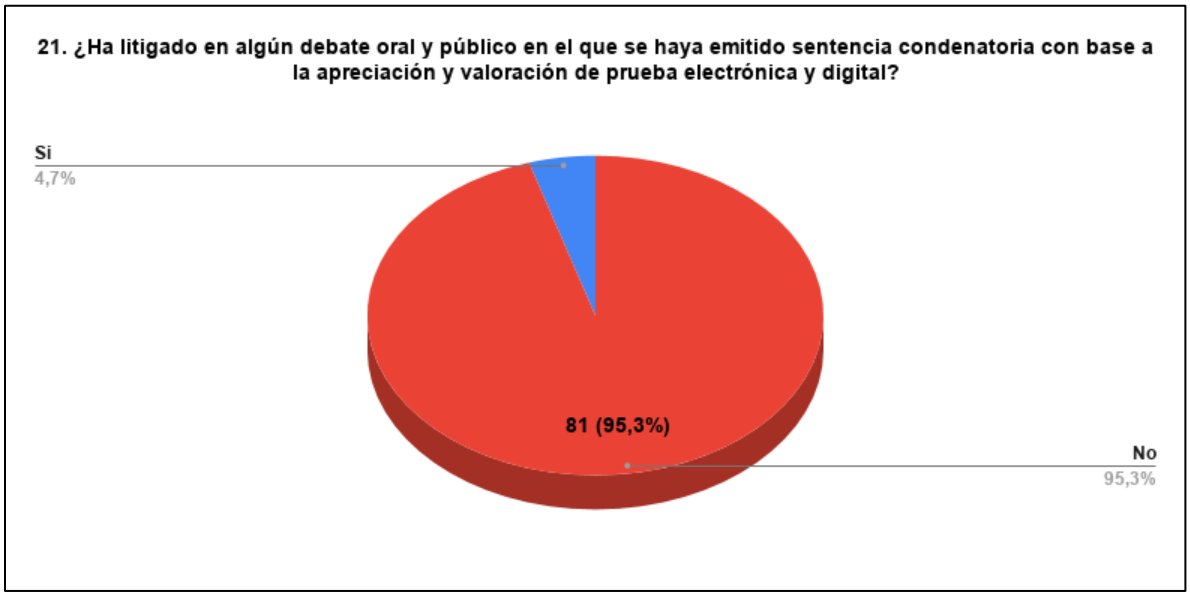


- **Resultado (19):** Del total de personas encuestadas, 13 respondieron “Si”, lo cual representa un 15.3% y 72 personas respondieron “No”, lo cual representa el 84.7%. Se comprueba que el mayor porcentaje de encuestados considera que los fiscales del Ministerio Público no implementan y aplican en su litigio penal, fundamentos teóricos y prácticos de evidencia y prueba electrónica y digital.

- **Cuestionamiento No. 20. (Gráfica No.20)**

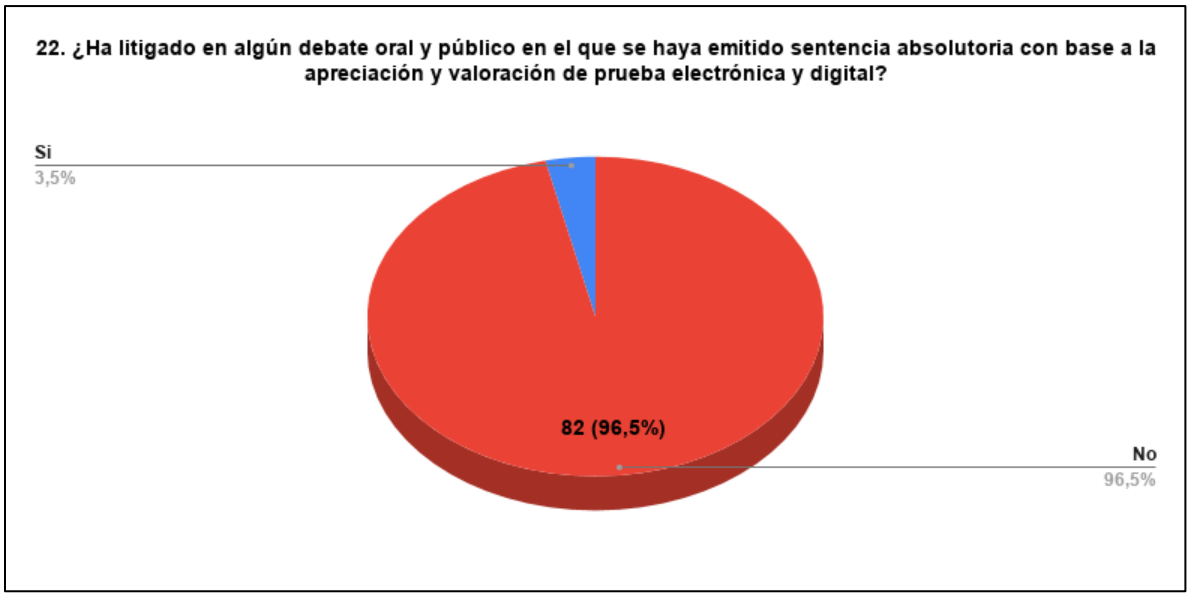
- **Resultado (20):** Del total de personas encuestadas, 5 respondieron “Si”, lo cual representa un 5.9% y 80 personas respondieron “No”, lo cual representa el 94.1%. En la ampliación de respuestas se destaca que algunos de los encuestados indican que los criterios son la efectividad de la cadena de custodia, pertinencia necesaria y legalidad y que de forma general se valora porque siempre y cuando no sea redargüido de nulidad. Se comprueba que el mayor porcentaje de encuestados no conocen los criterios que tienen los jueces en materia penal para apreciar y valorar la prueba electrónica y digital.

- **Cuestionamiento No. 21. (Gráfica No.21)**



- **Resultado (21):** Del total de personas encuestadas, 4 respondieron “Si”, lo cual representa un 4.7% y 81 personas respondieron “No”, lo cual representa el 95.3%. Se comprueba que el mayor porcentaje de encuestados no ha litigado en algún debate oral y público en el que se haya emitido sentencia condenatoria con base a la apreciación y valoración de prueba electrónica y digital.

- **Cuestionamiento No. 22. (Gráfica No.22)**



- **Resultado (22):** Del total de personas encuestadas, 3 respondieron “Si”, lo cual representa un 3.5% y 82 personas respondieron “No”, lo cual representa el 96.5%. Se comprueba que el mayor porcentaje de encuestados no ha litigado en algún debate oral y público en el que se haya emitido sentencia absolutoria con base a la apreciación y valoración de prueba electrónica y digital.

- **Cuestionamiento No. 23. (Gráfica No.23)**

- **Resultado (23):** Del total de personas encuestadas, 1 respondió “Si”, lo cual representa un 1.2% y 84 personas respondieron “No”, lo cual representa el 98.8%. No hubo ampliación de respuestas por parte de los encuestados. Se comprueba que el mayor porcentaje de encuestados no conoce alguna resolución judicial de un tribunal de alzada en el que se haya emitido un razonamiento y fundamentación técnica y legal sobre prueba electrónica y digital en caso de delincuencia común.

- **Cuestionamiento No. 24. (Gráfica No. 24)**

- **Resultado (24):** Del total de personas encuestadas, 1 respondió “Si”, lo cual representa un 1.2% y 84 personas respondieron “No”, lo cual representa el 98.8%. No hubo ampliación de respuestas por parte de los encuestados. Se comprueba que el mayor porcentaje de encuestados no conoce alguna resolución judicial de un tribunal de alzada en el que se haya emitido un razonamiento y fundamentación técnica y legal sobre prueba electrónica y digital en casos de delincuencia organizada.

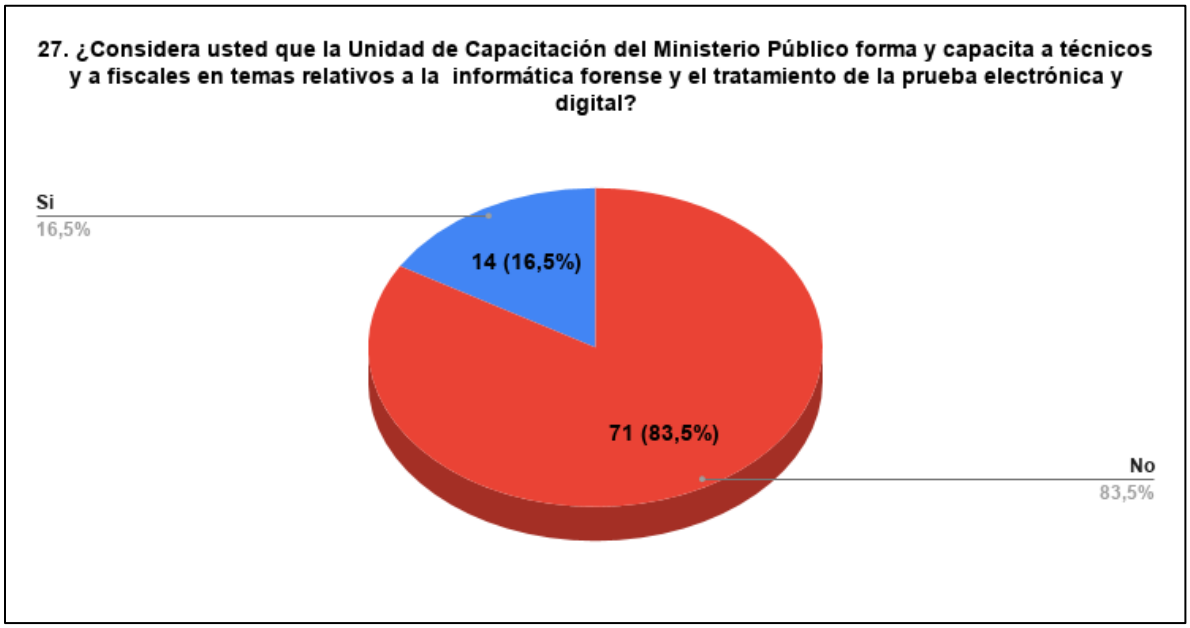
- **Cuestionamiento No. 25. (Gráfica No. 25)**

- **Resultado (25):** Del total de personas encuestadas, 5 respondieron “Si”, lo cual representa un 5.9% y 80 personas respondieron “No”, lo cual representa el 94.1%. En la ampliación de respuestas se destaca que algunos de los encuestados refieren el caso denominado “La Línea” y en la ciudad de Guatemala con la juez Yazmin solo dio intervención en un caso para referirse a toda la prueba digital. pero en forma general. Se comprueba que el mayor porcentaje de encuestados l.

- **Cuestionamiento No. 26. (Gráfica No. 26)**

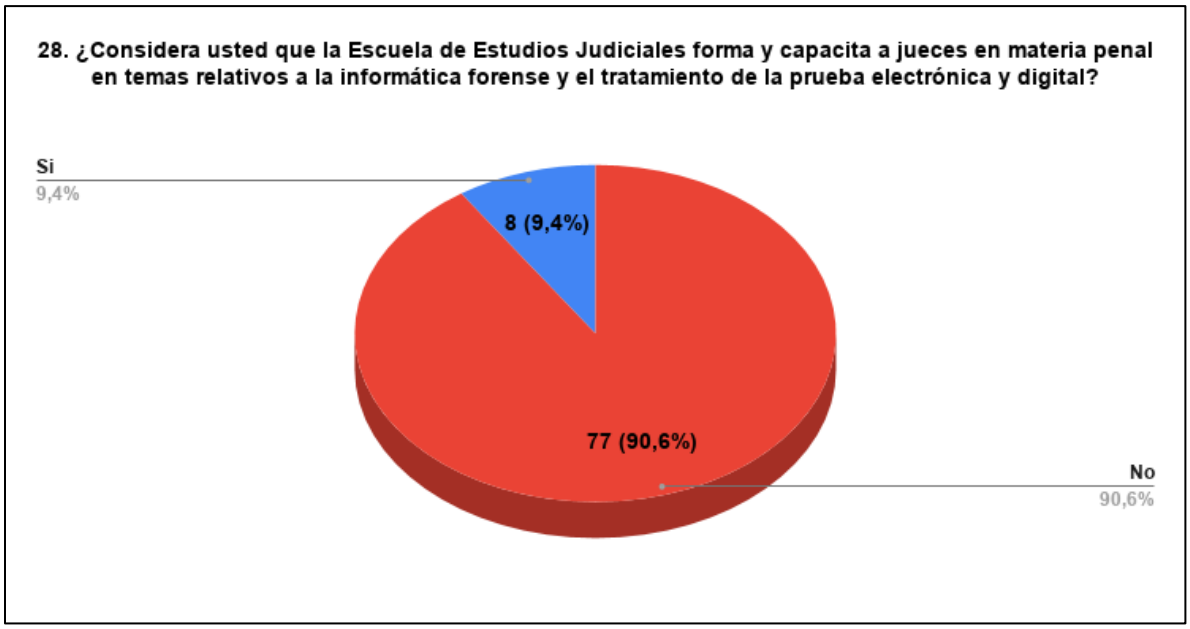
- **Resultado (26):** Del total de personas encuestadas, 6 respondieron “Si”, lo cual representa un 7.1% y 79 personas respondieron “No”, lo cual representa el 92.9%. Se comprueba que el mayor porcentaje de encuestados no tiene conocimiento de los protocolos que existen para darle validez a la prueba electrónica y digital.

- **Cuestionamiento No. 27. (Gráfica No. 27)**



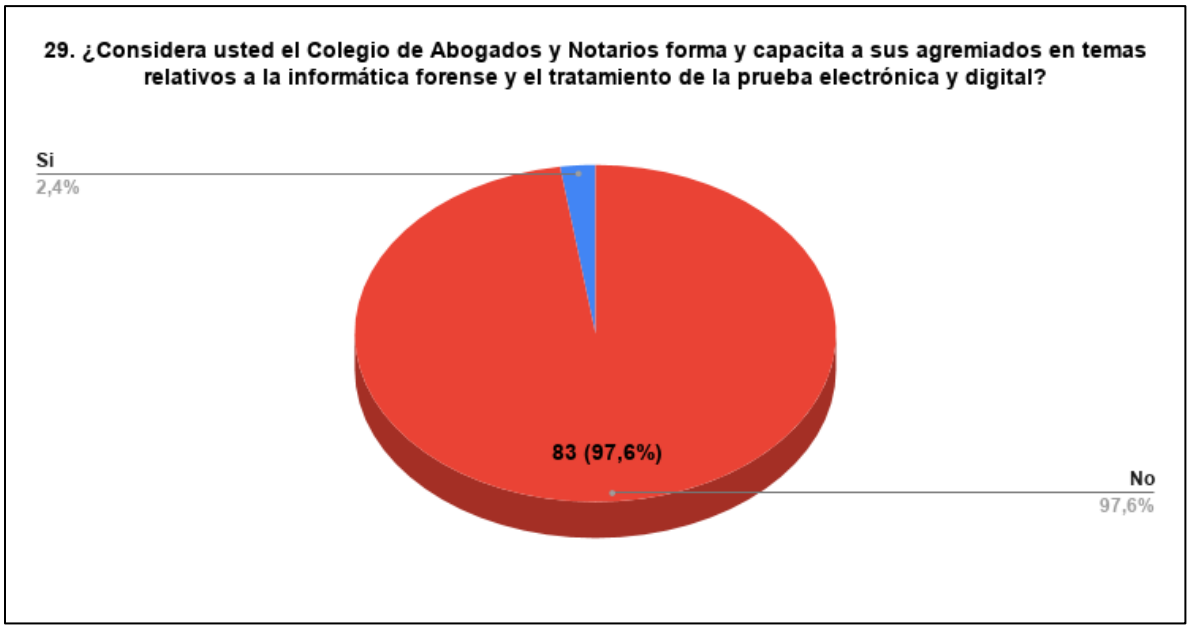
- **Resultado (27):** Del total de personas encuestadas, 14 respondieron “Si”, lo cual representa un 16.5% y 71 personas respondieron “No”, lo cual representa el 83.5%. Se comprueba que el mayor porcentaje de encuestados considera que la Unidad de Capacitación del Ministerio Público no forma ni capacita a técnicos y a fiscales en temas relativos a la informática forense y el tratamiento de la prueba electrónica y digital.

- **Cuestionamiento No. 28. (Gráfica No. 28)**



- **Resultado (28):** Del total de personas encuestadas, 8 respondieron “Si”, lo cual representa un 9.4% y 77 personas respondieron “No”, lo cual representa el 90.6%. Se comprueba que el mayor porcentaje de encuestados considera que la Escuela de Estudios Judiciales no forma ni capacita a jueces en materia penal en temas relativos a la informática forense y el tratamiento de la prueba electrónica y digital.

- **Cuestionamiento No. 29. (Gráfica No. 29)**

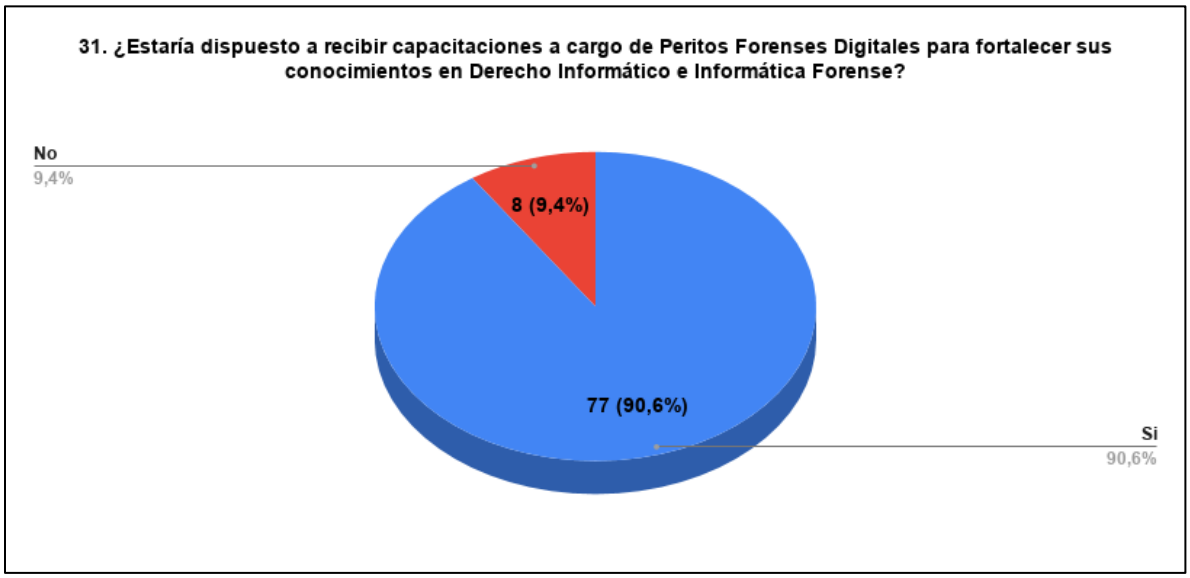


- **Resultado (29):** Del total de personas encuestadas, 2 respondieron “Si”, lo cual representa un 2.4% y 83 personas respondieron “No”, lo cual representa el 97.6%. Se comprueba que el mayor porcentaje de encuestados considera que el Colegio de Abogados y Notarios no forma ni capacita a sus agremiados en temas relativos a la informática forense y el tratamiento de la prueba electrónica y digital.

- **Cuestionamiento No. 30. (Gráfica No. 30)**

- **Resultado (30):** Del total de personas encuestadas, 5 respondieron “Si”, lo cual representa un 5.9% y 80 personas respondieron “No”, lo cual representa el 94.1%. En la ampliación de respuestas varios encuestados indicaron que dentro de estas entidades privadas se encuentra Redlif, Observatorio guatemalteco de delitos informáticos, grupos en internet, la Superintendencia de Administración Tributaria y el Ministerio de Economía, aunque estos dos últimos son entes gubernamentales; además refieren que no hay capacitación en estos temas para los litigantes ni mucho menos el Colegio de Abogados hace algo al respecto. Se comprueba que el mayor porcentaje de encuestados considera que no hay conoce a entidades privadas que capaciten sobre temas relativos la informática forense y el tratamiento de la prueba electrónica y digital.

- **Cuestionamiento No. 31. (Gráfica No. 31)**



- **Resultado (31):** Del total de personas encuestadas, 77 respondieron “Si”, lo cual representa un 90.6% y 8 personas respondieron “No”, lo cual representa el 9.4%. Se comprueba que el mayor porcentaje de encuestados está dispuesto a recibir capacitaciones a cargo de Peritos Forenses Digitales para fortalecer sus conocimientos en Derecho Informático e Informática Forense.

10.4. Entrevista

a) Entrevista realizada al <u>MSc. Milton Alberto Estrada Morales,</u> quien es Juez del Tribunal de Sentencia Penal, Narcoactividad y Delitos contra el Ambiente de Quetzaltenango, el 13 de febrero de 2021.

I. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

- ✓ *El derecho es evolutivo y cambiante y de igual forma la delincuencia también ha evolucionado en la forma en que realiza sus actos ilícitos, es necesario que se profundice en estos temas porque la comunicación hoy en día ha cambiado, la delincuencia se vale de los medios que la tecnología provee; el ente fiscal debe tener al alcance las herramientas para descubrir la verdad y de igual forma el aparato estatal debe conocer estos mecanismos de comunicación para conocer estos tipos de prueba; es importante saber en qué tipo de medio probatorio caben los medios electrónicos*.

II. Según su experiencia ¿qué protocolos y metodología ha visto que son más utilizados en el procesamiento de una escena de crimen digital (Cadena de custodia digital, embalaje)?

- ✓ *He visto dos situaciones, en donde no se manejan correctamente los protocolos para extraer la información y eso puede repercutir en el proceso más adelante porque la contraparte puede objetar la forma en que se obtiene la información. Otra situación es que los investigadores toman el debido cuidado y luego se recurre ante el Juez para que provea la autorización judicial para extraer la información de los*

dispositivos electrónicos. No he visto que el Ministerio Público utilice bolsas o cajas de Faraday, solo bolsitas o cajas de cartón o similares.

III. Según su experiencia, ¿ha tenido la oportunidad que el ente fiscal presente la certificación digital de la evidencia electrónica y digital mediante un MD5 o similar?

- ✓ *No he visto que presenten ese tipo de certificaciones. Ninguna fiscalía utiliza ese tipo de certificaciones que deberían utilizarse para resguardar la pulcritud de esa información*.

IV. ¿Según su experiencia, ¿en alguna audiencia los sujetos procesales han ofrecido o mencionado un sistema UFED (Universal Forensic Extraction) para acreditar algún extremo?

- ✓ *En mi experiencia no he visto ese tipo de sistemas.*

V. ¿Según su experiencia, ¿qué protocolos y técnicas forenses se aplican en el proceso penal guatemalteco para el tratamiento de la evidencia electrónica y digital?

- ✓ *No conozco alguno en específico.*

VI. Según su experiencia, ¿ha tenido la oportunidad de que en alguna audiencia hayan presentado como Consultor Técnico a un Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery?

- ✓ *En donde he visto lo de los analistas técnicos es en una unidad en donde recolectan la información, pero solo es el único perfil que podría encuadrar en esos expertos, de otra institución no he visto que se ofrezcan a ese tipo de consultores técnicos.*

VII. Según su experiencia, ¿el Ministerio Público cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales?

- ✓ *Considero que no hay, falta bastante conocer bien estos protocolos para manejar la evidencia digital, la información hoy en día es uno de los bienes más preciados y esta debe tratarse de la mejor forma porque es esencial; hoy en día no se maneja adecuadamente la evidencia digital*.

VIII. Según su criterio, ¿ha visto la aplicación de los protocolos ISO/IEC 27037 e ISO/IEC27042 en el proceso penal guatemalteco?

- ✓ *Recuerdo que los analistas en algún momento han presentado algún protocolo de esa naturaleza para presentar los informes. Existen diferentes instrumentos internacionales que marcan la pauta de cómo debe tratarse la evidencia electrónica y digital y por ejemplo cuando se extra la información sin cuidar un protocolo determinado violenta a lo regulado en estos instrumentos, todo esto para garantizar la fidelidad de la cadena de custodia, se debe cuidar la seguridad jurídica evitando que las personas que no tiene las calidades técnicas manipulen la información que después será tratada en el proceso*.

IX. ¿Ha desestimado o no aceptado alguna prueba por violentar la cadena de custodia digital?

- ✓ *En un caso que conocí en la judicatura la defensa advirtió este extremo, en donde objeto la admisión de determinada información sin tener autorización judicial para inspeccionar el dispositivo*.

X. ¿Considera usted si los jueces, fiscales y abogados litigantes conocen con propiedad las características propias de la prueba electrónica y digital?

- ✓ *A todos nos falta bastante, dentro de programas de capacitación que yo he tenido conocimiento dentro de la Escuela de Estudios judiciales no he visto sobre alguna formación en evidencia digital*.

XI. ¿Considera usted que un pantallazo o screenshot es prueba documental o prueba digital?

- ✓ *Podría ser una prueba documental si por ejemplo fue tomada una foto porque son impresas. Sin embargo, en el tema de certificación digital es limitada, algunos abogados presentan actas notariales para acreditar por ejemplo el cotejo o visita a páginas o para hacer constar determinadas evidencias digitales*.

XII. ¿Le han presentado pruebas referentes memoria RAM, volcados de memoria y espectrogramas de audio?

- ✓ *En ningún momento*.

XIII. Según su experiencia, ¿cuál es el mecanismo que se utiliza en el proceso penal guatemalteco para validar o incorporar como prueba conversaciones de WhatsApp o de cualquier otra red social?

- ✓ *El WhatsApp está fuera de territorio guatemalteco, la única forma es la impresa o pantallazos; la forma correcta sería obtener la información de los servidores con previa autorización judicial*.

XIV. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital que utilice actualmente para litigar o conocer casos penales en Guatemala.

- ✓ *No conozco ningún material al respecto.*

XV. Según su experiencia, ¿considera usted que, dentro del proceso penal guatemalteco de diligencia, ofrece y valora la prueba electrónica y digital en una forma empírica y bajo los mismos principios de la prueba tradicional?

- ✓ *Pienso que se trabaja en forma empírica y mecánica porque se piensa que todos los casos deben manejarse en una misma forma. No se ha aprendido a trabajar en forma individualizada, no se maneja en forma científica.*

b) Entrevista realizada al <u>Dr. Luis Alberto Fernández Ramírez</u>, quien es Juez del Tribunal de Sentencia Penal, Narcoactividad y Delitos contra el Ambiente de Quetzaltenango, el 15 de febrero de 2021.

I. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

- ✓ *Debemos recordar que la ley impone que casos deben conocer en competencia de mayor riesgo y el trámite respectivo, los tipos penales que se regulan en Ley contra la Delincuencia Organizada se conocen esta competencia. Ha sido ordinario, pero no exclusivo que los casos de delincuencia organizada se trasladen a mayor riesgo. En la práctica tengo cierta experiencia en la forma en que se ha conocido este tipo de pruebas, cosa diferente es la teoría.*

II. ¿Cómo se desarrolla la prueba electrónica y digital en el debate y de esa cuenta cuál es la denominación de la prueba electrónica y digital en la actualidad en Guatemala?

- ✓ *No se conoce, trata ni se denomina así tal cual como prueba electrónica y digital. En la práctica solo tenemos peritos, testigos, documentos y objetos, puede existir prueba audiovisual pero no más que un video grabado no es prueba es electrónica, esto es lo más técnico y desarrollado y en la práctica hasta traen a un técnico para poner un video y eso no es prueba electrónica, es una ilusión estamos muy alejados de la realidad. Existe desconocimiento y como en el Código Procesal Penal en su artículo 182 y 185 refiere sobre la*

libertad probatoria ahí fácilmente entra la prueba digital, pero como no tiene una regulación específica, desarrollo o tratamiento no se pasa de lo tradicional y cuando existe algún indicio digital ha sido incorporada como peritaje. Lo usual es que un técnico del Ministerio Público que haga el peritaje sin orden judicial, esto es mi apreciación. La fiscalía aún está muy lejos de tratar estos temas con propiedad.

III. Según su experiencia ¿cuáles son las falencias en los protocolos y metodología en el procesamiento de una escena de crimen digital (Cadena de custodia digital, embalaje)?

- ✓ *Debemos comprender que la prueba digital vive en un entorno virtual, sobre esa base debe ser obtenida y almacenada de una buena forma. La prueba digital puede modificarse con mucha facilidad; la manipulación y destrucción de la prueba digital es más sensible. Se debería tener a las personas idóneas para este tratamiento. Por ejemplo, en un caso determinado la fiscalía en un allanamiento y ahí se recolectan varios indicios con una gran variedad de dispositivos electrónicos y lo que se llevan son los objetos porque se embalan estos dispositivos tal y como se embala una chumpa, un arma, etc. En cuanto a la extracción de la información llama la atención como en varias ocasiones se pretender tomar esa información cuando aun así esté resguardada sin obtener autorización judicial. El artículo 187 del Código Procesal Penal refiere la forma en que se debe inspeccionar lugares y esto debe trasladarse a los dispositivos electrónicos, que en un caso simple se aprehende a una persona y de esa cuenta se toma el teléfono celular y se empieza a revisar y manipular sin ningún tipo de autorización judicial y eso no es factible. La prueba digital en su tratamiento debe ser técnica y legal. En el ofrecimiento de prueba pasa muchas veces que se imprime o se presenta un pantallazo o captura de pantalla. Los técnicos del Ministerio Público donde se duda de su idoneidad. Son pocos los peritajes que se realizan, en Inacif son*

limitados. Al juez se le pide conocer derecho, pero hay otras disciplinas como la informática en donde los peritos y consultores tienen una función importante para explicar diversos extremos, el juez falla muchas veces con lo que se tiene y en este caso solo está acostumbrado a peritos y documentos. Todo mundo usa tecnología, pero para los jueces es nueva la propuesta como prueba en sede penal de herramientas tecnológicas o prueba digital.

IV. ¿Cuál es su opinión sobre la utilización utilizan bolsas o cajas de Faraday y la certificación digital de la evidencia digital y electrónica mediante MD5 dentro de proceso penal?

- ✓ *Estamos muy lejos de eso, no existen los insumos, el embalaje de la evidencia electrónica y digital se da en sobre manilas, las certificaciones no son digitales, no se redarguye de nulidad los las copias de screenshot, usualmente los técnicos del Ministerio Publico toman fotografías del contenido del teléfono y ahí se forma un álbum fotográfico que usa la fiscalía y se le pretende dar un valor cuando no es así. Probablemente se da esta práctica por la falta de regulación legal en nuestro país, estamos lejos que se utilicen estos insumos y certificación digital*.

V. Según su experiencia, ¿en casos de delincuencia organizada, ha sido presentado en alguna ocasión como consultor técnico un Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery?

- ✓ *En casos de delincuencia organizada es muy poco, la prueba digital es muy poco, la fiscalía se ha ceñido solo a informes de otro tipo. Considero que son pocos profesionales que se dedican a esta labor y supongo que ha de ser muy oneroso para el interesado en costear esos servicios. Es muy difícil ver esto en la realidad, sería interesante ver como se cuestiona a un técnico de Cradic por parte de uno de*

estos especialistas y conocer los extremos sobre los cuales se le examina.

VI. Según su experiencia, ¿el Ministerio Público cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales?

- ✓ *Se ha discutido falsamente que por tener un título universitario se tiene la experiencia de efectuar una pericia y eso no es así, es punto a discusión porque lo importante es un real de conocimiento sobre el punto de pericia; muchas veces quienes no están graduados pues se complementan con cursos, capacitaciones y que de alguna forma adquieren el conocimiento.*
  Se discute más el aspecto de experiencia sobre el plano formal que de fondo.

VII. En su experiencia, ¿el Instituto Nacional de Ciencias Forenses ha presentado y utilizado en sus informes los protocolos ISO/IEC 27037 e ISO/IEC27042?

- ✓ *No los había escuchado ni oído. Inacif cuando tiene actuaciones no se basa en protocolos que no sean de la institución. La tarea de Inacif es segunda, por eso es importante la recolección de indicios por la fiscalía, es decir este es el primer momento; el peritaje de Inacif lo realiza sobre la base del indicio que es enviado y que si está viciado el procedimiento desde el inicio desde el momento que la fiscalía realiza su trabajo ahí surge el punto de discusión, dudo que un auxiliar fiscal tenga esa información para el buen tratamiento de la evidencia electrónica y digital.*

VIII. En su experiencia ¿ha sido invocado el Decreto 47-2008 “Ley para el reconocimiento de las comunicaciones y firmas electrónicas” en una audiencia de debate refiriéndose a la prueba electrónica y digital?

- ✓ *No se utiliza ni invoca esta ley, probablemente se conoce como una ley poco penal, cualquier persona con interés podría incluso venir a la judicatura y escuchar los audios de las audiencias y verificar que esta ley no se invoca, nunca he escuchado eso*.

IX. Según su experiencia, ¿cuál es el mecanismo que se utiliza en el proceso penal guatemalteco para validar o incorporar como prueba conversaciones de WhatsApp o de cualquier otra red social?

- ✓ *En algunas fiscalías, como por ejemplo de Extorsiones existe una unidad llamada enlace que es la que localiza información en redes sociales para que luego nosotros como fiscales la analicemos para seguir la ruta de investigación, como por ejemplo los contratos de Facebook, fotografías y otra información, porque son datos públicos*.

X. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital que utilice actualmente para litigar o conocer casos penales en Guatemala o en la Escuela de Estudios Judiciales.

- ✓ *No conozco ningún material. Por ejemplo, en la Escuela de Estudios Judiciales existe un amplio catálogo de cursos sin embargo en tema de prueba electrónica y digital sería muy bueno su difusión y conocimiento, pero de momento no han existido cursos sobre ésta temática.*

XI. Según su experiencia, ¿considera usted que, dentro del proceso penal guatemalteco de diligencia, ofrece y valora la prueba electrónica y digital en una forma empírica y bajo los mismos principios de la prueba tradicional?

- ✓ *Puedo hablar solamente desde el punto de vista de mi judicatura y en forma referencial considero que la prueba electrónica y digital tiende a ser más tradicional es decir ingresar este tipo de prueba en algo que ya existe, es decir lo electrónico lo imprimimos y ya es prueba*

documental, hay algo electrónico y no lo entiendo entonces llamamos a un perito y esto ya es prueba pericial, se maneja en forma análoga.

c) Entrevista realizada al <u>MSc. Félix Magdiel Sontay Chávez</u>, quien es Juez de Primera Instancia, Penal, Narcoactividad y Delitos contra el Ambiente de Quetzaltenango, el 14 de febrero de 2021.

I. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

- ✓ *Es una ciencia un poco joven y que muchas veces se propone como medio de investigación y solo lo conocemos como medios científicos de prueba, como medios de convicción, hay tendencia del Ministerio Público para solicitar una autorización judicial para requerir a una propia unidad del ente fiscal encargada de extraer información de dispositivos electrónicos, esto no puede ser porque de lo contrario se volvería burocrático. Como jueces conocemos la preinvestigación e investigación y es ahí donde podríamos conocer un poco sobre informática forense, desconozco si en el Instituto Nacional de Ciencias Forenses se estudia ésta parte.*

II. Según su experiencia ¿qué protocolos y metodología ha visto que son más utilizados en el procesamiento de una escena de crimen digital (Cadena de custodia digital, embalaje)?

- ✓ *A nosotros nos llegan ya los medios embalados y nosotros solo convalidamos, si por ejemplo el ente fiscal obtiene información de una cámara desconozco el procedimiento que se usa porque nosotros como jueces no tenemos ese control, el ente fiscal a través de un acta de inspección ocular tendría que detallar ese control, nosotros solo lo tomamos como medio de convicción*.

III. Según su experiencia, ¿se utilizan bolsas o cajas de Faraday para embalar la evidencia electrónica y digital?

- ✓ *La evidencia como tal no se pone a la vista del juez, a nosotros solo nos presentan el acta que acredita el embalaje de los dispositivos electrónicos, porque es hasta en el debate en donde se presenta la evidencia. El acta de inspección ocular es lo que nosotros le damos ese crédito junto a una cadena de custodia*.

IV. ¿Según su experiencia, ¿se utiliza la certificación digital de la evidencia electrónica y digital?

- ✓ *A nosotros como jueces no nos interesa como se certifica una evidencia toda vez que lo relativo a los procedimientos correctos se debe conocer hasta en debate.*

V. Según su experiencia, ¿se ha presentado un consultor técnico tales como Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery en el tratamiento de la evidencia electrónica y digital dentro un proceso penal?

- ✓ *No he visto que alguna de los sujetos procesales haya presentado este tipo de consultores técnicos*.

VI. Según su experiencia, ¿el Ministerio Público cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales?

- ✓ *Debe tenerse la experiencia para obtener esa prueba científica, pero aún falta mucho. Desconozco además que tipo de personal cuenta el Ministerio Público, desconocemos si el técnico es idóneo o no porque eso se ve hasta en debate*.

VII. Según su criterio, ¿cuál la importancia de aplicar los protocolos ISO/IEC 27037 e ISO/IEC27042 en el proceso penal guatemalteco?

- ✓ *No conocemos ese tipo de protocolos porque no nos corresponde valorar la prueba, toda vez que en la fase en la que el juez de garantías conoce el proceso penal, no debe efectuarse ningún tipo de valoración.*

VIII. Según su experiencia ¿en el proceso penal es aplicable el Decreto 47-2008 "Ley para el reconocimiento de las comunicaciones y firmas electrónicas – sobre el tratamiento de la evidencia electrónica y digital?

- ✓ *En la etapa de investigación e intermedia el fiscal puede hacer uso de cualquier tipo de normativa, pero en esta fase no se puede valorar la prueba.*

IX. ¿Considera usted que un pantallazo o screenshot es prueba documental o prueba digital?

- ✓ *Considero que es una ilustración de la prueba digital.*

X. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital que utilice actualmente para litigar o conocer casos penales en Guatemala, específicamente en la Escuela de Estudios Judiciales.

- ✓ *No recuerdo, tal vez exista, pero no estoy seguro, nosotros como jueces tenemos mucho trabajo y posiblemente no nos percatamos de ese tipo de material. Además, en el Colegio de Abogados en la Unidad Académica no veo que exista ese tipo de material. Esta ciencia es demasiada amplia y se necesitan expertos.*

d) Entrevista realizada al <u>Licenciado Herbert Roberto Pérez Maldonado</u>, quien es abogado litigante, el 18 de febrero de 2021.

I. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

- ✓ *Actualmente la informática forense y la tecnología ha avanzado mucho e indudablemente en los tribunales de justicia se ve ejemplificado en el uso de las videoconferencias, cuando se ponen como pruebas videos de cámaras de seguridad, actualmente hay mucha información y es material probatorio en un juicio*.

II. Según su experiencia ¿qué protocolos y metodología ha visto que son más utilizados en el procesamiento de una escena de crimen digital (Cadena de custodia digital, embalaje)?

- ✓ *El Ministerio Publico maneja sus propios, protocolos, cuando nosotros como abogados litigantes nos llaman nuestros clientes, lo que hacemos es asesorarlos, pero por lo regular es hasta que se defiende a una persona en su primera declaración y otras cuando se le asiste desde que es detenido en la escena criminal, pero supongo que esos protocolos y metodología ha de estar en el manual de fiscal actual*.

III. Según su experiencia, ¿existe seguridad y certeza jurídica cuando se embala evidencia electrónica y digital aun cuando no se utilizan bolsas o cajas de Faraday. Y ¿cómo se efectúa la certificación digital de la evidencia digital y electrónica mediante MD5 dentro de proceso penal?

- ✓ *No recuerdo haber visto que utilicen algún tipo de embalaje especial que pueda ayudar a proteger los indicios o evidencia de este tipo electrónico y en la práctica que he tenido tampoco he visto que se use ese tipo de certificación, aunque si he escuchado que el MD5 si se usa para garantizar la integridad de la prueba electrónica y digital*.

IV. ¿Según su experiencia, ¿cuál es la importancia del sistema UFED (Universal Forensic Extraction) en una escena del crimen digital y en el análisis forense de información digital?

- ✓ *Tengo conocimiento que es un sistema especial para recolectar información digital y que se emplea para casos de alto impacto o en algunos casos cuando se da un delito en el que se analizan dispositivos electrónicos, pero es muy raro verlos en los procesos, según recuerdo esto lo vi en internet y sé que tiene un precio elevado*.

V. Según su experiencia, ¿cuál es la función de un Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery en el tratamiento de la evidencia electrónica y digital dentro un proceso penal?

- ✓ *No conozco este tipo de especialistas y tampoco he visto o escuchado que el Ministerio Público los utilice o en su caso que algunos colegas los hayan presentado específicamente en un proceso penal.*

VI. Según su experiencia, ¿el Ministerio Público cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales?

- ✓ *El Ministerio Publico tiene especialistas en la "Dicri" y estimo que si están desempeñando funciones en esa unidad han de tener la expertiz necesaria, sin embargo, opino que una de las falencias más grandes que tiene el ente fiscal es ahí en la recolección de evidencias y eso nos sirve a nosotros cuando desempeñamos el rol de abogado defensor, ellos dan esa pauta para que nosotros contra argumentemos y podamos atacar la hipótesis fiscal*.

VII. Según su criterio, ¿cuál la importancia de aplicar los protocolos ISO/IEC 27037 e ISO/IEC27042 en el proceso penal guatemalteco?

- ✓ *No había escuchado sobre ese tipo de protocolos en materia probatoria, aunque si lo vi en algún momento en algún informe de Inacif, pero a ciencia cierta no recuerdo puntualmente que estudia cada uno de esos protocolos*.

VIII. ¿Además de lo contenido en el Decreto 47-2008 "Ley para el reconocimiento de las comunicaciones y firmas electrónicas –articulo 9 al 14- sobre el tratamiento de la evidencia electrónica y digital, ¿que otro fundamento legal considera que puede utilizarse para darle credibilidad y valor probatorio a la prueba electrónica y digital en el proceso penal guatemalteco?

- ✓ *Solo lo relativo a la privacidad de las comunicaciones en el bloque constitucional y sobre la libertad de prueba que regula nuestro Código Procesal Penal*.

IX. Según su experiencia, ¿cómo se ofrece y diligencia la prueba digital de memoria RAM, volcados de memoria y espectrogramas de audio?

- ✓ *Si yo en algún momento ofrecí pruebas sobre audios y videos, aunque e término de volcados y espectrogramas no recuerdo si a eso se refería, pero sí sé que se debe ofrecer en algún disco compacto y luego conocerse en debate*.

X. ¿Considera usted que un pantallazo o screenshot es prueba documental o prueba digital?

- ✓ *Para mí no es ninguna de ellas, pero lamentablemente muchos jueces la aceptan y esperan a que sea discutida hasta en debate, considero que no es técnico y legal pero la mala práctica ha originado que nosotros como litigantes la usemos, yo en varias ocasiones me he opuesto en las audiencias, pero no he tenido una respuesta favorable, muchas veces por desconocimiento de fiscales y jueces.*

XI. Según su experiencia, ¿cuál es el mecanismo que se utiliza en el proceso penal guatemalteco para validar o incorporar como prueba conversaciones de WhatsApp o de cualquier otra red social?

- ✓ *Lo que se hace comúnmente es imprimir una captura de pantalla o en algunas ocasiones se requiere a algún Notario para que de fe de lo que está en la pantalla y luego mediante acta notarial se presenta ante el juez competente y la fiscalía*.

XII. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital que utilice actualmente para litigar o conocer casos penales en Guatemala.

- ✓ *Desconozco de textos que puedan tratar de estos temas*.

XIII. Según su experiencia, ¿considera usted que, dentro del proceso penal guatemalteco de diligencia, ofrece y valora la prueba electrónica y digital en una forma empírica y bajo los mismos principios de la prueba tradicional?

- ✓ *A la fecha considero que no se una un procedimiento prestablecido y cada profesional lo interpreta a su manera y puedo entonces decir que se maneja en forma empírica, sería muy bueno tener inducciones y capacitaciones sobre estos temas para que mejoremos el servicio a nuestros clientes*.

e) Entrevista realizada a la <u>Licenciada Betzy Mireida Alvarado Alfonzo</u>, quien es Jueza de Primera Instancia Penal, Narcoactividad y Delitos contra el Ambiente de Quetzaltenango, el 18 de febrero de 2021.

I. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

- ✓ *Es muy importante que esta sea conocida en Guatemala en virtud que la expansión en el uso de la tecnología cada día va en forma muy acelerada y conocer los diferentes temas tecnológicos por parte de jueces, fiscales y abogados defensores coadyuve a que el sistema de justicia cumpla con su función inherente, además conocer los procedimientos de la informática forense ayudan de mejor forma para que el juez tenga una ilustración concreta en hechos donde otros medios probatorios no son suficientes o claros, es decir la tecnología ayuda de gran forma hoy en día para la resolución de casos en donde la prueba científica es fundamental.*

II. Según su experiencia ¿qué protocolos y metodología ha visto que son más utilizados en el procesamiento de una escena de crimen digital (Cadena de custodia digital, embalaje)?

- ✓ *He visto que el Ministerio Publico manejan procedimientos estándares en la recolección de evidencias y muchas veces en tratamiento de evidencia electrónica y digital se queda muy limitado su actuar porque considero que este tipo de pruebas deben tratarse de maneja muy diferentes especial, esto porque se debe tomar en cuenta la volatilidad y puede perderse información valiosa, el ente fiscal hace su mejor esfuerzo pero aún tiene muchas cosas que mejorar en estos temas en virtud que el embalaje y cadena de custodia son los mismos y esto puede originar un perjuicio en el desarrollo del proceso*.

III. Según su experiencia, ¿existe seguridad y certeza jurídica cuando se embala evidencia electrónica y digital aun cuando no se utilizan bolsas o cajas de Faraday. Y ¿cómo se efectúa la certificación digital de la evidencia digital y electrónica mediante MD5 dentro de proceso penal?

- ✓ *Como lo decía anteriormente existe mucho por mejorar, en varios casos se me han presentado dispositivos electrónicos y que en varias ocasiones se observa que ha sido manipulado con tal de obtener*

datos que ayuden a la investigación, siendo objetiva y como juez contralora he resuelto que es imperativo que se respete la privacidad de las comunicaciones y que si el ente fiscal necesita extraer determinada información debe requerir autorización judicial, esto para que se cumpla con una tutela judicial efectiva y evitar que existan vicios en el procedimiento.

IV. ¿Según su experiencia, ¿cuál es la importancia del sistema UFED (Universal Forensic Extraction) en una escena del crimen digital y en el análisis forense de información digital?

- ✓ *Sería muy atinado que el ente fiscal pudiera implementar este tipo de tecnología ya que el obtener información en el escenario criminal con este tipo de sistemas garantiza que desde el inicio la evidencia sea integra y cuando sea discutida en la fase de debate se observe la misma integridad, sabemos que es necesario una considerable inversión, pero como sujetos y partes procesales debemos de encaminar nuestro actuar en aras de la justicia*.

V. Según su experiencia, ¿cuál es la función de un Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery en el tratamiento de la evidencia electrónica y digital dentro un proceso penal?

- ✓ *No conozco que en algún proceso penal me hayan presentado este tipo de especialistas tanto como consultores como también como peritos del INACIF, sin embargo, sería muy interesante saber el tipo de aporte o expertiz que ellos manejan*.

VI. Según su experiencia, ¿el Ministerio Público cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales?

- ✓ *Siendo objetiva opino que no tiene el personal adecuado en virtud que hay muchos técnicos de la escena del crimen que tratan la evidencia electrónica y digital que una evidencia de otra categoría y esto en muchas ocasiones vicia el procedimiento o causa que la prueba sea ilegitima o ilegal*.

VII. Según su criterio, ¿cuál la importancia de aplicar los protocolos ISO/IEC 27037 e ISO/IEC27042 en el proceso penal guatemalteco?

- ✓ *No había sobre este tipo de protocolos en materia probatoria, aunque en algunas ocasiones vi en algunos informes de Inacif que tenían como referencia este tipo de protocolos, aunque no recuerdo el contenido como tal.*

VIII. ¿Además de lo contenido en el Decreto 47-2008 "Ley para el reconocimiento de las comunicaciones y firmas electrónicas –articulo 9 al 14- sobre el tratamiento de la evidencia electrónica y digital, ¿que otro fundamento legal considera que puede utilizarse para darle credibilidad y valor probatorio a la prueba electrónica y digital en el proceso penal guatemalteco?

- ✓ *En el caso que ostento he visto muy poco manejo en conceptos y doctrina sobre evidencia digital y electrónica, no recuerdo que fiscales o abogados litigantes hayan utilizado de alguna forma en su argumentación lo relativo al Decreto 47-2008, regularmente utilizan como fundamento legal lo concerniente al artículo veinticuatro de la Constitución Política de la República de Guatemala, el principio de tutela judicial efectiva y libertad probatoria, además de Convenios y Tratados en materia de Derechos Humanos.*

IX. Según su experiencia, ¿cómo se ofrece y diligencia la prueba digital de memoria RAM, volcados de memoria y espectrogramas de audio?

- ✓ *En los años que llevo desempeñando mi rol como jueza no he escuchado que algunos de los sujetos procesales hayan presentado este tipo de pruebas*.

X. ¿Considera usted que un pantallazo o screenshot es prueba documental o prueba digital?

- ✓ *Considero que no es prueba documental, aunque sirve de soporte para acreditar algunos extremos y tampoco es digital porque esta debe reunir determinados requisitos para que sea considerada como legal y legítima, uno de esos aspectos es una certificación digital.*

XI. Según su experiencia, ¿cuál es el mecanismo que se utiliza en el proceso penal guatemalteco para validar o incorporar como prueba conversaciones de WhatsApp o de cualquier otra red social?

- ✓ *Es muy común que lo sujetos procesales presenten impresiones o también traten de incorporar la prueba a través de actas notariales o declaraciones juradas, aspecto que no estoy de acuerdo porque sé que existen procedimientos especiales y es ahí donde debe de profundizarse en esos temas para dotar de seguridad jurídica a la prueba*.

XII. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital que utilice actualmente para litigar o conocer casos penales en Guatemala.

- ✓ *Desconozco en este momento algún material en especial*.

XIII. Según su experiencia, ¿considera usted que, dentro del proceso penal guatemalteco de diligencia, ofrece y valora la prueba electrónica y digital en una forma empírica y bajo los mismos principios de la prueba tradicional?

- ✓ *Considero que los jueces que tenemos el control de la investigación hacemos nuestro mejor esfuerzo de conformidad a la preparación que*

tenemos en estos temas; los mismos abogados litigantes y fiscales también hacen lo que pueden sin embargo no puedo hablar de que sea empírico sino que por el contrario se maneja en la forma en que se trata otro tipo de material probatorio; estoy de acuerdo que debemos de seguir actualizados y debemos seguir en formación constante en estos temas para evitar que se utilicen formas empíricas en el tratamiento de la evidencia electrónica y digital.

f) Entrevista realizada al <u>MSc. Jairo Boris Calderón de León</u>, quien es Juez presidente del Tribunal de Sentencia Penal, Narcoactividad y Delitos contra el Ambiente en Procesos de Mayor Riesgo de Quetzaltenango, el 23 de febrero de 2021.

I. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

- ✓ *Es fundamental, la criminalidad va a avanzando y usan los medios tecnológicos para alcanzar sus fines. El Estado tiene la responsabilidad de capacitar a sus personeros o funcionarios, en el ambiente tecnológico. Es importante que se combata la criminalidad porque en muchas ocasiones se usa el ambiente tecnológico para cometer ilícitos y en otros el fin es el perjuicio de los medios tecnológicos, por ejemplo, los ciberdelitos, el Estado debe dar una respuesta sólida según el mandato constitucional. El beneficio de la informática forense no es nuevo, otros países como Argentina, Chile y Colombia, el uso de la informática jurídica coadyuva a que las personas accedan a la justicia. Peritos se ven beneficiados en el uso de la tecnología por la carga de trabajo. Chile es un país que ha avanzado en esos temas y más en estos tiempos de pandemia. Se debe de invertir recursos y capacitación. Como jueces se es más*

productivo utilizar salas virtuales porque el servicio se presta de mejor forma por la misma carga de trabajo.

II. Según su experiencia ¿qué protocolos y metodología ha visto que son más utilizados en el procesamiento de una escena de crimen digital y en la presentación de la prueba electrónica y digital en debate? (Cadena de custodia digital, embalaje)?

- ✓ *Es necesario apuntar que el ente fiscal tiene retos que superar en cuanto a la presentación de evidencias porque los mismos errores que se origina en el plano presencial en las evidencias físicas corre el riesgo que se traslade al plano digital. Por la fase en la que me desenvuelvo dentro del proceso penal en que me desenvuelvo puedo indicar que el ente fiscal en muchas ocasiones no sabe cómo demostrar e ilustrar al juez este tipo de pruebas, es decir no sabe cómo utilizar los medios digitales*.

III. Según su experiencia, ¿existe seguridad y certeza jurídica cuando se embala evidencia electrónica y digital aun cuando no se utilizan bolsas o cajas de Faraday. Y ¿cómo se efectúa la certificación digital de la evidencia digital y electrónica mediante MD5 dentro de proceso penal?

- ✓ *El problema que existe es que el ente fiscal no tiene una planificación estratégica para tratar los casos según sea su naturaleza, porque cuando se trata de manejar esa evidencia electrónica tratan de emplearse métodos o técnicas estándar, en mi experiencia he visto que tratan de diligenciarse y presentarse todos los casos de la misma forma, el juez debe tener la amplitud para conocer estos temas tecnológicos pero también los demás sujetos que interactúan en el proceso penal deben tener esa apertura. Por ejemplo, hay dispositivos electrónicos que se le dan el mismo tipo de tratamiento a sabiendas que existe la posibilidad de alterar o modificar el dispositivo en forma externa; existe un grato reto de actualización y especialización para*

evitar este tipo de asuntos. El juez debe ser objetivo, pero eso no impide el referido juez de control exija al Estado en este caso a través del Ministerio Público para que tome la debida diligencia y mejore ese tratamiento de la evidencia electrónica y digital, porque si se le da el mismo tratamiento por ejemplo a una billetera, cualquier objeto que a disco duro o algún dispositivo el juez debe impulsar la debida diligencia, con esto se resguarda en forma oportunidad y debida los indicios de tipo digital que al final de cuentas será analizada por el Tribunal de juicio que serán quienes analizaran toda esa cadena de actos en materia probatoria en el momento procesal correspondiente.

IV. ¿En cuanto al tratamiento de la información que se obtiene de las interceptaciones telefónicas contenidos en discos compactos que tipo d falencias consideran que existen?

- ✓ *Existe un desconocimiento generalizado en donde debe analizarse la forma en que se traslada la información a los discos, es decir la información debemos de contextualizar que la información está almacenada en los servidores y es ahí se efectúa el análisis y el problema es que no se explica cuál es el procedimiento que se efectúa en el traslado de información de los servidores a los dispositivos de almacenamiento es decir a los discos compactos y resulta preocupante que en muchas ocasiones los analistas efectúan ese traslado de información a algunas presentaciones de Power Point, no dudo de lo completo de esta herramienta de ofimática pero considero que existen herramientas más avanzadas y que pueden proveer de seguridad jurídica que sirvan para la presentación y exposición de las ideas o tesis fiscal. Se puede poner en tela de juicio que la información que contiene la presentación sea la misma que está contenida en el disco compacto y la misma que está en los servidores. Considero que esa información debe estar contenido en lugares remotos para que sea segura, porque esas presentaciones en Power Point deja mucho*

que desear. Es muy delicado que un analista traslade la información de tipo digital de un lado a otro y pretenda presentarla porque se debe entonces entrar a una discusión fuerte sobre si es válido ese escenario donde se ignora si el analista es idóneo o no.

V. Según su experiencia, ¿ha visto la participación de algún experto como: ¿Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery en el tratamiento de la evidencia electrónica y digital dentro un proceso penal?

- ✓ *No he tenido la oportunidad de escuchar sobre este tipo de expertos, aunque sería muy interesante saber el aporte que darían para el caso concreto*.

VI. Según su experiencia, ¿el Ministerio Público cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales?

- ✓ *Desconozco cuáles sean las políticas internas, pero le comento que he tenido sociólogos, abogados, técnicos en información que manejan este tipo de indicios y si los comparamos con los estándares aceptables estimo que estamos muy distantes de tener este tipo de personas con expertiz adecuada*.

VII. En su experiencia, ¿en la fase de conclusiones han basado sus argumentos en la aplicación o no de los protocolos ISO/IEC 27037 e ISO/IEC27042?

- ✓ *No, sin embargo, si han apuntado sobre el método de obtención de los datos, en ocasiones se usan métodos que son métodos especiales de investigación para investigar casos de delincuencia común. El tribunal de juicio no puede valorar pruebas en forma ilegal. Esos protocolos no se usan porque como abogados en muchas ocasiones somos tan positivistas afirmando que si no está en la ley no es válido.*

VIII. En su experiencia, ¿en la fase de conclusiones han basado sus argumentos en el Decreto 47-2008 “Ley para el reconocimiento de las comunicaciones y firmas electrónicas –articulo 9 al 14- sobre el tratamiento de la evidencia electrónica y digital, ¿que otro fundamento legal considera que puede utilizarse para darle credibilidad y valor probatorio a la prueba electrónica y digital en el proceso penal guatemalteco?

- ✓ *En ningún momento he escuchado ese tipo de argumentaciones*.

IX. ¿Considera usted que un pantallazo o screenshot es prueba documental o prueba digital?

- ✓ *Todo puede ser prueba, el problema no es que “es” sino la forma de presentación, se debe evaluar la posición del investigador, es decir si podía hacerlo o no, si había autorización judicial, verificar que no haya existido una alteración de la información y verificar que la metadata sea integra y ver la huella digital de la misma información para acreditar que sea integra. Se deben respetar las reglas procesales para dotarle de seguridad jurídica al caso en investigación*.

X. ¿Según su experiencia, ¿le han presentado en alguna ocasión alguna certificación digital de la evidencia digital y electrónica mediante MD5 dentro de proceso penal?

- ✓ *En ningún momento, creo que sería muy exigente solicitar eso o esperar que se pudiera presentar ello por el ente fiscal, sin embargo, considero que si se pudiera tratar este tipo de extremos como la certificación digital coadyuvaría mucho a conocer la verdad histórica de los hechos y que en su momento analizamos uno o dos medios de prueba podría ser que el uso de medios tecnológicos podría existir celeridad en la valoración y apreciación de diferentes hechos.*

XI. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital a lo interno del Organismo Judicial.

- ✓ *Que yo conozca no, la escuela ha hecho sus mejores esfuerzos, pero han sido aislados. Nosotros como funcionarios del Organismo Judicial tenemos como postulado ético el prepararnos a lo externo para mejorar el servicio, es una responsabilidad de todos los actores del sistema de justicia. En el Colegio de Abogados no he visto de algún material al respecto, todas estas limitantes son parte del sistema que tiene el reto de mejorar y capacitar a sus funcionarios.*

g) Entrevista realizada al <u>Licenciado Oscar Iván Alvarado Serrano</u>, quien es fiscal de la Fiscalía Especial contra la Impunidad Agencia Quetzaltenango, el 03 de marzo de 2021.

I. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

- ✓ *En el Ministerio Público la forma en que se trata este tipo de evidencia debe ser especializada, si no se trata de buena forma podría ocasionar el daño irreversible y que puede repercutir en el debate. El manejo de muy importante*.

II. Según su experiencia ¿qué protocolos y metodología ha visto que son más utilizados en el procesamiento de una escena de crimen digital (Cadena de custodia digital, embalaje)?

- ✓ *El fiscal que tiene a cargo el caso debe tener cuidado, la fiscalía contra el delito de extorsión es una de las que impulsa este tipo de protocolos para resguardar la evidencia. El procedimiento que se debe seguir es que cuando se recolecta la evidencia se debe guardar en una bolsa especial o un embalaje especial para evitar que el dispositivo se destruya, también ayuda para evitar que se borre la información en forma remota. El Ministerio Público no cuenta con*

recursos, se maneja mucho que en el caso de los dispositivos se colocan en modo avión para evitar daño a los dispositivos.

III. Según su experiencia, ¿existe seguridad y certeza jurídica cuando se embala evidencia electrónica y digital aun cuando no se utilizan bolsas o cajas de Faraday. Y ¿cómo se efectúa la certificación digital de la evidencia digital y electrónica mediante MD5 dentro de proceso penal?

- ✓ *Desconozco sobre el uso de la cadena de custodia digital, la informática avanza mucho y en la institución no existen recursos para obtener un embalaje y cadena de custodia digital, las instituciones no están capacitadas para manejar este tipo de procedimientos porque resulta muy oneroso y debe ser un compromiso de los entes que intervienen en el sector justicia porque a la fecha descuidan estos procedimientos que muchas veces son vitales para la investigación, actualmente solo se llega al embalaje y cadena de custodia física pero la certificación digital no se da*.

IV. ¿Según su experiencia, ¿cuál es la importancia del sistema UFED (Universal Forensic Extraction) en una escena del crimen digital y en el análisis forense de información digital?

- ✓ *En la escena del crimen los encargados de recabar la información no cuentan con ese equipo, incluso se usan bolsas de papel para resguardar esa información. Se necesita autorización de juez para realizar la extracción de información, existe una unidad en el Ministerio Público que se encarga de ver todo ese tema de digitalización*.

V. Según su experiencia, ¿cuál es la función de un Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery en el tratamiento de la evidencia electrónica y digital dentro un proceso penal?

- ✓ *No conozco a este tipo de especialistas, sin embargo, en los casos en los que he estado los sujetos procesales llevan a algunas personas para que les auxilien, pero no a éstos que usted preguntó, además resulta muy oneroso que se pague a uno de estos especialistas*.

VI. Según su experiencia, ¿el Ministerio Público cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales?

- ✓ *Existe una mala práctica por parte de Agentes fiscales y auxiliares fiscales de designar a personal de otras áreas del Ministerio Público para efectuar este tipo de procedimientos, pero esto se da porque muchas veces no hay este tipo de personal capacitado o si lo hay son muy pocos y están muy sobrecargados de trabajo. Hay mucho desconocimiento en el manejo de información*.

VII. Según su criterio, ¿cuál la importancia de aplicar los protocolos ISO/IEC 27037 e ISO/IEC27042 en el proceso penal guatemalteco?

- ✓ *No había escuchado sobre ese tipo de protocolos, la Comisión Internacional contra la Impunidad tenía personal capacitado y ellos manejaban la evidencia para luego presentar informes, pero no sé si tiene relación con la pregunta planteada*.

VIII. ¿Además de lo contenido en el Decreto 47-2008 “Ley para el reconocimiento de las comunicaciones y firmas electrónicas –articulo 9 al 14- sobre el tratamiento de la evidencia electrónica y digital, ¿que otro fundamento legal considera que puede utilizarse para darle credibilidad y valor probatorio a la prueba electrónica y digital en el proceso penal guatemalteco?

- ✓ *No he utilizado el decreto 47-2008, en las audiencias penales solo se limita a demostración o reproducción en audiencias, como fiscales nos gustaría demostrar que dentro de un dispositivo electrónico existe información relevante para el caso que se investiga, pero solo nos*

limitamos a la reproducción de lo que ahí se contiene sin llegar a mayores detalles.

IX. Según su experiencia, ¿cómo se ofrece y diligencia la prueba digital de memoria RAM, volcados de memoria y espectrogramas de audio?

- ✓ *Desconozco esa terminología tal vez en alguna ocasión se utilizó con algún otro nombre, pero sinceramente es algo que me consta*.

X. ¿Considera usted que un pantallazo o screenshot es prueba documental o prueba digital?

- ✓ *Todo lo que puede ayudar en la investigación puede ser un indicio, entonces solo es un indicio*.

XI. Según su experiencia, ¿cuál es el mecanismo que se utiliza en el proceso penal guatemalteco para validar o incorporar como prueba conversaciones de WhatsApp o de cualquier otra red social?

- ✓ *En algunas fiscalías, como por ejemplo de Extorsiones existe una unidad llamada enlace que es la que localiza información en redes sociales para que luego nosotros como fiscales la analicemos para seguir la ruta de investigación, como por ejemplo los contratos de Facebook, fotografías y otra información, porque son datos públicos*.

XII. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital que utilice actualmente para litigar o conocer casos penales en Guatemala.

- ✓ *Desconozco de algún tipo de material de esta índole*.

XIII. Según su experiencia, ¿considera usted que, dentro del proceso penal guatemalteco de diligencia, ofrece y valora la prueba electrónica y digital en una forma empírica y bajo los mismos principios de la prueba tradicional?

- ✓ La prueba electrónica y digital se trata igual que la prueba documental y en forma empírica, no se determina si se está o no haciendo un buen uso de esa evidencia, el juez es el que decide, se valora al igual que una prueba documental y según la apreciación del juez.

h) Entrevista realizada la <u>Dra. Zonia Edith Soto Barrios</u>, quien es abogada litigante, el 05 de marzo de 2021.

I. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

- ✓ *El Ministerio Público muchas veces no se ha valido de estos medios de investigación. He tenido experiencias donde el ente fiscal y la policía vulneran derechos de las personas en la manipulación de indicios electrónicos. El ente fiscal tiene muchas falencias en el tratamiento de evidencia electrónica y digital*. Y muchas veces la policía manipula este tipo de evidencia y sin tener ningún tipo de conocimientos.

II. Según su experiencia ¿qué protocolos y metodología ha visto que son más utilizados en el procesamiento de una escena de crimen digital (Cadena de custodia digital, embalaje)?

- ✓ *El ente fiscal maneja los indicios electrónicos como si fuera cualquier otro, no siguen ningún protocolos o metodología alguna. Hay sentencias de la Corte de Constitucionalidad que protege la privacidad de las personas y en donde se establece que se debe tener autorización judicial para extraer la información de los dispositivos electrónicos.*

III. En su experiencia, ¿en alguna ocasión ha invocado usted la ruptura de cadena de custodia digital en alguna audiencia penal?

- ✓ *Soy muy cuidadosa para ver estos aspectos y verificar estos extremos y si existe alguna anomalía promuevo algún incidente*.

IV. En su experiencia, ¿en algún proceso penal el Ministerio Publico ha presentado la certificación digital de los indicios electrónicos o digitales?

- ✓ *No he visto eso, solo recuerdo que una ocasión el Ministerio Público oculto información relevante de un disco duro externo, que, no obstante, se nos facilitó la información, pero no había nada que garantizara en forma digital que la información había sido manipulada o proporcionada en forma parcial.*

V. Según su experiencia, ¿en alguna ocasión ha impugnado por el hecho que la evidencia electrónica y digital no se encuentra en bolsas o cajas de Faraday?

- ✓ *No he llegado a profundizar en este tema.*

VI. Según su experiencia, ¿cuál es la función de un Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery en el tratamiento de la evidencia electrónica y digital dentro un proceso penal?

- ✓ *Solo conozco la importancia del Analista Digital que en algunos casos se encarga de realizar un estudio profundo de la información obtenida. En el Instituto Nacional de Ciencias Forenses dudo que haya ese tipo de expertos*.

VII. En su experiencia, ¿ha impugnado alguna prueba de interceptación telefónica en casos de delincuencia organizada?

- ✓ *No lo he hecho, sin embargo, tengo un caso que estoy trabajando actualmente y probablemente ahí lo haré para saber si se siguió o no un protocolo determinado. Pero si le sé decir que como abogados litigantes carecemos de conocimientos técnicos para saber cómo*

atacar este tipo de aspectos y no se encuentra fácilmente a un consultor técnico con este tipo de conocimientos.

VIII. En su experiencia, ¿en algún proceso penal se ha invocado el uso de los protocolos ISO/IEC 27037 e ISO/IEC27042?

- ✓ *En mi experiencia no lo he visto*.

IX. En su experiencia, ¿ha utilizado en algún proceso penal el Decreto 47-2008 "Ley para el reconocimiento de las comunicaciones y firmas electrónicas?

- ✓ *A la fecha no lo he utilizado.*

X. En su experiencia, ¿ha presentado o impugnado la prueba relativa a memoria RAM, volcados de memoria y espectrogramas de audio?

- ✓ *Posiblemente en alguna ocasión con algún consultor técnico sin embargo no tengo el conocimiento expreso sobre estos términos.*

XI. ¿Considera usted que un pantallazo o screenshot es prueba documental o prueba digital?

- ✓ *Hay libertad de prueba, pero tiene que usarse el medio idóneo, un pantallazo no tiene ningún tipo de valor y si fuere documental tendría que tener otras características*. Es muy común que en material civil a ese pantallazo se le adjunte un acta notarial para darle valor probatorio en forma conjunta.

XII. En su experiencia, ¿jueces, fiscales y abogados manejan con propiedad la informática forense y lo relativo a la prueba electrónica y digital?

- ✓ *Aún falta mucho en conocer estos temas, considero que este tema de investigación será de gran importancia para todos los colegas.*

XIII. Según su experiencia, ¿cuál es el mecanismo que se utiliza en el proceso penal guatemalteco para validar o incorporar como prueba conversaciones de WhatsApp o de cualquier otra red social?

- ✓ *Lo que se hace es presentar extractos de la información para darle credibilidad a la información, porque solo se presenta lo que le interesa a la parte procesal. Tendría que llevar al procedimiento determinado, pero actualmente no se emplea alguno en específico.*

XIV. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital que utilice actualmente para litigar o conocer casos penales en Guatemala.

- ✓ *No conozco alguno porque lo que se hace en la práctica es buscar la información en Google algo que me sirva para usarlo en el proceso, pero sin mayor formalidad*.

XV. Según su experiencia, ¿considera usted que, dentro del proceso penal guatemalteco de diligencia, ofrece y valora la prueba electrónica y digital en una forma empírica y bajo los mismos principios de la prueba tradicional?

- ✓ *Es empírica, sin tener los lineamientos pertinentes, según como se crea conveniente, los jueces le dan valor en forma empírica basado en la libertad de prueba.*

10.5. Formulario de encuesta.

A continuación, se presenta el formulario utilizado para realizar la encuesta a los diferentes profesionales, entre ellos jueces, fiscales del Ministerio Público y abogados litigantes, abogados de la Procuraduría General de la Nación, consultores técnicos, técnicos en investigaciones criminalísticas y profesionales jurídicos con funciones en instituciones privadas y otras instituciones públicas siendo el siguiente:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE OCCIDENTE
DIRECCION DE ESTUDIOS DE POSTGRADO
MAESTRIA EN DERECHO PENAL

BOLETA DE ENCUESTA.

La presente boleta de encuesta tiene como finalidad recabar datos de campo relativos al tema denominado "EL DILIGENCIAMIENTO, OFRECIMIENTO Y VALORACION DE LA PRUEBA ELECTRONICA Y DIGITAL EN CASOS DE DELINCUENCIA ORGANIZADA", tema que como punto de tesis se desarrolla en la Maestría en Derecho Penal. Se hace de su conocimiento que la información que usted brinde será tratada en forma confidencial, será utilizada única y exclusivamente para fines académicos. Al agradecer el favor de su atención se le ruega marcar con una "X" la opción que considere correcta y explicar brevemente cuando el caso lo amerite.

Ciudad de Quetzaltenango, febrero del año 2021.

1. ¿Conoce usted qué es la prueba electrónica y digital certificada?
SI_____ NO_____
Si su respuesta es SI, explique la diferencia entre ellas: ___

2. ¿Conoce usted en qué consiste la cadena de custodia digital?
SI_____ NO_____
Si su respuesta es SI, explique brevemente en que consiste: ___

3. ¿Conoce usted en que consiste la certificación digital de prueba electrónica y digital mediante un algoritmo Hash??

SI_____ NO_____

4. ¿Usted ha ofrecido y diligenciado prueba electrónica y digital en algún proceso penal?

SI_____ NO_____

5. ¿Conoce usted el procedimiento técnico y científico que deben utilizar los técnicos de la Dirección de Investigaciones Criminalísticas del Ministerio Público para procesar una escena del crimen en donde se encuentra evidencia electrónica y digital?

SI_____ NO_____

Si su respuesta es SI, explique brevemente el procedimiento: ___

6. ¿Conoce usted los procedimientos, metodología y técnicas que son utilizados por el Ministerio Público para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital?

SI_____ NO_____

7. ¿Considera usted que los abogados litigantes conocen los procedimientos, metodología y técnicas que son utilizados en el proceso penal para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital?

SI_____ NO_____

8. ¿Considera usted que los jueces en materia penal conocen los procedimientos, metodología y técnicas que son utilizados para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital?

SI_____ NO_____

9. ¿Considera usted que los fiscales del Ministerio Público conocen y dominan la informática forense y los procedimientos idóneos para diligenciar y ofrecer prueba electrónica y digital dentro de un proceso penal, inclusive en casos de delincuencia organizada?

SI_____ NO_____

Explique las deficiencias o aciertos: ___

10. ¿Considera usted que los abogados litigantes conocen y dominan la informática forense y los procedimientos idóneos para diligenciar y ofrecer prueba electrónica y digital dentro de un proceso penal, inclusive en casos de delincuencia organizada?

SI_____ NO_____

Explique las deficiencias o aciertos: ___

11. ¿Considera usted que los jueces conocen y dominan la informática forense y los procedimientos idóneos para valorar prueba electrónica y digital dentro de un proceso penal, inclusive en casos de delincuencia organizada?

SI_____ NO_____

Explique las deficiencias o aciertos: ___

12. ¿Tiene conocimiento del uso que se le da en el proceso penal a las normativas ISO/IEC 27037:2012, ISO/IEC 27042?

SI_____ NO_____

13. ¿Tiene conocimiento de la aplicación en materia penal que se le da al Decreto 47-2008 Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas?

SI_____ NO_____

14. ¿Tiene conocimiento de las categorías, calidades y competencias que debe tener un Perito Forense Digital que maneja evidencia electrónica y digital?

SI_____ NO_____

15. ¿Conoce usted si la Unidad de Capacitación del Ministerio Público posee manuales o instrucciones sobre el tratamiento de la evidencia electrónica y digital?
SI_____ NO_____
Si su respuesta es SI, indique cuáles: ___

16. ¿Conoce usted si la Escuela de Estudios Judiciales del Organismo Judicial posee manuales o instrucciones sobre el tratamiento de la evidencia electrónica y digital?
SI_____ NO_____
Si su respuesta es SI, indique cuáles: ___

17. ¿Considera usted que los abogados litigantes conocen manuales o textos guías sobre el tratamiento de la evidencia electrónica y digital?
SI_____ NO_____
Si su respuesta es SI, indique cuáles: ___

18. ¿Considera usted que los abogados litigantes implementan y aplican en su litigio penal, fundamentos teóricos y prácticos de evidencia y prueba electrónica y digital?
SI_____ NO_____

19. ¿Considera usted si los fiscales del Ministerio Público implementan y aplican en su litigio penal, fundamentos teóricos y prácticos de evidencia y prueba electrónica y digital?
SI_____ NO_____

20. ¿Conoce usted los criterios que tienen los jueces en materia penal para apreciar y valorar la prueba electrónica y digital?
SI_____ NO_____
Si su respuesta es SI, indique cuáles: ___

21. ¿Ha litigado en algún debate oral y público en el que se haya emitido sentencia condenatoria con base a la apreciación y valoración de prueba electrónica y digital?
SI_____ NO_____

22. ¿Ha litigado en algún debate oral y público en el que se haya emitido sentencia absolutoria con base a la apreciación y valoración de prueba electrónica y digital?

SI_____ NO_____

23. ¿Conoce alguna resolución judicial de un tribunal de alzada en el que se haya emitido un razonamiento y fundamentación técnica y legal sobre prueba electrónica y digital en caso de delincuencia común?

SI_____ NO_____

Si su respuesta es SI, indique el número de expediente o resolución: ___

24. ¿Conoce alguna resolución judicial de un tribunal de alzada en el que se haya emitido un razonamiento y fundamentación técnica y legal sobre prueba electrónica y digital en casos de delincuencia organizada?

SI_____ NO_____

Si su respuesta es SI, indique el número de expediente o resolución: ___

25. ¿Tiene usted conocimiento de algún caso de delincuencia organizada en el que se hayan empleado prácticas arbitrarias para el ofrecimiento y diligenciamiento de prueba electrónica y digital?

SI_____ NO_____

Si su respuesta es SI, indique cuáles: ___

26. ¿Tiene conocimiento de los protocolos que existen para darle validez a la prueba electrónica y digital?

SI_____ NO_____

27. ¿Considera usted que la Unidad de Capacitación del Ministerio Público forma y capacita a técnicos y a fiscales en temas relativos a la informática forense y el tratamiento de la prueba electrónica y digital?

SI_____ NO_____

28. ¿Considera usted que la Escuela de Estudios Judiciales forma y capacita a jueces en materia penal en temas relativos a la informática forense y el tratamiento de la prueba electrónica y digital?

SI_____ NO_____

29. ¿Considera usted el Colegio de Abogados y Notarios forma y capacita a sus agremiados en temas relativos a la informática forense y el tratamiento de la prueba electrónica y digital?

SI_____ NO_____

30. ¿Conoce usted el nombre de entidades privadas que capaciten sobre temas relativos la informática forense y el tratamiento de la prueba electrónica y digital?

SI_____ NO_____

Si su respuesta es SI, explique cuáles: ___

31. ¿Estaría dispuesto a recibir capacitaciones a cargo de Peritos Forenses Digitales para fortalecer sus conocimientos en Derecho Informático e Informática Forense?

SI_____ NO_____

ID Y ENSEÑAD A TODOS

10.6. Guía de entrevista.

A continuación, se presenta la guía que fue utilizada para realizar la entrevista a los diferentes profesionales encontrándose jueces, fiscales del Ministerio Público y abogados litigantes, siendo la siguiente:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE OCCIDENTE
DEPARTAMENTO DE ESTUDIOS DE POSTGRADO

GUIA DE ENTREVISTA

OBJETO DE ESTUDIO "EL DILIGENCIAMIENTO, OFRECIMIENTO Y VALORACION DE LA PRUEBA ELECTRONICA Y DIGITAL EN CASOS DE DELINCUENCIA ORGANIZADA".

ENTREVISTADO: _____

CARGO: _____

FECHA DE LA ENTREVISTA: _____

1. ¿Cuál es su opinión sobre la importancia, uso y utilidad de la informática forense, la prueba electrónica y digital en el sistema de justicia de Guatemala?

2. Según su experiencia ¿qué protocolos y metodología ha visto que son más utilizados en el procesamiento de una escena de crimen digital (Cadena de custodia digital, embalaje)?

3. Según su experiencia, ¿existe seguridad y certeza jurídica cuando se embala evidencia electrónica y digital aun cuando no se utilizan bolsas o cajas de Faraday?

4. Según su experiencia, ¿cómo se efectúa la certificación digital de la evidencia digital y electrónica mediante MD5 dentro de proceso penal?

5. ¿Según su experiencia, ¿cuál es la importancia del sistema UFED (Universal Forensic Extraction) en una escena del crimen digital y en el análisis forense de información digital?

6. Según su experiencia, ¿qué protocolos y técnicas forenses se aplican en el proceso penal guatemalteco para el tratamiento de la evidencia electrónica y digital?

7. Según su experiencia, ¿cuáles son los errores más comunes que se presentan cuando se procesa una escena del crimen en donde se encuentra evidencia electrónica y digital?

8. ¿Cuál es la diferencia entre evidencia electrónica y digital y prueba electrónica y digital?

9. Según su experiencia, ¿cuál es la función de un Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery en el tratamiento de la evidencia electrónica y digital dentro un proceso penal?

10. Según su criterio, ¿cuál la importancia de aplicar los protocolos ISO/IEC 27037 e ISO/IEC27042 en el proceso penal guatemalteco?

11. ¿Cuándo una persona sin las calidades necesarias descarga y guarda información en un dispositivo de almacenamiento para después presentarla como evidencia, que según protocolos internacionales se considera como contaminada o viciada, según su experiencia, que fundamento legal es válido para que el juez le otorgue o no valor probatorio?

12. ¿Además de lo contenido en el Decreto 47-2008 “Ley para el reconocimiento de las comunicaciones y firmas electrónicas –articulo 9 al 14- sobre el tratamiento de la evidencia electrónica y digital, ¿que otro fundamento legal considera que puede utilizarse para darle credibilidad y valor probatorio a la prueba electrónica y digital en el proceso penal guatemalteco?

13. Según su experiencia, ¿cómo se aplica la teoría del fruto del árbol envenenado en el área de la prueba electrónica y digital.

14. ¿Según su experiencia, cuáles son los errores más comunes que se cometen cuando se manipula evidencia digital y electrónica proveniente de interceptaciones telefónicas?

15. ¿En su función dentro del sistema de justicia, considera que los abogados litigantes, fiscales y jueces conocen con propiedad las características y principios propios sobre la prueba electrónica y digital?

16. Según su experiencia, ¿cómo se ofrece y diligencia la prueba digital de memoria RAM, volcados de memoria y espectrogramas de audio?

17. ¿Considera usted que un pantallazo o screenshot es prueba documental o prueba digital?

18. Según su experiencia, ¿cuál es el razonamiento que efectúa un juez para valorar o no la prueba electrónica y digital?

19. Según su experiencia, ¿cuál es el mecanismo que se utiliza en el proceso penal guatemalteco para validar o incorporar como prueba conversaciones de WhatsApp o de cualquier otra red social?

20. Según su experiencia, ¿el Ministerio Público cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales?

21. Podría indicarnos el nombre de algún manual, guía o texto sobre prueba electrónica y digital que utilice actualmente para litigar o conocer casos penales en Guatemala.

22. Según su experiencia, ¿considera usted que, dentro del proceso penal guatemalteco de diligencia, ofrece y valora la prueba electrónica y digital en una forma empírica y bajo los mismos principios de la prueba tradicional?

ID Y ENSEÑAD A TODOS.

10.7. Comprobación de hipótesis.

- El problema de investigación que en su momento se planteó fue el siguiente:

  ¿Existe seguridad jurídica y legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada?

- La hipótesis que resultó como respuesta provisional se formuló de la siguiente forma:

  No existe seguridad jurídica ni legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada dentro del proceso penal guatemalteco, como consecuencia de la inexistencia de procedimientos uniformes y reglamentados, poco conocimiento y uso escaso de los procedimientos adecuados para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la información.

- **Al interpretar los resultados que arrojó la investigación de campo, específicamente la encuesta, manifiesto lo siguiente**:

a) Los encuestados no conocen la diferencia entre una prueba electrónica y digital, además de ello, desconocen en que consiste una cadena de custodia digital.

b) Los encuestados no conocen en que consiste la certificación digital de la prueba electrónica y digital mediante un algoritmo hash.

c) Según la información cuantitativa proporcionada por los encuestados, no han ofrecido, diligenciado, o valorado (según corresponde su función) una prueba electrónica y digital dentro del proceso penal.

d) Además, resulta importante destacar que los encuestados, manifestaron que no conocen el procedimiento técnico y científico que deben utilizar los técnicos de la Dirección de Investigaciones Criminalísticas del Ministerio Público para procesar una escena del crimen endone se encuentra evidencia electrónica y digital, ni mucho menos la metodología y técnicas para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital.

e) Según la información cuantitativa obtenida, se establece que los abogados litigantes, jueces y fiscales del Ministerio Público no conocen los procedimientos, metodología y técnicas que son utilizados para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital, tampoco dominan la informática forense y los procedimientos idóneos para diligenciar y ofrecer prueba electrónica y digital dentro de un proceso penal, inclusive en casos de delincuencia organizada.

f) Los encuestados no conocen el uso que se le da en el proceso penal a las normativas ISO/IEC 27037:2012, ISO/IEC 27042.

g) Los encuestados no tienen conocimiento de la aplicación en materia penal que se le da al Decreto 47-2008 Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

h) Los encuestados no tienen conocimiento de las categorías, calidades y competencias que debe tener un Perito Forense Digital que maneja evidencia electrónica y digital.

i) Se establece, además, que los profesionales encuestados no conocen si la Unidad de Capacitación del Ministerio Público y Escuela de Estudios Judiciales poseen manuales o instrucciones sobre el tratamiento de la evidencia electrónica y digital. De esa misma cuenta se considera que los abogados litigantes no conocen manuales o textos guías sobre el tratamiento de la evidencia electrónica y digital.

j) Los encuestados afirman que abogados litigantes, jueces y fiscales del Ministerio Público no implementan ni aplican en su litigio penal, fundamentos teóricos y prácticos de evidencia y prueba electrónica y digital.

k) Los encuestados no conocen los criterios que tienen los jueces en materia penal para apreciar y valorar la prueba electrónica y digital.

l) Los encuestados indican que no han litigado en algún debate oral y público en el que se haya emitido sentencia condenatoria o absolutoria con base a la apreciación y valoración de prueba electrónica y digital, ni mucho menos alguna resolución judicial de un tribunal de alzada en el que se haya emitido

un razonamiento y fundamentación técnica y legal sobre prueba electrónica y digital en caso de delincuencia común o delincuencia organizada.

m) Los encuestados indican que no tienen conocimiento de algún caso de delincuencia organizada en el que se hayan empleado prácticas arbitrarias para el ofrecimiento y diligenciamiento de prueba electrónica y digital, a excepción del caso denominado “La Línea” en la ciudad de Guatemala.

n) Los entrevistados no tienen conocimiento de los protocolos que existen para darle validez a la prueba electrónica y digital.

o) Los entrevistados refieren que la Unidad de Capacitación del Ministerio Público, Escuela de Estudios Judiciales y el Colegio de Abogados y Notarios no forma ni capacita a técnicos, fiscales y jueces, según corresponde, en temas relativos a la informática forense y el tratamiento de la prueba electrónica y digital.

p) Los encuestados no conocen a entidades privadas que capaciten sobre temas relativos la informática forense y el tratamiento de la prueba electrónica y digital, a excepción de Redlif, Observatorio Guatemalteco de Delitos Informáticos.

q) Los encuestados después de responder a todos los cuestionamientos afirmaron que están dispuestos a recibir capacitaciones a cargo de Peritos Forenses Digitales para fortalecer sus conocimientos en Derecho Informático e Informática Forense.

- **De conformidad a la información proporcionada en las entrevistas realizadas podemos indicar lo siguiente**:

a) No se diferencia, trata ni se denomina así tal cual como prueba electrónica y digital. En la práctica solo tenemos peritos, testigos, documentos y objetos, puede existir prueba audiovisual pero no más que un video grabado no es prueba es electrónica, esto es lo más técnico y desarrollado y en la práctica hasta traen a un técnico para poner un video y eso no es prueba electrónica.

b) Todo puede ser prueba, el problema no es que “es” sino la forma de presentación, se debe evaluar la posición del investigador, es decir si podía hacerlo o no, si había autorización judicial, verificar que no haya existido una alteración de la información y verificar que la metadata sea integra y ver la huella digital de la misma información para acreditar que sea integra. Se deben respetar las reglas procesales para dotarle de seguridad jurídica al caso en investigación.

c) El problema que existe es que el ente fiscal no tiene una planificación estratégica para tratar los casos según sea su naturaleza, porque cuando se trata de manejar esa evidencia electrónica tratan de emplearse métodos o técnicas estándar

d) La prueba digital puede modificarse con mucha facilidad; la manipulación y destrucción de la prueba digital es más sensible si no lo manejan personas con el perfil adecuado y con la expertiz necesaria.

e) No se manejan correctamente los protocolos para extraer la información y eso puede repercutir en el proceso más adelante porque la contraparte puede objetar la forma en que se obtiene la información, el Ministerio Público utiliza bolsas o cajas de Faraday, solo bolsitas o cajas de cartón o similares.

f) No se utilizan la certificación digital de la evidencia electrónica y digital mediante un MD5 o similar, tampoco en audiencia se ha utilizado un sistema UFED (Universal Forensic Extraction). Sería muy atinado que el ente fiscal pudiera implementar este tipo de tecnología ya que el obtener información en el escenario criminal con este tipo de sistemas garantiza que desde el inicio la evidencia sea integra y cuando sea discutida en la fase de debate se observe la misma integridad, es necesario una considerable inversión.

g) A muchos jueces no les interesa como se certifica una evidencia toda vez que lo relativo a los procedimientos correctos se debe conocer hasta en debate.

h) No se conoce la función del Consultor Técnico como Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery.

i) La tarea de Inacif es segunda, por eso es importante la recolección de indicios por la fiscalía, es decir este es el primer momento; el peritaje de Inacif lo realiza sobre la base del indicio que es enviado y que si está viciado el procedimiento desde el inicio desde el momento que la fiscalía realiza su trabajo ahí surge el punto de discusión, dudo que un auxiliar fiscal tenga esa información para el buen tratamiento de la evidencia electrónica y digital.

j) El Ministerio Público no cuenta con el personal idóneo, capacitado y con el perfil adecuado para realizar la diligencia de extracción de información de dispositivos electrónicos y digitales.

k) Jueces, fiscales y abogados litigantes difieren en considerar que un pantallazo o screenshot es prueba documental o prueba digital.

l) La prueba electrónica y digital tiende a ser más tradicional es decir ingresar este tipo de prueba en algo que ya existe, es decir lo electrónico lo imprimimos y ya es prueba documental, hay algo electrónico y no lo entiendo entonces llamamos a un perito y esto ya es prueba pericial, se maneja en forma análoga, vemos ahí un gran error.

m) Dentro del proceso penal guatemalteco se diligencia, ofrece y valora la prueba electrónica y digital en una forma empírica y bajo los mismos principios de la prueba tradicional ocasionando una grave vulneración de derechos fundamentales para las partes procesales.

- El anterior análisis de los instrumentos de recolección de información nos permite manifestar que la hipótesis que al inició se planteó se confirmó totalmente, quedando así:

No existe seguridad jurídica ni legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada dentro del proceso penal guatemalteco, como consecuencia de la inexistencia de procedimientos uniformes y reglamentados, poco conocimiento y uso escaso de los procedimientos adecuados para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la información digital.

10.8. Conclusiones.

I) Después de realizar un trabajo minucioso en relación a identificar los mecanismos actuales que el Ministerio Público utiliza para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de información digital que posteriormente podría utilizarse como prueba electrónica y digital, se establece que el ente fiscal tiene una grave problema procedimental, toda vez que no existen mecanismos ni procedimientos uniformes o reglamentados, inclusive, que puedan orientar de mejor forma a los Técnicos en Investigaciones Criminalísticas del Ministerio Público (DICRI) cuando procesan un escenario criminal digital. Se identificó que los fiscales y los mismos técnicos no ubican la diferencia entre la prueba electrónica y digital, no implementan la cadena de custodia digital ni conocen la importancia de las cajas y bolsas de Faraday para la preservación de la información digital en sus procedimientos, todo esto por desconocimiento, además, se establece que no tienen el conocimiento necesario sobre las diferentes áreas que estudia el derecho informático y la informática forense a pesar que dentro de los procesos penales que actualmente se ventilan en las diferentes judicaturas tanto en casos de delincuencia común pero especialmente delincuencia organizada, a diario, los dispositivos electrónicos y los metadatos son parte fundamental en las investigaciones, siendo entonces que simplemente utilizan métodos pocos convencionales y no científicos afectando de gran forma los derechos humanos de las partes procesales, es decir se aplican procedimientos arbitrarios. Además se identificó que no tienen conocimiento sobre la aplicación de las normativas ISO/IEC 27037:2012, ISO/IEC 27042 , siendo la primera un protocolo internacional para identificar, recolectar, adquirir y preservar la evidencia digital y la segunda un protocolo para analizar e interpretar la evidencia digital, es decir, es crítico que el ente fiscal a la fecha no implemente a través de la Unidad de Capacitación del Ministerio Público (Unicap) capacitaciones encaminadas a fortalecer éstas áreas.

II) Respecto a los criterios que utilizan los jueces para la aceptación y valoración de la prueba electrónica y digital en el proceso penal, se establece que aplican las reglas de la prueba documental y prueba científica, es decir la apreciación y valoración que se le provee a la prueba electrónica y digital es muy distante a la que realmente se le debe proveer en materia pericial informática. Los jueces aplican criterios subjetivos originado por el desconocimiento en las áreas del derecho informático e informática forense bajo la idea subyacente que todo lo referente a dispositivos electrónicos y datos son parte de las ciencias de la computación o ingeniería y que para eso simplemente basta la participación de un consultor técnico con título o conocimiento en éstas áreas, sin embargo, en esta investigación pudimos establecer que la informática forense tiene un punto en común entre el derecho y la informática y que para ello existe el aporte fundamental de expertos en materia de evidencia electrónica y digital siendo estos los Peritos Forenses Digitales con sus diferentes roles: Primer Respondiente (Digital Evidence First Responder- DEFR), del Analista Digital (Digital Evidence Specialist DES) y el e-Discovery; en el entendido que el primero actual en el escenario criminal y debe implementar la cadena de custodia física y digital con el cuidado de insertar los dispositivos electrónicos en cajas o bolsas de Faraday, el segundo es quien recibe y analiza la información digital en todo su contexto y quien podría emitir un informe técnico y ejecutivo para dar conocer lo encontrado para que los sujeto procesales lo conozcan y entre al contradictorio en juicio; el tercero es decir el e-Discovery es el experto informático en utilizar herramientas forenses acordes para analizar los metadatos de los dispositivos objetos de investigación.

III) En relación a los conocimientos que tienen los usuarios del sistema de justicia penal sobre derecho informático, prueba digital y electrónica, en la investigación de campo a través de los diferentes instrumentos de recopilación de datos se estableció que abogados litigantes, jueces y fiscales no conocen los protocolos para el procesamiento de la evidencia electrónica y digital y que consecuentemente influye negativamente al momento que es presentado como prueba, y más aún, porque tampoco tienen conocimiento sobre la forma en que diligencia, ofrece y debe valorar la prueba electrónica y digital en casos de delincuencia común, mucho menos delincuencia organizada, que es más complejo; y para ello partimos indicando que desconocen la importancia en la implementación de la cadena de custodia digital, la certificación digital mediante un algoritmo Hash MD5 y las bolsas de Faraday en un proceso penal. Además, al hacer referencia al sistema UFED (Universal Forensic Extraction) solo se limitaron a que es utilizado en algunos procesos y que aparece en informes de investigación, sin embargo, desconocen la importancia de su uso en el procesamiento de un escenario criminal digital. En ese orden de ideas, también se identificó que no conocen el uso y aplicación de protocolos ISO/IEC 27037 e ISO/IEC27042 y del Decreto 47-2008 “Ley para el reconocimiento de las comunicaciones y firmas electrónicas dentro en el proceso penal guatemalteco. Existen otros protocolos que también se identificaron en el desarrollo del marco teórico sin embargo estos tienen una dinámica especial según el contexto del caso.

IV) De igual forma tal y como lo referí en la conclusión anterior, en la investigación de campo se estableció el desconocimiento de los diferentes temas en derecho informático e informática forense por los profesionales que actúan en el sector de justicia penal, pero esto va más allá, porque también se pudo establecer que dentro del área de la informática forense que incluye el tratamiento de la evidencia electrónica y digital también se desconocen fundamentos teóricos y prácticos para aplicar en litigio penal en relación a la prueba electrónica y digital que obviamente se transcribe en que se desconoce sobre la existencia de igual forma en sentencias condenatorias o absolutorias en estos temas con un razonamiento técnico y legal, aspecto que también fue comprobado y también se evidenció que los profesionales indicaron que conocen de casos en donde se emplearon malas prácticas para en el ofrecimiento y diligenciamiento de la prueba electrónica y digital. En ese mismo orden de ideas afirmamos que la preparación teórica y práctica de los usuarios del sistema de justicia penal sobre derecho informático, prueba digital y electrónica es limitada y Organismo Judicial a través de la Escuela de Estudios Judiciales, Ministerio Público a través de la Unidad de Capacitación y el Colegio de Abogados y Notarios por medio de la Unidad Académica no cuentan con planes o programas para formar y capacitar a los profesionales y mucho menos cuenta con manuales o textos guías que ayuden en su rol diario dentro del sistema de justicia penal, sin embargo también se comprobó que la gran mayoría de personas encuestada y entrevistadas está en la disposición de recibir capacitaciones a cargo de Peritos Forenses Digitales para fortalecer sus conocimientos en Derecho Informático e Informática Forense.

V) También podemos concluir que en referencia a las técnicas y metodología utilizada por los usuarios del sistema de justicia penal de Quetzaltenango sobre prueba digital y electrónica en relación a los protocolos internacionales en manejo de evidencia electrónica y digital existe una gran brecha digital, toda vez que no conocen la forma en que deben integrarse, complementarse e interpretarse la criminalística, investigación penal, litigio penal y derecho probatorio con las normativas ISO/IEC 27037:2012, ISO/IEC 27042 , siendo la primera un protocolo internacional para identificar, recolectar, adquirir y preservar la evidencia digital y la segunda un protocolo para analizar e interpretar la evidencia digital y por ende lo contenido en el Decreto 47-2008 Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, integrado también, a la Constitución Política de la República Guatemala y Convenios y Protocolos internacionales en materia de derecho informático como por ejemplo con el Convenio de Budapest, mismo del que Guatemala no es parte.

VI) Con relación a las ilegalidades practicadas por los usuarios del sistema de justicia penal sobre el procedimiento pericial informático que consiste en identificar, preservar, analizar y presentar la prueba electrónica y digital en el proceso penal, se evidenció que al no existir procedimientos prestablecidos, regulación legal propician las practicas arbitrarias que atentan con la integridad de la evidencia electrónica y digital y que riñe con los principios del derecho probatorio entre ellos el de legalidad, legitimidad e integridad, desde el momento de su obtención en el escenario criminal hasta su diligenciamiento y ofrecimiento ante el juez sentenciador y critico resulta que al momento de dar un valor probatorio se duda sobre la seguridad y certeza jurídica de los fallos judiciales por carecer de fundamentos técnicos y lógicos-jurídicos.

VII) Con todo lo anterior afirmo que no existe seguridad jurídica y legalidad en los procedimientos utilizados para el diligenciamiento, ofrecimiento y valoración de la prueba electrónica y digital en casos de delincuencia organizada, no obstante que se encuentra en discusión la Ley de Prevención y Protección contra la Ciberdelincuencia y que a la fecha se ha presentado al Pleno del Congreso de la República como iniciativa de ley 5601, la cual dentro de su contenido también refiere el procedimiento correcto para el manejo de evidencia electrónica y digital que posteriormente podría utilizarse como prueba, es menester subrayar que actualmente se encuentran una ley afín que dan una pauta de cómo debe manejarse lo concerniente a este tipo de pruebas tal y como lo es la Ley para el Reconocimiento de Comunicaciones y Firma Electrónica (Decreto 47-2008), sin embargo existen vacíos legales para la identificación, recopilación, recuperación, reproducción, análisis, preservación y presentación de la prueba electrónica y digital en virtud que no se encuentra una normativa legal vigente que provea los lineamientos concretos al respecto, no obstante que en diferentes órganos jurisdiccionales a diario se diligencian pruebas de este tipo y la forma en que es utilizada, incorporada y valorada es incorrecta en virtud que se violentan los protocolos internacionales en materia de evidencia digital y electrónica, de esa misma cuenta los órganos contralores y tribunales de sentencia emiten sus fallos sin tener claro lo que aporta el contenido de la prueba digital y electrónica y ello se ve reflejado en la escasa fundamentación con respecto a este tipo de pruebas encajonándolas dentro del tipo de prueba tradicional.

10.9. Sugerencias.

1. Es necesario que dentro de la profesión de Abogado y Notario en Guatemala se implemente un mecanismo de actualización sobre Derecho Informático e Informática Forense tomando en consideración que nuestra profesión es dinámica y que no queda al margen de los cambios generalizados que se presentan en la esta sociedad postindustrial.

2. Deben de existir un cambio de paradigmas sobre las nuevas tendencias tecnológicas y que inciden en el ámbito forense, nuestro país lleva aproximadamente diez años de atraso en estos temas y se debe fomentar la academia para mejorar nuestro desempeño profesional.

3. El Ministerio Público debe efectuar una revisión de sus protocolos de actuación y así evitar las malas prácticas en la fase de obtención, recolección, preservación, análisis y presentación de la prueba electrónica y digital.

4. El Organismo Judicial debe propiciar la formación de los Jueces en las áreas de Derecho Informático e Informática Forense y evitar las malas prácticas al momento de emitir sus resoluciones.

5. En la Dirección de Postgrados de la Universidad de San Carlos de Guatemala se debe realizar una actualización de Derecho Informático y de las Nuevas Tecnologías de la Información encaminados a abordar temas como el derecho procesal tecnológico o digital, Big Data, Blockchain, inteligencia artificial e internet de las cosas aplicadas a investigaciones criminales, entre otros temas, que pueden fortalecer capacidades y mejorar la formación de profesionales y así propiciar la el sustento técnico y legal del abogado 3.0

C. BIBLIOGRAFÍA.

1. (28 de marzo de 2017). Obtenido de http://scm.oas.org/Pdfs/2017/CP37680T.pptx

2. Acán Guerrero, S. (2015). *El Crimen Organizado.* Guatemala: Impresos El Aguila.

3. ACCION DE EXTINCION DE DOMINIO-, Sentencia C-958/14 (Corte Constitucional 2014).

4. Acurio del Pino, S. (s.f.). *Delitos Informáticos: Generalidades.* Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

5. Acurio del Pino, S. (s.f.). *Manual de Manejo de Evidencias Digitales y Entornos Informátios. Version 2.0.* Obtenido de https://www.oas.org/juridico/english/cyb_pan_manual.pdf

6. Almeida Romo, O. (2011). *Metodologia Forense_Repositorio utn.* Obtenido de resumen técnico - Repositorio UTN: http://repositorio.utn.edu.ec/bitstream/123456789/539/21/04%20ISC%20157%20RESUMEN%20TECNICO%20ESPA%C3%91OL.pdf

7. Amoroso, Y. (2000). *Alfa-Redi revista de Derecho Informático.* Obtenido de https://www.google.com.gt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjj9YP0k-feAhXyw1kKHbVSDEYQFjAAegQIAhAB&url=http%3A%2F%2Fwww.alfa-redi.org%2Frdi-resultado.shtml%3FAA_SL_Session%3D0ec69364cfcf5658955c301e799bc259%26scrl%3D1%26sc

8. Anguas, J. (s.f.). *Anguas.* Obtenido de La prueba en informatica: Evolución, estado actual y propuesta de formalización.: https://www.anguas.com/e1m6/Docs/UNIJES_Estado_de_la_prueba_en_informatica.pdf

9. Anónimo. (s.f.). *tesis.uson.mx.* Obtenido de http://tesis.uson.mx/digital/tesis/docs/21251/Capitulo3.pdf

10. Arbulora Valverde, A. (2000). *La Cadena de Custodia.* Costa Rica: Marphasa.

11. Armilla, N., Panizzi, M., Eterovic, J., & Torres, L. (2017). sedici.unlp.edu.ar. *Buenas Practicas para la recolección de la evidencia digital en la Argentina*, (págs. 1249-1258). La Plata, Argentina. Obtenido de Buenas prácticas para la recolección de la evidencia digital en la Argentina: http://sedici.unlp.edu.ar/bitstream/handle/10915/63930/Documento_completo.pdf?sequence=1

12. Ashcroft, John. (July de 2001). *www.ncjrs.gov.* Obtenido de Electronic Crime Scene Investigation: https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

13. Ayelén Scherma, L. (s.f.). *Comisión de Jovenes Procesalistas. Asociación argentina de Derecho Procesal* . Obtenido de https://cjprocesalistas.com.ar/publicaciones/122-%E2%80%9Cla-valoraci%C3%B3n-de-la-prueba-y-la-importancia-del-testigo-t%C3%A9cnico%E2%80%9D

14. Badilla, J. (1999). *Procesamiento de la escena del crimen.* San Jose Costa Rica: Escuela Judicial.

15. Baudino, F., & Torres, G. N. (2016). *La reconstrucción Virtual. Su incorporación legal en el proceso penal*. Obtenido de https://www.criminalisticaycriminologia.com/la-reconstruccion-virtual-su-incorporacion-legal-en-el-proceso-penal/

16. Bechimol, D. (2011). En *Hacking desde cero* (pág. 39). Buenos Aires, Argentina: RerUSERS.

17. Blanco, B. (s/f). El crimen organizado y las nuevas tecnologías. *El Fisco*.

18. Borges, R. (2018). La prueba electronica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea. *Rev. Boliv de Derecho No. 25*, 536-549.

19. Burguete Stanek, L. (s.f.). *Situación actual del derecho informático. Firma Electrónica, Certificación Digital y Comercio Electrónico.* Obtenido de http://ordenjuridico.gob.mx/Congreso/pdf/144.pdf

20. Canedo Estrada, A. (2010). La informática forense y los delitos informáticos. *Revista Pensamiento Americano*, 81-88.

21. Cano, E. S. (Marzo de 2017). *Derecho Informático*. Obtenido de http://jessenializ2403.blogspot.com/2017/03/informatica-juridica-e-informatica.html

22. Cano, J. (2009). *Computación Forense. Descubriendo los rastros informáticos.*

23. Cano, J. J. (2010). Obtenido de El Peritaje informático y la evidencia digital en Colombia: https://repository.upb.edu.co/bitstream/handle/20.500.11912/1834/digital_22203.pdf?sequence=1&isAllowed=y

24. Cantú, S. (2013). El Regimen penal de excepción para delincuencia organizada bajo el test de los derechos humanos. *Investigaciones Juridicas de la UNAM*, 1739-1765. Obtenido de https://archivos.juridicas.unam.mx/www/bjv/libros/8/3568/21.pdf

25. Carrascosa, V. (1998). *La Regulación Jurídica del fenómeno informático.* Recuperado el Febrero de 2019, de https://dialnet.unirioja.es/servlet/autor?codigo=274150

26. Casado, L. (2008). Evidencia. En *Diccionario de Derecho* (pág. 165). Ediciones Valleta.

27. Castillo González, J. M. (2016-2017). *Constitución Política de la República de Guatemala, Comentada.* Guatemala.

28. Castillo Viquez, F., Rodriguez Loaiza, O., & Arguedas Rodriguez, G. (s.f.). *Convención Americana sobre Derechos Humanos, Anotada y conrcordadacon la Jurisprudencia de la Corte Interamericana de Derecho Humanos.* Obtenido de http://www.corteidh.or.cr/tablas/r31024.pdf

29. Chirinos, I. (2017). *Evolución Historica del Derecho Informático*. Obtenido de https://elderechoymisapuntes.blogspot.com/2017/12/evolucion-historica-del-derecho.html

30. Ciberdelincuencia, C. s. (s.f.). Recuperado el 2019, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

31. Clarin, D. E. (21 de Enero de 2013).

32. Comisión de Asuntos de Seguridad Nacional del Cong. (Noviembre de 2019). *Iniciativa 5601 -Ley de Prevención y Protección contra la Ciberdelincuencia-.*

33. Comisión Presidencial, C. d. (Abril de 2014). Resolución 58/167. "El Derecho a la Privacidad en la era Digital". Guatemala.

34. Corcoy Bidasolo, M. (Diciembre de 2007). *Problemática de la Persecución Penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ambito espacio temporal de la comisión de hechos.* Obtenido de https://www.ehu.eus/documents/1736829/2176629/Eguzkilore+21.pdf

35. Corrales, M. (2015). *repository.uniminuto.edu.* Obtenido de Diseño de la metodología para el manejo de incidentes TI mediante forénsica digital: https://repository.uniminuto.edu/bitstream/handle/10656/3659/TEPRO_Corrales Margarita_2015.pdf?sequence=1&isAllowed=y

36. Cortes Coto, R. (s.f.). *Poder Judicial. Costa Rica. La Valoración de la Prueba en Crimen Organizado.* Obtenido de https://escuelajudicialpj.poder-judicial.go.cr/

37. Cossío, J. (2005). *Contradicción de Tesis: 154/2005 P-S.* Obtenido de http://207.249.17.176/Transparencia/Epocas/Primera%20sala/Novena%20%C3%A9poca/2005/20.pdf

38. Cuervo, J. (s.f.). *www.derecho.org.* Obtenido de Delitos Informáticos y Protección Penal a la Intimidad: www.derecho.org

39. Del Peso Navarro, E. (2001). *Peritajes Informáticos.* Obtenido de https://es.scribd.com/document/55774403/Peritajes-Informaticos

40. Delgado Martin, J. (s.f.). *Diario La Ley.* Obtenido de http://diariolaley.laley.es/home/DT0000245602/20170411/La-prueba-digital-Concepto-clases-y-aportacion-al-proceso

41. Delgado, J. (s.f.). *La prueba digital.* Obtenido de https://diariolaley.laley.es/home/DT0000245602/20170411/La-prueba-digital-Concepto-clases-y-aportacion-al-proceso

42. Delgado, M. (s.f.). *files.wordpress.* Obtenido de https://peritoit.files.wordpress.com/2013/10/la-prueba-eletronica-en-el-proceso-penal.pdf

43. Delgado, Miguel. (Junio de 2007). *www.oas.org.* Obtenido de Análisis Forense Digital: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

44. Denti, V. (s.f.). *revistas.juridicas.unam.mx.* Obtenido de Cientificidad de la prueba y libre valoración del juzgador: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/890/1150

45. Di lorio. et al., 2. (s.f.). *Info-lab. El Rastro Digital del Delito.* Obtenido de http://info-lab.org.ar/images/pdf/Libro.pdf

46. Diaz, M. (Junio de 2017). Retención de datos y Registro de Informacin de Móviles. Chile.

47. Escobar, L. (Mayo de 2017). Manejo de la cadena de custodia en la recolección de evidencia digital. Quetzaltenango.

48. Espanes, L., & Hiruela de Fernández, M. d. (s.f.). *Protección Juridica del Software.* Obtenido de http://www.acaderc.org.ar/doctrina/articulos/artsofware/at_download/file

49. Espinoza, J., & Verdezoto, R. (Abril de 2015). *dspace.ups.edu.ec.* Obtenido de El rol de la auditoria forense ante los nuevos delitos informaticos tipificados en el actual codigo orgánico integral penal del Ecuardo Coip, metodologicas y herramientas a usar ante una evidencia digital: https://dspace.ups.edu.ec/bitstream/123456789/10348/1/UPS-GT001274.pdf

50. *Evidencias electronicas*. (2020). Obtenido de http://www.csuc.cat/es/e-administracion/evidencias-electronicas/que-son-las-evidencias-electronicas.

51. Expediente 863-2011 (Corte de Constitucionalidad 21 de 06 de 2011).

52. Fallo prueba electrónica DVD, 404/2009 (Tribunal Supremo Sala de lo Penal 01 de Febrero de 2010).

53. Galvis Feria, J. (s.f.). *Abogado en la Web*. Obtenido de La Prueba Electrónica en Colombia: https://abogadoenlaweb.com/2018/08/la-prueba-electronica-en-colombia

54. García Dahinten, C. R. (Febrero de 2014). Cadena de Custodia Digital de las Evidencias para la realización de un peritaje. Guatemala.

55. Garcia Maynez, E. (2002). *zoonpolitikonmx.files.wordpress.com.* Obtenido de https://zoonpolitikonmx.files.wordpress.com/2014/08/introduccic3b3n-al-estudio-del-derecho-eduardo-garcc3ada-maynez.pdf

56. García, M. (s.f.). *Prueba Documental Electrónica.* Obtenido de http://181.189.159.2/2014/septiembre/prueba/contenido/ponencias/Maria%20Fernanda%20Garcia/Prueba%20documental%20electronica.pdf

57. García, Z. (s.f.). *iusfilosofiamundolatino.* Obtenido de La argumentación en la valoración de la prueba científica en el sistema penal acusatorio, emergente en elmundo latino: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwi0yJHI46bdAhWH-6QKHew4Ai4QFjAAegQIAxAC&url=http%3A%2F%2Fiusfilosofiamundolatino.ua.es%2Fdownload%2FVALORACIO%25CC%2581N%2520DE%2520LA%2520PRUEBA%2520CIENTI%25CC%2581

58. Garduza, I. G. (s.f.). *http://www.diccionariojuridico.mx/?pag=vertermino&id=1704.* Obtenido de http://www.diccionariojuridico.mx/?pag=vertermino&id=1704

59. GDPR Legal. (19 de enero de 2018). *Protección de Datos en el Panorama Internacional*. Obtenido de https://dpd.aec.es/la-proteccion-datos-panorama-internacional-una-primera-aproximacion/

60. *genbetadev*. (2020). Obtenido de https://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

61. Girón Higueros, F. (Agosto de 2009). El Nombramiento y Discernimiento del cargo de los Peritos. Guatemala: Tesis de Grado. Universidad de San Carlos de Guatemala.

62. Gómez Manrique, J. (2014). *Factores que inciden en la alteración de la evidencia digital*. Obtenido de http://informaticaforenseuccaraucacolombia.blogspot.com/2014/05/en

63. González Bedmar, M. C. (2015). *El Valor de la Prueba Electrónica en el Proceso Penal Español.* Tarragona.

64. González, M. (2015). *El valor de la prueba electronica en el proceso penal español.* Obtenido de http://nportal0.urv.cat:18080/fourrepo/rest/digitalobjects/DS?objectId=TFG:523&datastreamId=Mem%C3%B2ria&mime=application/pdf

65. Gonzalez-Cuellar, N. (2006). *Garantias Constitucionales en la persecución penal en el entorno digital.*

66. Gozaini, O. A. (2012). La Prueba Cientifica no es Prueba Pericial. *Revistas ICDP. Derecho de Sociedad*, 169-175.

67. Guatemala, C. d. (1993). *Decreto Número 17-93, Código Penal.* Guatemala.

68. Guatemala, C. d. (01 de Julio de 1994). *Decreto Número 51-92, Codigo Procesal Penal.* Guatemala.

69. Guatemala, C. d. (02 de Agosto de 2006). Decreto numero 21-2006 "Ley contra la Delincuencia Organizada".

70. Guatemala, C. d. (15 de Febrero de 2017). Proyecto de Ley contra la Ciberdelincuencia Guatemala. Guatemala.

71. Gustavo y Mejia Vargas, A. (s.f.). Reforma Procesal Penal: Sistema Acusatorio y Delincuencia Organizada. Mexico.

72. Guzman, C. (2000). En *Manual de Criminalística* (págs. 39, 40). Buenos Aires, Argentina: Ediciones de la Roca.

73. Hall, A. (s.f.). *Tipos de Delitos Informáticos*. Recuperado el 19 de Junio de 2019, de http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

74. Hernández, L. (Septiembre de 2008). *Importancia de la prueba en el proceso penal guatemalteco como medio idóneo de garantía contra la arbitrariedad de las decisiones judiciales en Guatemala.* Obtenido de http://biblioteca.usac.edu.gt/tesis/04/04_7536.pdf

75. Ibor, V., & Garcia, S. (s.f.). *Situación del derecho informática en España y en Europa: algunas consideraciones.* Obtenido de https://dialnet.unirioja.es/descarga/articulo/251099.pdf

76. Jurado, A. (211). Valor probatorio del documento electrónico. *Revista de Ciencias Juridicas de la Universidad Rafael Urdaneta*, 51-68.

77. Killalea, B. &. (s.f.). Obtenido de Guidelines for Evidence Collection and Archiving: “http://www.ietf.org/rfc/rfc3227.txt”

78. Leal Medina, J. (2011). *Técnicas Policiales y Judiciales en la Investigación Criminal.* Obtenido de https://dialnet.unirioja.es/descarga/articulo/3763113.pdf

79. Lepe, A. (Diciembre de 2007). *Valor Probatorio de los Documentos Electrónicos.* Obtenido de http://biblioteca.usac.edu.gt/tesis/04/04_1754.pdf

80. Libano Manzur, C. (s.f.). *Delitos informáticos.* Recuperado el Junio de 2019, de http://www2.udec.cl/contraloria/docs/materias/delitosinformaticos.pdf

81. López Manrique, Y. V. (2007). En *Computacion Forense* (pág. 31). Guatemala.

82. Martin, R. (s.f.). *Deontologia y Legislación Informática. .* Obtenido de https://previa.uclm.es/profesorado/raulmmartin/Legislacion/apuntes.pdf

83. Martinez, E. (2012). *Apuntes de Derecho Informático.* Guatemala: Mayte.

84. Martinez-Villalba, J. (2004). *La Prueba Electrónica.* Obtenido de http://www.worldcat.org/title/prueba-electronica/oclc/880998589

85. Ministerio de Gobernación. (2018). *Estrategia Nacional de Seguridad Cibernética.* Guatemala.

86. Ministerio Público. (octubre de 2006). Instrucción General para la aplicación del manual de procedimientos para el procesamiento de escenas del crimen. Guatemala.

87. Ministerio Público de Venezuela. (2012). *Manual Unico de Procedimientos en Materia de Cadena de Custodia de Evidencias Fisicas.* Obtenido de http://www.oas.org/juridico/pdfs/mesicic4_ven_man_cad_cust.pdf

88. Mojica, G. (2009). *RELACION CON EL DERECHO CONSTITUCIONAL (HABEAS DATA)*. Obtenido de http://informaticajuridicausco.blogspot.com/2009/06/relacion-con-el-derecho-constitucional.html

89. Molina, G.-P. (s.f.). *Los Delitos Informáticos de Nueva Generación.* Recuperado el Junio de 2019, de https://glifos.umg.edu.gt/digital/90616.pdf

90. Monsálvez, C. R. (2015). *Derecho Informático.* Obtenido de Manual Chileno de Derecho Informático: https://www.google.com.gt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiewdLozvbfAhWwtVkKHUvHAHkQFjABegQIBxAF&url=http%3A%2F%2Fwww.reusser.cl%2Fwp-content%2Fuploads%2F2015%2F05%2Fmanualderechoinformatico-v05.pdf&usg=AOvVaw3109ONF9S_KR-0ITnmGBxC

91. Montaño, J. (24 de 03 de 2017). *Derecho Informático*. Obtenido de http://blogdederech.blogspot.com/

92. Montoya Rojas, A. (s.f.). *La informática forense como herramienta para la aplicación de la prueba electrónica.* Obtenido de https://dialnet.unirioja.es/descarga/articulo/4863623.pd

93. Mora Izquierdo, R., & Sánchez Prada, M. (2007). *La evidencia fisica y la cadena de custodia dentro del procedimiento penal acusatorio.*

94. Morales Sánchez, F. (s.f.). *Validez de la Prueba Electrónica. Un estudio sobre la firma digital y electrónica.* Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/13779/4/VALIDEZ%20DE%20LA%20PRUEBA%20ELECTRONICA.pdf

95. Morales, S. (s.f.). *Procuraduria de los Derechos Humanos.* Obtenido de http://www.fao.org/tempref/upload/eims_object/Photo_library/Guatemala_Informe_Resumen_Ejecutivo.pdf

96. Naciones Unidas. (2000). *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.* Palermo.

97. Navarro Clérigues, J. (2015-2016). *Guia actualizada para futuros peritos informáticos. Ultimas herramientasde análisis forense digital. Caso práctico.* Obtenido de http://www.pensamientopenal.com.ar/system/files/2016/05/doctrina43429.pdf

98. Navas, A. (s.f.). *La Prueba Electrónica en Material Penal.* Obtenido de https://www.anahuac.mx/mexico/files/investigacion/2011/sep-oct/73p.pdf

99. Oliva. et al., 2. (s.f.). *Ecija. La Prueba Electrónica, Validez y Eficacia Procesal.* Obtenido de https://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf

100. Organización de Estados Americanos. (s.f.). Obtenido de Estándares para una Internet libre, abierta e incluyente: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf

101. Ortiz Pradillo, J. C. (2013). *La investigación del delito en la era digital.* Obtenido de http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf

102. Ostale García, J. (s.f.). *www.researchgate.net.* Obtenido de https://www.researchgate.net/publication/49112577_Notas_para_el_concepto_de_informacion_semantica

103. Paz, G. (s.f.). *Publicaciones Cientificas.* Obtenido de La era de la tecnologia y los nuevos medios probatorios. El correo electrónico y su valor probatorio: publicacionescientificas.uces.edu.ar/index.php/ratioiurisB/article/view/50/53

104. Peñaranda, H. (s.f.). *La informática jurídica: mecanismo de gestión de la información jurídica.* Obtenido de http://www.cibersociedad.net/congreso/comms/c13penaranda2.htm

105. Pérez Luño, A. E., Soriano Diaz, R. L., & Gómez Torres, C. (s.f.). *Diccionario Jurídico . Filosofía y Teoría del Derecho e Informática jurídica.* Obtenido de http://www.tirant.com/derecho/libro/diccionario-juridico--filosofia-y-teoria-del-derecho-e-informatica-juridica-antonio-enrique-perez-luno-9788484447665

106. Pérez, J. E. (03 de julio de 2014). *openaccess.uoc.edu.* Obtenido de La Prueba Electrónica: Consideraciones: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf

107. Piña Libien, H. (s.f.). *El Derecho informático y su autonomía como nueva rama del derecho.* Obtenido de http://www.ordenjuridico.gob.mx/Congreso/pdf/78.pdf

108. Quiles, L. (2015-2016). Las nuevas tecnologías como medio de prueba en el proceso penal. *Trabajo de fin de grado*.

109. Ramos, B. (2007-2008). Regulación, Admisibilidad y Valoración de la Prueba Pericial Penal en el Derecho Nacional. *Proyecto de Actividad Formativa Equivalente a Tesis Magister en Derecho, Mención en Derecho Penal*. Chile.

110. Riego, C., & Binder, A. M. (9). El rol de las nuevas tecnologías en el sistema de justicia. *Sistemas Judiciales*.

111. Rivera Clavería, J. (enero de 2011). *El Crimen Organizado.* Obtenido de https://www.galileo.edu/ies/files/2011/04/EL_CRIMEN_ORGANIZADO-IES.pdf

112. Rivolta, M. (2007). *Medios de prueba electrónicos: estado de avance en la legislación argentina.* Obtenido de http://www.saij.gob.ar/doctrina/dacc070049-rivolta-medios_prueba_electronicos_estado.htm

113. Rivolta, M. (2007). *Saij*. Obtenido de Medios de prueba electrónicos: estado de avande en la legislación argentina: http://www.saij.gob.ar/doctrina/dacc070049-rivolta-medios_prueba_electronicos_estado.htm

114. Roatta, S., Casco, M., & Fogliato, M. (s.f.). *El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012.* Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/50586/Documento_completo.pdf-PDFA.pdf?sequence=1

115. Robledo, M. (2015). La aportación de la prueba pericial cientifica en el proceso penal. *Gaceta Int. ciencia forense*, 5-12.

116. Rodriguez, F. (Febrero de 2013). Legislación y Etica Profesional. 133. Argentina.

117. Rodriguez, F. (s.f.). *Lecciones de Derecho y Etica Profesional.* Obtenido de http://www.feliperodriguez.com.ar/wp-content/uploads/2013/11/LIBRO-7-DERECHO-INFORMATICO.pdf

118. Rodriguez, F. (s.f.). *Legislación y Etica Profesional.* Obtenido de http://www.feliperodriguez.com.ar/wp-content/uploads/2013/11/LIBRO-7-DERECHO-INFORMATICO.pdf

119. Romina, M. (s.f.). *FUENTES DEL DERECHO INFORMATICO*. Recuperado el 13 de Febrero de 2019, de http://romina-mayra.blogspot.com/2009/12/fuentes-del-derecho-informatico.html

120. Ronderos, J. (Noviembre de 2015). *La Prueba Digital en el contexto juridico actual.* Obtenido de https://www.deceval.com.co/portal/page/portal/Home/Marco_Legal/Eventos/Presentacion_Deceval_JGRFINAL.pdf

121. Ronderos, J. (11 de Noviembre de 2015). La Prueba Digital en el Contexto Juridico Actual. Colombia.

122. Rubio, J. (5 de Noviembre de 2016). *peritoinformaticocolegiado.es*. Obtenido de Estandares nacionales e internacionales que puede seguir un perito informático para realizar análisis forense de una evidencia y para la elaboración de un peritaje informático: https://peritoinformaticocolegiado.es/blog/estandares-nacionales-e-internacionales-que-puede-seguir-un-perito-informatico-para-realizar-el-analisis-forense-de-una-evidencia-y-para-la-elaboracion-de-un-peritaje-informatico/

123. Ruiz Alquijay, J. (2012). En *La utilización de la informática forense en los casos de alto impacto social en Guatemala* (pág. 57). Guatemala.

124. Ruyer, R. (1992). *La cibernética y el origen de la información.* Obtenido de https://www.google.com.gt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjB3pO1peLeAhXExVkKHSqIDsEQFjAAegQIChAC&url=https%3A%2F%2Fwww.u-cursos.cl%2Fderecho%2F2005%2F1%2FD124D0795%2F3%2Fmaterial_docente%2Fbajar%3Fid_material%3D60230&usg=AOvVaw1crRUnHA

125. Salas, E., Ramírez, A., & Núñez, O. (s.f.). *www.alfa-redi.org.* Obtenido de Propuesta de Protocolo para la Recolección de Evidencias Digitales relacionado con la Legislación Peruana: http://www.alfa-redi.org/sites/default/files/articles/files/salas.pdf

126. Salom Clotet, J. (2011). *Dialnet-El Ciberespacio y el Crimen Organizado.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=3837304

127. Sánchez Hérnadez, J. (Diciembre de 2016). *Estudio de la Prueba Electrónica en el Proceso Penal. .* Obtenido de

https://gredos.usal.es/bitstream/handle/10366/132621/TFM_SanchezHernandez_Estudio.pdf.txt;jsessionid=FAF3B93C6BB923D97DDBF09015D8F959?sequence=8

128. Sánchez, A. (15 de septiembre de 2016). *Tesis Doctora: Ciencia y proceso penal. Un estudio sobre el concepto y regimen jurídido de la llamada <<prueba cientifica>>.* Obtenido de https://www.google.com.gt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiDqr_zu5HdAhVHtlkKHW1mCGIQFjAAegQIAxAC&url=https%3A%2F%2Frio.upo.es%2Fxmlui%2Fbitstream%2Fhandle%2F10433%2F3719%2Fsanchez-rubio-tesis16.pdf%3Fsequence%3D1%26isAllowed%3Dy&usg=AO

129. Sánchez, J. (2015-2017). *Pensamiento Penal.* Obtenido de http://www.pensamientopenal.com.ar/doctrina/45051-estudio-prueba-electronica-proceso-penal-especial-referencia-conversaciones-whatsapp

130. Sanso-Rubert, D. (2016). Nuevas tendencias de organización criminal y movilidad geográfica. Aproximación geopolítica en clave de inteligencia criminal. *UNISCI / UNISCI Journal*.

131. Santos, J. (Septiembre de 2013). *Procedimientos en la Investigación, recolección y manejo de la evidencia digital en la escena del crimen.* Obtenido de http://biblio3.url.edu.gt/Tesario/2013/07/03/Santos-Jorge.pdf

132. Saquimux, E. (2010). *Hagamos una Tesis .* Quetzaltenango.

133. Sebastián Gómez, L. (Enero de 2006). *https://www.researchgate.net/.* Obtenido de https://www.researchgate.net/publication/28111576_Argentina_Guia_Operativa_para_Procedimientos_Judiciales_con_secuestro_de_tecnologia_Informatica/link/56e1f02b08aebc9edb19ccf7/download

134. Sebastián Gómez, L. (Marzo de 2018). *Evidencia Digital en la Investigación Penal.* Obtenido de https://www.researchgate.net/publication/323613054_Evidencia_digital_en_la_investigacion_penal

135. Solórzano, E. R. (2012). *Apuntes de Derecho Informático.* Guatemala: Ediciones Mayté.

136. Soto Caldera, M. (s.f.). *La tipicación de los delitos informáticos en la legislación penal venezolana.* Recuperado el 12 de junio de 2019, de http://www.corteidh.or.cr/tablas/R06731-5.pdf

137. Suñe, E. (2000). *DERECHO INFORMÁTICO AL DERECHO DEL CIBERESPACIO Y A LA CONSTITUCIÓN DEL CIBERESPACIO.* Obtenido de https://www.google.com.gt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiE3b-h4uTeAhXS2FMKHVU5C04QFjAAegQIBxAC&url=https%3A%2F%2Fwww.uexternado.edu.co%2Fwp-content%2Fuploads%2F2017%2F01%2FEl-derecho-informatico-De-donde-viene-y-hacia-donde-va.doc&us

138. Tato, N. (2015). *Informática Jurídica.* Obtenido de http://www.nicolastato.com.ar/esp/docs/UNIDAD%20I.pdf

139. Téllez, J. (2008). *Derecho Informático.* México D.F.: McGraw-Hill.

140. Torres, O. G. (13 de 07 de 2016). *El Nacional*. Recuperado el 19 de 09 de 2016, de El Nacional: http://elnacional.com.do/extincion-de-dominio/

141. *Tuabogadodefensor*. (s.f.). Recuperado el Junio de 2019, de https://www.tuabogadodefensor.com/contratos-informaticos/#

142. *UNE Normalización Española*. (2020). Obtenido de https://www.une.org/

143. Universidad del Rosario. (s.f.). *www.urosario.edu.co.* Recuperado el 19 de Septiembre de 2016, de www.urosario.edu.co: http://www.urosario.edu.co/observatorio-de-lavado-de-activos/extincion-de-dominio/

144. Vazquez-Rojas, C. (2014). Anuario de Psicología Juridica 2014. *Sobre la cientificidad de la prueba científica en el proceso judicial.* Girona, España.

145. Velasco Melo, A. (2008). El Derecho Informático y la Gestión de la seguridad de la información. *Revista de Derecho.*

146. Velasco, E. (s.f.). *Crimen Organizado, Internet y Nuevas Tecnologías. .* Obtenido de https://ruc.udc.es/dspace/bitstream/handle/2183/9173/ponencias_13_Velasco_Nunez_245-282.pdf?sequence=1&isAllowed=y

147. Verbic, F. (s.f.). *biblioteca.asesoria.gba.gov.ar.* Obtenido de La prueba cientifica en el proceso judicial: http://biblioteca.asesoria.gba.gov.ar/redirect.php?id=4700

148. Vicente Martínez, A. (2016). Obtenido de La prueba digital en la automatización de los procesos jurisdiccionales.: https://archivos.juridicas.unam.mx/www/bjv/libros/9/4250/30.pdf

149. Vides Alvarez, R. (2011). Evidencia Digital. Colombia.

150. Viega, M. J. (s.f.). *Cade.* Obtenido de Formalidades de presentación de la prueba electrónica: http://www.cade.com.uy/formalidades-presentacion-prueba-electronica/

151. Villanueva, E. (2006). *Derecho de Información.* Obtenido de http://biblioteca.diputados.gob.mx/janium/bv/ce/scpd/LIX/der_inf.pdf

152. Wikipedia. (s.f.). *Wikipedia La Enciclopedia Libre*. Recuperado el 2019 de 05 de 23, de https://es.wikipedia.org/wiki/Ley_Org%C3%A1nica_de_Protecci%C3%B3n_de_Datos_de_Car%C3%A1cter_Personal_(Espa%C3%B1a)

153. Williams, Janet. (Marzo de 2012). *Digital-detective.* Obtenido de ACPO Good Practice Guide for Digital Evidence: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

154. Xol Choc, H. B. (2017). *La reconstrucción virtual de la escena del crimen como elemento de prueba.* Guatemala.

155. Zuccardi, G., & Gutierrez, J. D. (Noviembre de 2006). *Informática Forense.* Obtenido de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

D. GLOSARIO.[18]

En virtud que son amplios los conceptos que se conocen y tratan en la informática forense y que tiene relación con ciberseguridad se adjunta el acceso a un sitio web en donde se puede visualizar y descargar el archivo que contiene cada uno de esto conceptos.

[18] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf