UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE
DEPARTAMENTO DE CIENCIAS JURÍDICAS

TRABAJO DE GRADO

PROBLEMAS PROBATORIOS DE LA PERICIA INFORMÁTICA EN EL DERECHO PENAL SALVADOREÑO

PARA OPTAR AL GRADO DE

LICENCIADO (A) EN CIENCIAS JURÍDICAS

PRESENTADO POR

CARLOS JOSUÉ AGUILAR BETETA

MANUEL ANTONIO CANTARERO PINTÍN

PAUL ALEXANDER MARCICANO RAMOS

JOSSELYN ASTRID MORÁN RODRÍGUEZ

JENIFER CAROLINA VILLEDA ARÉVALO

DOCENTE ASESOR

LICENCIADO RAYMUNDO ALIRIO CARBALLO MEJÍA

OCTUBRE, 2019

SANTA ANA, EL SALVADOR, CENTROAMÉRICA.

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES

M.Sc. ROGER ARMANDO ARIAS ALVARADO

RECTOR

DR. MANUEL DE JESÚS JOYA ÁBREGO

VICERRECTOR ACADÉMICO

ING. NELSON BERNABÉ GRANADOS ALVARADO

VICERRECTOR ADMINISTRATIVO

LICDO. CRISTÓBAL HERNÁN RÍOS BENÍTEZ

SECRETARIO GENERAL

M.Sc. CLAUDIA MARÍA MELGAR DE ZAMBRANA

DEFENSORA DE LOS DERECHOS UNIVERSITARIOS

LICDO. RAFAEL HUMBERTO PEÑA MARÍN

FISCAL GENERAL

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

AUTORIDADES

DR. RAÚL ERNESTO AZCÚNAGA LÓPEZ

DECANO

M.Ed. ROBERTO CARLOS SIGÜENZA CAMPOS

VICEDECANO

M.Sc. DAVID ALFONSO MATA ALDANA

SECRETARIO

M.Ed. MIRNA ELIZABETH CHIGÜILA DE MACAL ZOMETA

JEFA DEL DEPARTAMENTO DE CIENCIAS JURÍDICAS

Índice.

Índice de cuadros

Introducción.

El desarrollo acelerado de las nuevas tecnologías ha generado cambios drásticos en las sociedades y El Salvador no se ha quedado al margen, al igual que el resto de países Latinoamericanos se ha visto en la necesidad de actualizarse y ponerse al día con las tecnologías que se están utilizando en la actualidad. Estamos en presencia de una nueva era denominada "Era de la Informática", en la cual la humanidad está en un constante contacto con las tecnologías de la información y comunicación (TICS).

Es por ello que el presente trabajo de grado versa sobre una temática meramente informática, y se ha organizado en cinco capítulos los cuales han desarrollado distintas fases y fueron encaminados de la siguiente manera:

El Capítulo I, presenta un esbozo sobre los orígenes del internet en El Salvador, asimismo se abordan las tecnologías de la información y comunicación, y se visualizan desde una perspectiva donde estas pueden ser utilizadas por personas inescrupulosas como herramientas para cometer delitos informáticos.

En vista que la temática abordada trata sobre ciberdelitos, cuya legislación sustantiva es relativamente nueva, debido a que la Ley Especial Contra los Delitos Informáticos y Conexos, fue creada el 4 de febrero de 2016, en consecuencia, surgió la necesidad que los sujetos procesales se actualizarán no solo en el área informática, sino que también en los procedimientos aplicables a la pericia informática, como eje central de los procesos informáticos.

En el Capítulo II, se abordó la pericia informática desde un punto de vista doctrinario y teórico, para conocer su esencia y establecer que piensan los estudiosos del derecho sobre la pericia informática y su función en los procesos informáticos, desde este panorama se discutió

su aplicación práctica y se definió su marco normativo, donde se tomó en cuenta la legislación nacional e internacional, sin dejar de lado los distintos tratados suscritos y ratificados por el Estado, asimismo se abordó el Protocolo de Investigación y Análisis de la Pericia Informática, donde se definen los pasos y procedimientos a seguir para tratar la evidencia digital cuando se desarrolle un proceso informático.

Debido a que la legislación sustantiva suprarelacionada, no establece dentro de su articulado como probar los delitos que ella regula, tampoco determina como ofertar y presentar las pruebas que se pretendan hacer valer en el proceso. Esto generó la necesidad de buscar internacionalmente un proceso o protocolo que dictaminara la forma de proceder en los delitos informáticos.

El Capítulo III, corresponde a la parte metodológica de la investigación y se inició tomando en cuenta que los delitos informáticos tienen a los mismos sujetos procesales como autores principales de un proceso penal, esto implicó la necesidad de conocer el dominio que tienen estos sobre la pericia informática, sus formas de valoración y como puede esta incidir para resolver un proceso informático.

Por ende, para dar respuesta a estas y otras todas interrogantes se programaron en el diseño metodológico entrevistar a aquellas personas directamente relacionadas con los procesos penales y fue así como se tomó en cuenta a jueces, fiscales, peritos informáticos y abogados particulares y públicos; así también se definieron las herramientas y técnicas que se utilizarían para la recolección y el posterior análisis de la información.

El Capítulo IV, contiene toda la información recabada de los informantes clave, la cual fue vaciada en las matrices correspondientes, del mismo modo contiene las matrices de análisis donde se detalló puntualmente las respuestas de las unidades de análisis y se formuló el análisis de la información.

El Capítulo V, presenta la culminación de este proceso investigativo, en vista que en los párrafos precedentes se determinan las etapas agotadas el proceso de grado, las cuales dieron origen a la etapa final donde se establecieron las conclusiones alcanzadas, las cuales tomaron como base la información obtenida en el desarrollo de la investigación y las respuestas de las unidades de análisis, esto permitió también formular las recomendaciones, las cuales fueron encaminadas para mejorar las falencias, para regular los vacíos y corregir los problemas encontrados en la pericia informática en la presente investigación.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Situación problemática.

El derecho penal al igual que el resto del sistema normativo jurídico, tiene por objeto regular el comportamiento de las personas, en un contexto social determinado, siendo su campo específico regulatorio las conductas humanas que constituyen delitos o faltas penales.

Esto significa, que el derecho penal puede volverse anacrónico en la medida que los constantes cambios sociales no sean seguidos por una constante actualización de la normativa jurídico penal, por parte del Órgano Legisferante, lo cual traería como consecuencia una inadecuada administración de justicia penal.

En este orden de ideas, si el carácter teleológico del sistema punitivo sigue siendo una de sus principales garantías penales, resulta entonces que para proteger los bienes jurídicos hay que tomar en cuenta los constantes cambios que se encuentran alrededor del bien jurídico tutelado.

Actualmente la sociedad se encuentra en la era de la informática, día a día se crean aparatos electrónicos más sofisticados que satisfacen las necesidades de diferentes ámbitos de la comunidad, como son los celulares inteligentes con acceso a internet, que permiten realizar llamadas de voz o video, a personas que se encuentren a distancias considerablemente enormes.

> Sectores como la banca, los seguros, los transportes, la educación, la bolsa, el tráfico aéreo y terrestre, las administraciones públicas, es decir, la sociedad en su conjunto, dependen, en gran medida, de las computadoras. A ellas se les encomienda no sólo el archivo y procesamiento de la información, sino, incluso, la adopción automática de decisiones. Oficina de las Naciones Unidas contra la Droga y el Delito (UNDOC, 2018p. 11)

Por lo que las TICS (Tecnologías de la Información y Comunicación), se han convertido en herramientas de trabajo del siglo XXI.

Pensando en esa dinámica social, Tünnermann (2003) expresa que:

> La humanidad ha entrado en un proceso acelerado de cambios, en el orden social, científico y cultural, por lo que el siglo XXl es una nueva era a la que se le puede denominar (Learning Society) o sociedad del conocimiento o sociedad de la

información, por el papel central que juega en el proceso productivo las nuevas tecnologías. (p. 90).

De hecho, dice, esta nueva era se caracteriza por una desmaterialización del proceso productivo. Afirma, que el siglo XX, fue la era basada en la producción de bienes básicos, la cual se ha derrumbado. Hoy se está en presencia de una economía del saber, donde las industrias más dinámicas son las llamadas industrias de la inteligencia, entre las que se destaca la informática, la biotecnología, la robótica, la ingeniería aeroespacial entre otras, todo lo cual sucede en un mundo globalizado.

Los países latinoamericanos entre ellos El Salvador no pueden quedarse atrás, al margen del proceso de globalización dominado por la intensidad del conocimiento, y por el desarrollo acelerado de las nuevas tecnologías. En el año 1994 se empieza a gestionar el uso del internet en el país, siendo en el año 1995 cuando por primera vez se logra el acceso a la red de redes.

Sin embargo, al insertarse en este nuevo orden, se notan claramente las asimetrías y desigualdades entre los países latinoamericanos y los grandes bloques de poder. Para el caso la desigualdad digital arranca del hecho de que la mayor parte de la población latina no tiene acceso a internet, que es la fuente del conocimiento y de la información. Un informe de la CEPAL indica que El Salvador es el segundo país con menos acceso a internet en Centro América, solo después de Nicaragua. Comisión Económica para America Latina y el Caribe.(2016). Estado de la banda ancha en América Latina y el Caribe

A pesar del sombrío panorama descrito en la última década, las Tecnologías de la Información y Comunicación (TIC) han permeado toda la esfera de la vida social salvadoreña, por lo que también El Salvador, con ciertas limitaciones se ha insertado en la denominada Sociedad de la Información o del Conocimiento.

En el año 2011 se realizó la primera feria TIC como una oportunidad para que los salvadoreños pudieran conocer sobre el uso de las nuevas tecnologías de la información y comunicación y tener acceso a ellas, llegando al punto que en la actualidad se puede ver el uso de estas tecnologías cuando se realiza transacciones bancarias, en el uso de cajero automático, el uso de teléfonos inteligentes, cámaras digitales, sensores de lectura óptica de códigos de barra, y una variada utilización de tecnología digital.

Se puede observar en el país, a la mayor parte de la población hacer uso de estas tecnologías en cualquier actividad social, laboral, educativa y judicial lo que le da ciertos indicios de desarrollo.

No obstante, al hacer uso de las TICS, no todo es beneficio, pues en manos de personas, inescrupulosas, estas se convierten en una nueva herramienta para delinquir.

Entre las ventajas del uso de las TICS, destacan una interacción sin barreras geográficas, el acceso a diversidad de información, el desarrollo de habilidades, la corrección inmediata, la agilización de trámites comerciales, administrativos y de otra naturaleza, mientras que en las desventajas se encuentra el aislamiento, el fraude, el acceso a información no deseada, la manipulación de información y por supuesto la comisión de delitos, vulnerando los bienes jurídicos de las personas lo que da lugar a los denominados delitos informáticos.

El uso de las nuevas tecnologías se ha convertido en un medio directo para cometer esa clase de crímenes informáticos que por su complejidad son difíciles de investigar y de procesar, existiendo limitadas herramientas técnicas y jurídicas para probar la verdad de los hechos en un proceso penal por delitos informáticos.

A pesar de que el uso de las nuevas tecnologías se volvió cotidiano en todas las esferas de la vida social y que con ello comenzaron a cometerse delitos de naturaleza informática, la legislación penal y procesal penal no regulaba en forma expresa los delitos informáticos por lo que fue necesario crear una ley especial.

> En ese sentido, mediante Decreto Legislativo No. 260 de fecha 26 de febrero de 2016, publicado en el Diario Oficial No. 40, Tomo No. 410, de fecha 26 de febrero de 2016, se aprobó la Ley Especial Contra los Delitos Informáticos y Conexos (en adelante LEDIC), la cual entró en vigencia 8 días después de su publicación en el Diario Oficial, es decir el 6 de marzo de 2016, y se hace necesaria la actualización de los diversos operadores de la justicia penal en su contenido. (UNDOC, 2018,p. 09).

Dicha ley, es una normativa moderna que obliga a jueces, fiscales, abogados, peritos y Policía Nacional Civil a especializarse en nuevas tecnologías o delitos informáticos, para vencer el desafío que imponen las TICS en materia legal y en el proceso probatorio.

Por ende los grandes retos que enfrenta la administración de justicia penal en la aplicación de esta normativa es en lo que se refiere al derecho procesal penal, especialmente

en materia probatoria por ejemplo con los recursos informáticos idóneos, control de la cadena de custodia de evidencia digital, la preservación y tratamiento, el embalaje, lo cual exige poseer herramientas idóneas, conocimientos especiales por parte de los sujetos procesales, llámese fiscal, defensor, juez y perito informático forense, que permitan en un proceso penal arribar a la verdad material de los hechos.

En el caso específico del uso del WhatsApp que es una aplicación de mensajería instantánea, utilizada por más de 700 millones de personas en el mundo que sirve para intercambiar mensajes de texto , de voz, ficheros de audio o video y cuyo uso por personas inescrupulosas permite la falsificación mediante la manipulación de la base de datos, esto implica que al utilizar los mensajes de texto en un proceso penal este puede ser falso, lo que puede llevar al juez a una verdad formal que no concuerda con verdad material, dictando una sentencia injusta ya sea condenando a un inocente o absolviendo a un culpable.

Es por ello, que corresponde al fiscal mediante el perito informático forense demostrarle al juez a través del peritaje informático ¿cómo sucedieron los hechos?, o al abogado defensor mediante el contra peritaje informático desvirtuar lo afirmado por el fiscal.

Por lo tanto, en esta clase de procesos penales la prueba pericial informática es determinante, sin embargo en la práctica judicial muchas veces no se cuenta con las herramientas idóneas, con los recursos suficientes, con peritos debidamente capacitados y que los sujetos procesales llámese Fiscal, Defensor y Juez, no tienen los suficientes conocimientos en materia informática, por lo que se plantea la siguiente situación problemática.

¿En qué medida la pericia informática incide en la administración de justicia penal en El Salvador en el contexto de la aplicación de la Ley Especial Contra los Delitos Informáticos y Conexos?

1.2. Justificación.

La Ley Especial Contra los Delitos Informáticos y Conexos está notoriamente influenciada por el Convenio Contra el Cibercrimen de Budapest, tratado internacional que sigue siendo un referente para el marco legal de la cibercriminalidad, brinda un preámbulo para la definición de los delitos y lineamientos que deben seguir los Estados parte.

El Convenio de Budapest dio la apertura para la creación de legislaciones que debían adaptarse a nuevas tecnologías. En el año 2007 la Unión Internacional de Telecomunicaciones (ITU), logró establecer recomendaciones por medio de la Agenda Global de Ciberseguridad,

entre ellas “adaptar legislaciones a crímenes cometidos con tecnologías de VoIP o videojuegos en línea, así como también de los procesos a realizar para investigar los ciberdelitos” (Vazquez, Regalado, & Guadron, 2017 p.65) entre otras, y aunque fueron muchas las sugerencias a las legislaciones contra el cibercrimen, la mayoría de Estados que regulan los delitos informáticos parten de la base de la Convención de Budapest.

Sin embargo parte de los esfuerzos de la ITU (2015) fue realizar un informe para clasificar a los países del mundo según su preparación ante en el cibercrimen, el IMC (Índice Mundial Del Cibercrimen), se realizó con 193 Estados miembros, enfocándose en los siguientes criterios, medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades, y cooperación, en el cual El Salvador logra un índice de 0.206, colocándose en la posición 22 de la clasificación mundial, este informe al igual que otro emitido por el Banco Interamericano de Desarrollo (BID), puntualizan falencias en la estructura de Ciberseguridad en El Salvador, ya que se encuentra aún en una etapa inicial. (Union Interamericana de Telecomunicaciones (ITU), 2015).

Al momento de ser publicados los informes por el BID y por la ITU, se aprobaba la Ley Especial Contra los Delitos Informáticos y Conexos en febrero del año 2016, por lo que se evidenciaba la intención del país por colocar la Ciberseguridad como agenda nacional, no obstante las principales falencias del país en esta materia, radican en la infraestructura para el tratamiento de estos delitos informáticos, la falta de estrategias nacionales de coordinación y organización, seguridad y defensa cibernética, aplicación de normas estándares internacionales de Ciberseguridad, educación especializada sobre el tema y cultura nacional de la seguridad informática.

Otro aspecto muy importante es que la LECDIC (Ley Especial Contra Delitos Informáticos y Conexos) no habla acerca del derecho procesal y la forma en que las autoridades reaccionaran ante un delito informático, por lo que en nuestro país el combate al cibercrimen apenas comienza porque aún no se ha logrado una cultura de seguridad informática, como es la creación de instituciones especializadas, infraestructura idónea, constantes capacitaciones para fiscales, procuradores, jueces y abogados, reacción del Estado ante el cibercrimen, el derecho procesal de estos delitos y su forma de investigación como es la informática forense.

> La informática forense es una ciencia moderna, que permite reconstruir lo que sucedió en un sistema informático tras un incidente de seguridad. Este análisis puede determinar quiénes, desde dónde, cómo, cuándo y que acciones realizo el intruso para ocasionar un incidente de seguridad en el sistema. Vazquez et al.(2017).

Para llegar a este análisis de forma eficiente debe existir no solo una cultura de seguridad informática, sino también las herramientas técnicas y jurídicas, cosa que no sucede en El Salvador, debido a que en ninguna de las 27 Universidades existe la formación de Licenciados o Ingenieros especialistas en esta ciencia, y son estos los profesionales idóneos para ser peritos en los procesos sobre Delitos Informáticos.

La falta de profesionales expertos en informática forense hace preguntarse ¿si los peritos ofertados por fiscalía en realidad son versados en dicha materia?

Por otro lado, la carencia de estos especialistas hace casi imposible que un abogado defensor solicite un contra peritaje pues no encontrará el profesional adecuado que lo realice, lo que podría concluir en que no brinde una verdadera defensa conforme a la ley.

A todas estas falencias se suman la omisión de la Ley Especial Contra Delitos Informáticos y Conexos en cuanto a la presentación de la evidencia en informática forense, debido a que, no establece el proceso a seguir para su incorporación en un proceso judicial, tampoco menciona el control de la cadena de custodia de la evidencia digital, que es fundamental en una investigación porque la información crucial tiene un primer contacto con el equipo encargado de inspección.

En consecuencia, tales carencias originadas por falta de infraestructura, falta de recursos idóneos como laboratorio informático actualizado, vacíos procesales de la Ley Especial Contra Delitos Informáticos y Conexos, poca capacitación a instituciones o sujetos que son determinantes, podrían ser atentatoria la administración de justicia penal en esta clase de delitos.

Es por las razones antes expuestas que se realizará la investigación sobre los problemas probatorios de la pericia informática en el derecho penal salvadoreño, a efecto de establecer cuáles son las falencias que se presentan en el proceso penal, específicamente en el campo probatorio y a partir de los resultados obtenidos arribar a conclusiones puntuales que permitan

hacer recomendaciones para mejorar el sistema de justicia penal en El Salvador en materia de delitos informáticos.

1.3. Objetivos de la investigación.

1.3.1. Objetivo general:

Analizar los problemas probatorios de la pericia informática, en los procesos penales que se instruyen con base a la Ley Especial Contra los Delitos Informáticos y Conexos en El Salvador para acreditar la verdad material de los hechos.

1.3.2. Objetivos específicos:

1) Diagnosticar si la pericia informática practicada en los procesos penales, instruida por delitos informáticos es realizada por un especialista en nuevas tecnologías con conocimientos forenses.

2) Indagar las falencias que experimenta la fiscalía General de la República en materia probatoria pericial para acreditar la tipicidad en los delitos informáticos.

3) Comprender que carencias enfrenta la defensa técnica que interviene en procesos penales, por delitos informativos, con la utilización de la pericia informática forense.

4) Verificar si los jueces que conocen de procesos penales, por delitos informáticos consideran idónea la pericia informática al presentarla para acreditar un ilícito penal.

1.4. Preguntas de investigación.

1) ¿La pericia informática practicada en procesos penales instruidos por delitos informáticos es realizada por peritos informáticos forenses?

2) ¿Cuáles son las falencias que enfrenta la Fiscalía General de la República para poder acreditar la tipicidad de un delito informático con base a la prueba pericial?

3) ¿Cuáles son las carencias que enfrenta la defensa técnica que interviene en procesos penales por delitos informáticos donde se necesita utilizar la pericia informática forense?

4) ¿Consideran los jueces que conocen de procesos penales por delitos informáticos, idónea la pericia informática y contra pericia informática que se aporta para acreditar la verdad material?

1.5. Delimitación.

Para el desarrollo de la investigación se tomó en cuenta el aspecto temporal y espacial, que permitió delimitar la ejecución, tanto en el tiempo como en el espacio.

1.5.1. Delimitación temporal:

Con respecto al alcance temporales de la investigación se tomó como punto de partida el seis de marzo del dos mil dieciséis, fecha en la cual, entró en vigencia la Ley Especial Contra los Delitos Informáticos y Conexos en El Salvador, se realizó un análisis al medio probatorio denominado pericia informática y a su aplicación en un proceso penal, así como también se realizó un estudio a las instituciones que manejan información sobre delitos informáticos, a manera de determinar si poseían conocimientos forenses en materia informática, en vista que es en torno a ello que se desarrolló la investigación.

1.5.2. Delimitación espacial:

Para el desarrollo de una investigación es preciso señalar un ámbito socio gráfico el cual se desarrollará la misma, por ende se definió al departamento de Santa Ana, estudiando instituciones como la Fiscalía General de la República, Procuraduría General de la República y Juzgados de Instrucción y Sentencia de Santa Ana para lo cual, se tomó como sujetos de investigación a Jueces, Fiscales, Defensores públicos y privados, y a los Peritos del Laboratorio Técnico Científico de la Policía Nacional Civil ubicado en San Salvador.

1.6. Consideraciones éticas.

El trabajo investigación se realizó utilizando la metodología cualitativa, y por ende para cumplir con el rigor metodológico que le del carácter de científico se sometió a los criterios de: credibilidad, confirmabilidad, aplicabilidad, utilidad y neutralidad, los cuales se plantearon de la siguiente manera.

Credibilidad: en el sentido de que al realizar el proceso de recolección de información se contará con hallazgos reales o verdaderos, que no estén sometidos a manipulación por el grupo investigador y que las personas que brindan la información sean las que estén directamente relacionadas con el fenómeno objeto de estudio.

Confirmabilidad: al someter la información obtenida al proceso de análisis que servirá para fundamentar las conclusiones, otros investigadores podrán seguir la pista del trabajo realizado obteniendo hallazgos similares.

Aplicabilidad: los resultados que se obtengan en el proceso de investigación también pueden transferirse o ser aplicados a otros contextos o grupos con características similares.

Utilidad: como resultado de la investigación se arribará a conclusiones que derivaran en recomendaciones para el beneficio de la comunidad jurídica.

El grupo investigador garantiza que no se revelará la identidad ni el cargo de los funcionarios informantes, así como también que la información obtenida será utilizada únicamente para fines educativos.

CAPÍTULO II

MARCO TEÓRICO

2.1. Marco histórico.

2.1.1. Breve reseña histórica de la informática a nivel internacional.

Según Barceló (2008) afirma que"…el primer precedente histórico de la informática es el Ábaco" (p.25). Este era empleado para realizar operaciones aritméticas, fue el primer instrumento en la historia de la humanidad en realizar un cómputo. "…Parece ser originario en el Antiguo Oriente, donde se utilizó incluso hace ya más de 5000 años" (Barceló, 2008, p.26).

Posteriormente en el siglo XVII otro de los hechos importantes en la evolución de la informática es cuando el científico Blaise Pascal inventa la máquina de pascal o pascalina, "…que consistía en una maquina mecánica para sumar" (Areitio & Areitio, 2009, p.85)

En el año 1694 Gottfried Von Leibniz construye una calculadora universal, con la que se podía realizar cuatro operaciones sumar, dividir, restar y multiplicar. (Areitio & Areitio, 2009)

Más adelante en 1835 Charles Babbage concibe la primer maquina analítica, considerada el antecedente histórico directo de los ordenadores actuales. Sin embargo, no se pudo construir, dado que en la época victoriana no contaban con suficiente tecnología. La estructura interna del diseño de la maquina analítica de Babbage es muy parecido a lo que hoy en día conocemos como la arquitectura Von Neumann, que se construyó en 1944, después que se descubrieran en 1937 los escritos y diseños de Babbage (Barceló, 2008).

En 1946 John Presper Eckert y John William Mauchly crean la computadora electrónica llamada ENIAC (por sus siglas en inglés Electronic Numerical Integrator and Computer O Integrador Numérico y Calculador Electrónico).

Posteriormente continuaron los avances y se originan los ordenadores de segunda, tercera y cuarta generación, siendo cada vez más sofisticados.

2.1.2. Historia del internet.

El internet se origina en los años sesenta durante la guerra fría, en Estados Unidos de América, donde se estaba buscando una manera de comunicación alternativa a las comunes, esto debido a un posible caso de existir una Guerra Nuclear.

Al buscar diferentes alternativas se decidió tener un proyecto dentro del cual, se plasmaran algunos principios como, el eliminar cualquier tipo de autoridad central, esto debido a que la autoridad central pudiera ser un punto de ataque, es por esa razón que se toma la decisión tener una red descentralizada en la cual cada máquina que estuviere conectada debía poseer el mismo estatus y la misma capacidad de almacenaje de información y a la vez poder enviarla (Moraga, 1995).

Sin embargo, el envío de datos debía ser posible incluso teniendo una red descentralizada, para lo cual los mensajes se dividieron en pequeños paquetes de información que contenían la dirección de destino. Cada paquete debía buscar la manera de llegar al destinatario según las rutas disponibles. El destinatario sería el encargado de re ensamblar los paquetes individuales para construir el mensaje original, de modo que el camino que tomase cada paquete no tendría importancia. Así, en dado caso que grandes porciones de la red fuesen destruidas no importaría; pues los paquetes permanecerían en la red en los nodos que hubieran sobrevivido.

Con este principio el Laboratorio Nacional de Física (National Physical Laboratory) de Gran Bretaña preparó la primera red de prueba en 1968. Poco después, la Agencia de Proyectos de Investigación Avanzada del Pentágono (ARPA) de los EEUU decidió financiar un proyecto más ambicioso y de mayor envergadura. Los nodos de la red iban a ser superordenadores de alta velocidad (o lo que se llamó así en aquel momento).

Eran máquinas poco usuales y de mucho valor y que estaban necesitadas de un buen entramado de red para proyectos nacionales de investigación y desarrollo.

En 1969 el primero de esos nodos fue instalado en UCLA (la Universidad de California). (Aroche, 2006).

En diciembre de ese año la pequeña red, llamada ARPANET y promocionada por el Pentágono, contaba con 4 nodos. En 1971 había quince nodos en ARPANET; en 1972, la cantidad se incrementó a treinta y siete. Sin embargo, ya en 1972, la mayor parte del tráfico de ARPANET no era el proceso de datos a largas distancias, sino noticias y mensajes personales.

Los investigadores estaban usando ARPANET para colaborar en proyectos, intercambiar notas sobre sus trabajos y, eventualmente, para pasar cualquier tipo de mensaje.

> En 1984, la National Science Foundation (NFS), una fundación creada para la investigación académica, conectó su propia red (NFSnet) con ARPANET. La conexión de ambas redes, recibió el nombre de Internet". (Aroche, 2006).

Posteriormente se conectarían otras redes gubernamentales (NASA, el Departament of Energy.). Sin embargo, dicha red estaba restringida, de manera que varias empresas empezaron a construir sus propias redes y a ofrecer servicios similares, que con el tiempo se fueron conectando entre sí, hasta desembocar en el Internet actual.

> En 1990 y 1995 se desconectaron ARPANET y NFSnet, las redes que unidades habían creado al internet y respectivamente los servicios comerciales las reemplazaron rápidamente. Desde entonces el crecimiento de Internet ha sido espectacular incluso más rápido que la telefonía móvil esto según estadísticas realizadas por Estados Unidos de América en las cuales dan a conocer el dato que en junio de 2010, los usuarios de Internet ascendían ya a 1966 millones de personas consistiendo en el 28,9% de la población mundial (Aroche, 2006).

2.1.4. Primeros problemas jurídicos que aparecen con la informática.

> En los últimos años de la década de 1950 y a finales de la década de 1970 surge la revolución digital en Estados Unidos, que consistía en el cambio de la tecnología industrial a la electrónica digital, debido a la proliferación y adopción de la computadora, la computadora personal y el internet. (Sain, 2018)

Tácitamente el término también alude a los cambios que se originaron por la tecnología de la comunicación durante y después del siglo pasado. Y es así como se da origen a la Era de la Información.

En esta nueva era desaparecen los límites territoriales que antes se conocían. Esto toma vital importancia cuando en esta nueva era se asocia las Tics con actividad delincuencial.

La erosión de las barreras geográficas plantea diferentes problemas jurídicos entre los que se puede mencionar:

> Los relativos a la publicidad en internet, la jurisdicción competente… los delitos informáticos, la falta de seguridad en la red, protección a los datos personales y las consecuencias a la violación al derecho de intimidad, transgresiones a los derechos de los consumidores y usuarios, la piratería, violación al derecho de propiedad intelectual y … pornografía infantil. (Scotti, 2016, p. 91).

2.1.3. Surgimiento del internet en el salvador.

Los países centroamericanos no podían quedarse atrás con el uso de las nuevas tecnologías. Para el año de 1993 Costa Rica se conecta a internet, siendo el primer país de Centroamérica en lograrlo, posteriormente El Salvador inicia los trámites y pasos para conectarse.

En El Salvador la administración de los recursos de Internet inicialmente fue delegada a instituciones públicas dedicadas al desarrollo de las ciencias y la investigación por ende necesariamente vinculadas con centros de educación superior. (Octavio, 2011). Inicialmente fue en CONACYT (Consejo Nacional de Ciencia y Tecnología), donde se instaló un nodo, el cual permitía manejar el tráfico del correo electrónico enviado y recibido en el país. (Ibarra, 2002).

Según el Ingeniero Ibarra (2002), considerado el padre del internet en El Salvador por sus grandes aportes establece que:

> En septiembre de 1994 se gestionó, ante el IANA (Internet Assigned Numbers Authority) y el InterNIC (Internet Network Information Center), respectivamente, un conjunto de direcciones IP, equivalentes a una clase B, y la administración del dominio de Nivel Superior correspondiente a El Salvador, SV.(p.5).

El termino SV, permite diferenciar los sitios web salvadoreños con los demás. Días después se creó el grupo SV.Net. Fue conformado por la Universidad de El Salvador, Universidad Centroamericana, el CONACYT, Universidad Don Bosco, ANTEL (Administración Nacional de Telecomunicaciones) y FUSADES (Fundación Salvadoreña para

el Desarrollo Económico y Social), con el propósito de administrar el dominio SV y un conjunto de direcciones IP.

En 1995 la embajada de los Estados Unidos imparte una capacitación a los miembros de SV. NET, llamada Criterios para la gestión y desarrollo de la red Internet en El Salvador. En diciembre del mismo año se realizaban pruebas e instalaciones, y es en enero de 1996 que se logra una conexión a Internet estable desde El Salvador en el edificio de ANTEL, San Salvador.

> En 1996, las telecomunicaciones fueron privatizadas y se creó la Superintendencia General de Electricidad y Telecomunicaciones (SIGET). Esto con el fin de actualizar las telecomunicaciones, pasando del monopolio público a la empresa e inversión privada, ya que ANTEL no cumplía con la demanda. (Superintendencia General de Electricidad y Telecomunicaciones, 2014).

2.1.5. Comisión de delitos.

En la década de los setenta con la expansión o difusión de ordenadores e internet, empieza el surgimiento de la delincuencia a través de medios informáticos, "Los primeros delitos informáticos eran de tipo económico, entre los que destacaban el espionaje informático, la "piratería" de software, el sabotaje a base de datos digitalizados y la extorsión." (Sain, 2018, p. 8).

> Posteriormente se desatan más ciberdelitos y en el Estado de Florida de EE. UU en 1978, se reconocen los crímenes de sistemas informáticos, entre ellos el sabotaje, copyright, modificación eliminación y sustracción de datos, y estas conductas empiezan a ser penadas, siendo en 1981 que se condena a la primera persona por un delito informático, Ian Murphy, quien hackeó redes y cambio el reloj para recargar tarifas fuera del horario en horas pico. (Gissel, 2005)

Después del reconocimiento de los crímenes de sistemas informáticos, era necesario auxiliarse de una ciencia para vencer los grandes retos, y técnicas de los ciber delincuentes, asimismo garantizar la verdad en referencia a la evidencia digital, que podría aportarse en este tipo de procesos judiciales.

Los delitos informáticos continuaban y toman relevancia. Para el año de 1983 Peter Norton un informático Estadounidense, creó el programa UnErase, que era un recuperador de datos eliminados, y se considera que fue el inicio de los procesos que dieron pie a una nueva ciencia llamada informática forense, que es:

> Aquella disciplina que se encarga de la obtención, el análisis y la valoración de diversos elementos que puedan considerare como una evidencia digital, la cual es hallada en ordenadores, soportes de datos e infraestructuras de red, que tenga la característica de poder aportar información capaz de esclarecer la implicación de uno o más individuos en actividades ilegales relacionadas o llevadas a cabo en contra de instalaciones de procesamiento de datos. Grupo Arga Detectives Privados (GADP, 2018 párr. 14).

Un año después el FBI creó el Programa De Medios Magnéticos en 1984, que hoy en día es conocido como CART (computer analysis and response team o análisis de informática y equipo de respuesta), que se utilizaba para la recuperación de datos en investigaciones federales. (GADP, 2018).

Michael Anderson agente de investigación criminal, trabajó varios años para el gobierno de Estados Unidos, era especialista en la recuperación e investigación. Años después fundó su empresa New Technologies, que trabajaba como una firma de forenses informáticos. Anderson es considerado el padre de la informática forense por su labor en ese campo. En 1995 se crea la IOCE (International Organization on Computer Evidence u Organización Internacional de Evidencia Informática), y la investigación en informática forense se reconoce como ciencia.

Como consecuencia en 1997 se exigía a todos los funcionarios judiciales en Estados Unidos poseer amplio conocimiento en esta rama, obligándolos a estudiar y conocer cómo se obtienen las evidencias en medios electrónicos y computadoras. Y la informática forense se convierte en una disciplina auxiliar de la justicia moderna.

2.1.6. Necesidad de la pericia informática.

En el Tratado Pericial Judicial, se habla sobre la pericia informática y la participación que tienen los peritos haciendo énfasis en este punto en vista que su papel es fundamental en la pericia informática ya que son estos quienes la practican.

> Los peritos en informática intervienen cuando para la introducción de hechos relevantes en un proceso reglado se requieran conocimientos especializados en informática. De forma sintética, la acción del perito consiste en responder las cuestiones que se le plantean. Tomando como entrada elementos indiciarios informáticos y haciendo uso de sus conocimientos y experiencia construye un ámbito de plausibilidad en el que se derivan hechos relevantes al proceso, dando la debida respuesta a dichas cuestiones. (LLUCH, 2014, pág. 319).

Hablar de la necesidad de la pericia informática implica el reconocimiento de la evolución de los delitos y de aquellos que los perpetran, debido a que la forma de comisión de estos ya no es la tradicional regulada por el Código Penal, esto genera como consecuencia que se necesiten actualizar los sistemas penales, los delitos se deben adecuar a las nuevas conductas y las pruebas deben ser acordes a estos delitos para que se genere en el juzgador la plena certeza jurídica para resolver los procesos penales.

La pericia informática encuentra su razón de ser en la necesidad de obtener evidencias que puedan ser utilizadas en un proceso penal y que no puedan ser obtenidas de otro modo que no sea a través de la experiencia de un especialista en la materia y que de este modo se pueda llegar a determinar la verdad real de los hechos.

> En este sentido, si el peritaje es informático se caracteriza por proporcionar al juez esos argumentos o razones acerca de los aspectos que resulten controvertidos en una determinada situación de un sistema informático y que tenga relevancia jurídica, (…). Para obtener tales razones y argumentos, el perito informático usa una rama de la Informática denominada Informática Forense. (Garcia Gomez, 2015, pág. 7)

> La informática forense constituye un conjunto de técnicas orientadas a la adquisición, preservación y análisis de elementos indiciarios informáticos de una forma verificable y sólida", (Balsera, 2014, pág. 322).

Esto con el objetivo de facilitar la introducción de los datos obtenidos en un peritaje informático al Proceso Penal.

En ese orden de ideas la pericia informática se vuelve necesaria también por el hecho que a través de ella, el juez que tiene bajo su conocimiento el caso, comprende nuevos elementos no contemplados normalmente en los procesos para tener claros aquellos aspectos básicos a contemplar para poder resolver, siendo estos quien cometió el hecho, como lo cometió, cuál fue el medio, etc., y es el perito forense quien a través de su informe le da estos elementos al juez para poder resolver el caso.

2.2 Marco doctrinario.

2.2.1. Aspectos generales de la prueba.

2.2.1.1. Definición.

Dentro de la prueba existe una variedad de aspectos que se presentan, relacionados al derecho penal y para lograr determinar cuáles pueden ser estos aspectos, es indispensable conocer diversas definiciones según autores o tratadistas penales que la han definido, parta no confundir prueba con medio de prueba.

> Algunos autores toman en un solo concepto el propósito de la prueba con los medios que esta puede llegar a presentar, por ejemplo, según Gimeno Sendra, "la prueba es aquella actividad de carácter procesal cuya finalidad consiste en lograr la convicción del Juez o Tribunal, acerca de la exactitud de las afirmaciones de hecho operadas por las partes en el proceso" (Sendra, 1981, p.214).

Esta definición que proporciona Gimeno Sendra da una clara idea sobre la función que tiene la prueba en un tribunal, siendo dicha función lograr conseguir la convicción en el juez que las afirmaciones que hacen las partes corresponden con el hecho material del delito, tomando la prueba como consideración el juez para llegar a la verdad real, sin embargo también es válido saber que toda prueba es un impulso en el proceso para descubrir el hecho

delictivo y que además de ser importante y útil en un proceso es un elemento esencial a la hora de hacer valer los derechos de las partes materiales.

Para la doctrina según el Vocabulaire Juridique prueba es: "la demostración de la existencia de un hecho material o de un acto jurídico, mediante las formas determinadas por la Ley (Caballenas, 1989).

Esta definición va encaminada más a la parte acusada, esto con el fin de que pueda presentar las pruebas que sean necesarias para hacer valer la presunción de inocencia, en vista que no se le puede atribuir lo contrario sin antes haberse probado en un juicio previo, relacionando así lo establecido en el artículo doce de la Constitución del país, el cual literalmente dice "Toda persona a quien se le impute un delito se presumirá inocente mientras no se pruebe su culpabilidad conforme a la Ley y en Juicio Público, en el que se le aseguren todas las garantías necesarias para su defensa". (Constitución, 1983, pág. 10).

Esto comprueba que las presentaciones de los medios de prueba son necesarias en un juicio para que este siga un rumbo real sobre el hecho que ha sido considerado como delito, y de esa manera poder acertar sobre la inocencia de la parte acusada o la culpabilidad de la misma.

Además se tiene como ejemplo otras definiciones como la que establece Hernando Devis Echandía quien sostiene que "prueba es el conjunto de reglas que regulan la admisión, producción asunción y valoración de los diversos medios que pueden emplearse para llevar al juez la convicción sobre los hechos que interesan al proceso" (Echandía, 1981, p.5).

Pero también es importante conocer lo que dice el Código Procesal Penal sobre la finalidad que la prueba tiene, haciendo mención a ello en el artículo ciento setenta y cuatro el cual establece que la finalidad de la prueba es llevar al conocimiento del juez o tribunal los hechos y circunstancias objeto del juicio, especialmente lo relativo a la responsabilidad penal y civil derivada de los mismos (Asamblea Legislativa de la República de El Salvador, 1983).

2.2.1.2. Objeto, órgano, elemento y medio de prueba.

Objeto de prueba: Todo aquello que debe ser probado. "Las circunstancias fácticas que se deben acreditar para que se obtenga la certeza o probabilidad acerca del acontecimiento histórico introducido al proceso como hecho incierto" (UNDOC, 2018 p. 107).

Órgano de prueba: "Es el sujeto que porta un elemento de prueba y lo trasmite al proceso". (Cafferrata, 1998, p. 23).

Elementos de prueba: se entiende como "la información o el dato que debe llevar o conducir a la convicción judicial sobre el objeto de prueba. a) Testigo y perito: Su dicho. b) Los documentos: La información que hacen constar". (UNDOC, 2018, p. 109).

Medio de prueba: Los modos instrumentales a través de los cuales ingresa información al proceso. En tal sentido, constituyen las diligencias específicas destinadas a la incorporación de datos relacionados con el objeto investigado y discutido. (UNDOC), 2018, p. 108). En otras palabras es el procedimiento establecido por la ley destinado a lograr incorporar el elemento de prueba en el proceso.

2.2.1.3. Principios que rigen la prueba.

Para obtener los resultados deseados dentro de un proceso en materia penal, es necesario tener la certeza, que la persona que se está siendo procesada, sea quien llevo a cabo el hecho delictivo que se le imputa o al contrario tener la seguridad, que la persona procesada no participo en el hecho que se le atribuye. Para llegar a esta certeza es preciso verificar por parte del juez todo el elenco probatorio que ha sido llevado a juicio, es preciso aclarar que estas pruebas no fueron obtenidas antojadizamente sino que respetando ciertos principios.

Los principios que la doctrina consideran que sustentan la prueba, en cuanto a su proposición, admisión, recepción y valoración, son los siguientes:

Libertad Probatoria: Este como uno de los más importantes implica, que se podrá utilizar cualquier medio probatorio para demostrar hechos vinculados con un delito, y en su defecto, se podrá disponer de medio distinto siempre y cuando se incorpore al proceso de la manera prevista para la incorporación de pruebas similares, siempre que se respeten las garantías primordiales de las personas y que están estipuladas en la Constitución (Sandoval, 2018). Esto implica que no se exige la aplicación de un medio probatorio en concreto, por lo que se puede recurrir al que promete mayores garantías de eficacia, se pueden emplear medios de prueba no reglamentados, siempre que sea adecuado para descubrir la verdad.

Pertinencia De Los Medios Probatorios: Es la que se refiere al hecho que se fija como objeto de la prueba y que trata sobre las proposiciones o hechos que son verdaderos (Sandoval, 2018). Siendo necesario que los medios probatorios ofrecidos guarden una relación lógica y jurídica con los hechos que sustentan la pretensión o la defensa; de lo contrario, no deben ser

admitidos en el proceso, por lo que los medios probatorios que resulten impertinentes deben ser rechazados por el Juzgador.

Valoración De La Prueba: El Juzgador tiene que fundamentar la sentencia que versa sobre la verdad real de los hechos, teniendo como base la prueba, la cual debe valorar con las reglas de la sana crítica como lo es el correcto entendimiento humano, la lógica y la experiencia del Juez (Sandoval, 2018). Los jueces fundan su decisión sobre aquellos actos que miran como demostrados, teniendo la prueba como la parte más importante de las prescripciones legales en materia penal.

Idoneidad De La Prueba: La aplicación de este principio, consiste en la exigencia de que la fuente de prueba, el medio de prueba y el objeto de prueba deben reunir condiciones tanto intrínsecas como extrínsecas para que se adecuen a la exigencia de la validez de la actividad probatoria, pues solamente un acto probatorio que ha sido válido tiene la aptitud de tener eficacia. (Mixan, 2003)

Comunidad O Unidad De La Prueba: Según este principio, las pruebas se valoran en su conjunto, bien sea que se hayan practicado a petición de alguno de los sujetos procesales o por disposición oficiosa del juez. "Durante la actividad probatoria, se incorporan en el proceso una pluralidad y diversidad de medios probatorios, lo que, para los fines de la valoración, deben ser consideradas como una totalidad, como un solo conjunto de lo diverso y múltiple" (Mixan, 2003, pág. 185). Ósea, no se puede prescindir arbitrariamente de apreciar por separado alguno de los componentes de ese conjunto unitario y complejo.

Legalidad De La Prueba: Este principio implica que los elementos de prueba solo tendrán valor si los mismos han obtenidos lícitamente e incorporados al proceso de acuerdo a las disposiciones del código. Según este principio, no pueden admitirse en el proceso aquellos medios probatorios que son obtenidos violando el ordenamiento jurídico y derechos personales (Sandoval, 2018).

2.2.1.4. Clasificación de la prueba.

La prueba, en materia penal se clasifica doctrinariamente de diversas formas, Davis Echandía en su libro "Teoría General de la Prueba" manifiesta que la prueba se divide en cuatro categorías, que a continuación se desarrollara de forma breve cada clasificación.

Conforme a su finalidad:

Prueba de descargo: También se le denomina contra prueba, y el cual consiste en acreditar la inocencia del procesado (Echandía, 1994)

Prueba de cargo incriminatoria: "Es la que va dirigida a demostrar la culpabilidad del imputado dentro del hecho delictivo que se le atribuye" (Echandía, 1994, pág. 177).

Conforme a su ilicitud o licitud:

Pruebas ilícitas: Se comprenden como aquellas que han sido recabadas e incorporadas al proceso penal violentando derechos constitucionales o una norma procesal (Echandía, 1994).

Pruebas lícitas: "Por su validez y eficacia probatoria se encuentran garantizadas por su estricto apego al debido proceso" (Echandía, 1994, pág. 178). De tal forma que dichas pruebas han sido obtenidas e incorporadas de forma licita.

Conforme a su resultado:

Prueba plena: También denominada como prueba completa o perfecta. "es una sola prueba que le proporciona al juzgador la suficiente convicción de que el acusado a participado en el delito que se le imputa o al contrario que este no tuvo participación dentro del hecho atribuido" (Echandía, 1994, pág. 180).

Prueba semiplena: Conocida como prueba incompleta o imperfecta en esta "el juez necesita que la única prueba sea complementada con otros elementos probatorios para llegar a la convicción" (Echandía, 1994, pág. 180).

De acuerdo con su utilidad:

Pruebas útiles: Estas "constituyen un apoyo que le permite al juzgador obtener la convicción con respecto a hechos que son relevantes en el proceso penal" (Echandía, 1994, pág. 182). Por medio de esta el juez puede llevar a obtener una certeza de la verdad real de los hechos.

Pruebas inútiles: Se refiere a las que no prestan ningún servicio o auxilio al juez.

Pruebas pertinentes: Tienen una relación de manera directa o indirecta con el hecho que se pretende probar.

Pruebas impertinentes: No guardan ningún tipo de relación con el hecho que se pretende demostrar, por lo que su incorporación dentro de un proceso no puede ser válida.

2.2.1.5. Reglas de valoración de la prueba.

2.2.1.5.1 ¿qué es valorar prueba?

Sobre la valoración de la prueba esta "consiste en una actividad interna, intelectual y moral del juez, que da lugar a la denominada íntima convicción sobre la culpabilidad o inocencia del imputado" (Casado Pérez, 2000, pág. 141).

Asimismo la valoración es una actividad en la que la evaluación de la prueba no ofrece aún exteriorización alguna, porque nos encontramos en el ámbito íntimo de la conciencia del juez y del proceso intelectual previo a la elaboración definitiva de la sentencia (Casado Pérez, 2000). Siendo el momento de exteriorización cuando se produzca la fundamentación fáctica de esta.

De lo dicho por el profesor Casado Pérez es válido resaltar dos aspectos importantes los cuales son: el primero de ellos la valoración de la prueba y el segundo la íntima convicción, entendida esta como la decisión final adoptada por el juez, es por ello que se vuelve preciso aclarar estos conceptos.

Según Ampuero (2016), suele confundirse entre los estudiosos del derecho el momento de "la decisión del juez" con "la valoración de la prueba" (P. 6). Pero se trata de dos distintas partes de un mismo todo que se pueden analizar por separado, entendida la primera como el momento en el cual el juez obtiene en sí mismo la certeza y elige cual será el resultado del proceso, ya sea absolviendo o condenando al procesado, por otro lado la valoración de la prueba es el momento previo a la decisión del juez, consiste en apreciar una prueba y considerar si genera un convencimiento en la psiquis de este para posteriormente tomar la ya mencionada decisión.

2.2.1.5.2. Sistemas de valoración de la prueba.

José María Casado Pérez (2000), cuando se refiere a los sistemas de valoración de la prueba en su libro La Prueba en el Proceso Penal Salvadoreño, distingue dos sistemas que han existido con el tiempo que son: el sistema de la prueba legal y el de la prueba libre, más un tercer sistema que denomina de la sana critica (mixto).

1.- El sistema de libre apreciación de la prueba. Este sistema se conoció desde la época romana y consiste en que los jueces resuelven los procesos sometidos a su conocimiento en base a la convicción que se forman de la prueba que desfila en juicio, no existen reglas o

criterios para otorgar a una prueba algún valor determinado, sino que es el juez per se, quien otorga el valor a la prueba.

2.- El sistema de la prueba legal o tasada. En el sistema de prueba legal o tasada fue introducido en el derecho canónico, básicamente se buscaba con este crearle limitaciones al juez, en el sentido que para resolver un litigio o caso este no se basara solo en sus valoraciones personales sino que tenía que tomar en cuenta lo que la ley disponía para el caso en concreto, obligándolo de este modo a ceñirse a los criterios legales dados por el legislador. Se buscaba también crear un proceso más transparente libre de arbitrariedades del juez, esto en razón a que antes de este la aplicación del sistema en comento el juez era quien ejercía el dominio sobre la valoración de la prueba y era quien disponía de cómo iba a valorarla según su criterio sin ninguna limitante.

3.- El sistema de prueba mixta. Este sistema surge de la unión de ambos sistemas tomando tanto elementos de uno como del otro, esto implica que el juzgador al momento de valorar prueba debe tomar en cuenta las normas jurídicas que rigen el sistema probatorio y apegarse a ellos para emitir su sentencia, pero no está enmarcado solo a lo que la ley le dice que debe ser el valor de cierta prueba sino que también tiene la facultad de valorar una prueba según sus apreciaciones personales expresando los motivos o razones en las cuales se funda para resolver un proceso, en ambos casos actuara según la ley.

Según Couture (2010) “este sistema es aquel que configura una categoría intermedia entre la prueba legal y la libre convicción. Sin la excesiva rigidez de la primera y sin la excesiva incertidumbre de la última” (Pág. 209).

Teniendo claros todos los elementos de la prueba, cabe entonces analizar un tipo especial de prueba llamado: prueba pericial, en vista que esta prueba no está siempre presente en los procesos penales sino que es ocasionalmente que esta se desarrolla, y en la actualidad su importancia es tan grande que puede ser la prueba que defina un proceso, es decir puede ser la que le deje claro al juez su decisión, ya sea absolviendo o condenando al procesado.

2.2.2. La prueba pericial.

La prueba pericial como eslabón de nuestro sistema probatorio en el proceso penal, es desarrollada en la ley, el libro primer capítulo lV del Código Procesal Penal vigente, contiene dentro de su articulado lo relativo a los peritos, así como también a los casos en que el juzgador tendrá que recurrir a ellos para verter la prueba a través de su dictamen.

Para entrar más a fondo en la prueba pericial, es necesario definir que es un perito, y este "es aquella persona especialmente cualificada en virtud de sus conocimientos especializados en una ciencia, arte, técnica o práctica" (Garciandía, 2008, pág. 71). Es decir, que es una persona que posee especiales conocimientos en materias que no son conocidas con ese nivel de precisión, por las demás personas de su mismo nivel cultural.

Por prueba pericial se comprende a un perito, este como un tercero ajeno al juicio que comparece a juicio y presta declaración ante el tribunal en forma directa a través del examen directo y el contraexamen de las partes, "Su declaración en juicio no puede ser reemplazada, sustituida o complementada por declaraciones previas registradas en actas o por su informe pericial escrito" (Baytelman , 2008, pág. 329).

Debido a lo anterior, la prueba pericial surge del dictamen de los peritos el cual conlleva una opinión emitida por este, siendo personas llamadas para la obtención de una determinada prueba por medio de técnicas, y del cual deben dar un informe al juez.

2.2.2.1. Clases de pericias.

La prueba pericial, típicamente se ha considerado como la prueba para contribuir en la solución de un proceso, en el caso en el que el Juez necesite de conocimientos especiales y/o técnicos que ayuden a dilucidar o establecer los hechos que son objetos de la investigación, puesto que, el funcionario judicial cuenta con conocimientos jurídicos, sin embargo, no posee conocimientos en áreas especiales o técnicas de cierta materias, es por ello, que recurre a las personas especializados que si lo tengan para dar la solución con mayor facilidad al proceso.

Es por ello, que existen diferentes clases de pericias que se consuman con el objeto de indicar en una investigación los efectos o las diferentes causas de un delito, por lo que, se hace necesario desarrollar cada pericia y establecer que roll cumple en una investigación de las cuales mencionaremos las siguientes:

Pericia Toxicológica: es conceptualizada como "la ciencia que estudia los efectos adversos que los agentes físicos y químicos pueden producir en el hombre y los animales". (Roque, 2016, pág. 1); Es decir, su estudio está basado con sustancias toxicas que está en el ser humano y que puede traer como consecuencia la muerte debido al grado de intoxicación que puede sufrir por medio de sustancias químicas, radioactivas, etc.

Pericia Odontológica Forense: Podemos entender como aquella rama " de la medicina forense que consiste en el estudio de características dentales y sus arreglos, apoyado de moldes y formulas dentarias, a efecto de hacer comparaciones formales con fichas odontológicas y establecer la identidad de la persona o cadáver" (Morales, 2013, pág. 17).

Es por ello, que a través de este tipo de pericia se logra establecer la individualización de cadáveres que han pasado por procesos de mutilación, que han sido calcinado o que el cuerpo de la víctima se encuentre en estado de putrefacción avanzada, por esa razón que se requiere la aplicación de métodos odontológicos, en la que mediante el estudio de los dientes y las reconstrucciones dentales, se busca su identificación. (Luján, 2010).

Pericia Psiquiátrica:

> Se trata de evaluar a una persona que ha delinquido, para establecer si existe o no nexo entre el delito y una enfermedad mental; se expresa en la experticia si algún estado psíquico anormal pudo hacer que el indiciado o acusado fuera incapaz de apreciar el carácter ilícito del acto. (Puente, 2014, parrá. 3).

Por ese motivo, está basada en hacer un estudio a una persona que ha tenido una conducta delictiva con el objetivo de verificar si existe o no un vínculo entre un delito y una enfermedad mental.

Pericia Clínico- Forense: Es entendida como aquella pericia que son perpetradas en ciertas personas que han obtenido experiencias procedentes de violencia intrafamiliar o de otras vivencias que incitan una desorientación en su personalidad y que son causadas por una persona que tiene una conducta desviada al momento de efectuarla a la víctima generándole ciertos daños psicológicos.

Autopsia: Es otra de las de las clasificaciones de la pericia y esta puede ser entendida como:

> Es una necrocirugía; es decir, procedimiento médico que emplea la disección (división en partes de una planta, un animal o un ser humano muertos para examinarlos y estudiar sus órganos), con el fin de obtener información anatómica sobre la causa, naturaleza, extensión y complicaciones de la enfermedad que sufrió en vida el sujeto. (Anónimo, 2014, parrá. 22)

No obstante, de este tipo de examen se deriva la autopsia científica y la autopsia y la autopsia médico- legal, siendo esta última que nos interesa, puesto que, se da a través de mandato judicial cuando la muerte de una persona sea dudosa.

Sin embargo, la autopsia como pericia es reconocida y regulada en el Código Procesal Penal en su artículo 189 por el cual, establece generalmente su objeto dentro del proceso.

Pericia en Balística Forense: Radica en el examen a las armas de fuego encontradas en la escena de un hecho delictual, la características de estas, cual es el medio de proyección y sobre sus municiones; además, la dominio de las circunstancias imprevisibles al momento de la ejecución del disparo. (Dirección General de Apoyo a la Investigación Penal , 2013).

Pericia Dactiloscópica: Este tipo de pericia "es la ciencia que se propone identificar a las personas físicamente consideradas por medio de la impresión o reproducción física de los dibujos formados por las crestas papilares en las yemas de los dedos de las manos" (Jinde, 2012, parrá. 1).

Es decir, hacer aquel estudio del rastro que han sido desarrollados por las crestas papilares de las yemas de los dedos de las manos de las personas que tiene indicios de sospechosa en cierta conducta delictiva.

Pericia Informática: Se refiere **"**en que una figura legal y especializada da support. Y ofrece sus servicios a particulares, empresas, ya sean estas públicas o privadas. Para poder resolver ciertos problemas o situaciones de conflicto. Todos ellos relacionados con la informática". (Informático Forense Madrid, 2018, parrá. 5).

Este tipo de pericia estriba en la agrupación de conocimientos de investigación y estudio con el objeto de decretar el sostenimiento de la prueba que ha sido obtenida en los sistemas de computación y/o algún otro medio informático.

Es por ello, que nuestra ley procesal penal establece, aunque no como una pericia en su artículo 201 la información electrónica, manifestando la facultad que tiene el fiscal a una autorización judicial para medidas que garanticen la obtención, resguardo o almacenamiento de una información.

2.2.3. La prueba pericial informática en el proceso penal.

2.2.3.1. Definición.

Se puede llegar a definir la prueba pericial informática o digital según (Puig, 2015) como:

> La información obtenida o transmitida a través de un medio electrónico o dispositivo digital que sirve para acreditar la evidencia de un hecho de relevancia en cualquier orden jurisdiccional, la cual es obtenida o transmitida a través de un medio electrónico o dispositivo digital que sirve para acreditar la evidencia de un hecho de relevancia en cualquier orden jurisdiccional. (p 505)

Es decir, la información que esté almacenada o sea transmitida mediante un medio o soporte electrónico.

Dentro de los medios que se pueden llegar a encontrar son los siguientes: sonido e imagen, instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase relevantes para el proceso, páginas web.

Sin embargo, nuestra legislación en materia procesal no hace énfasis a este tipo de prueba, pero se da por entendido que esta incorpora los medios probatorios previstos en la Ley Especial Contra los Delitos Informáticos y Conexos.

La prueba pericial va de la mano con el análisis e imparcialidad de parte del profesional encargado en la búsqueda del rastro que haya dejado el hecho cometido, además se debe de tomar en cuenta que cuando este tipo de acciones son realizadas por medio del uso del internet o medios informáticos es necesario tener apoyo sobre conocimientos técnicos científicos debido al manejo que se puede llegar a tener con este tipo de pruebas y al análisis que se le deberá de hacerle saber al Juez conocedor de algún delito relacionado al tema.

Dentro del análisis que se hace a ella, se pueden llegar a presentar una variedad de clases o tipos, según el informe pericial informático realizado a la misma prueba, muy útil para resolver casos de múltiples naturalezas, estos casos en donde se aplica el peritaje informático pueden ser: autenticar cualquier tipo de prueba informática de la que se quiere hacer uso en el proceso judicial, defensa de delitos informáticos (contra pericial informática), análisis de discos duros de ordenador o identificación de cualquier indicio informático, aclarar cualquier cuestión técnico-informática que se encuentren en los autos del proceso, pericia en la suplantación de identidad en redes sociales, certificar una imagen con validez judicial. Picón. (2019,11 de febrero) Peritos Ingenieron Informaticos.

Para llegar a obtener esta clase de pruebas periciales informáticas o para que se logre cumplir la finalidad por la cual se solicitó en un juicio, estas deben respetar ciertas características con el manejo que tengan, desde la recolección, análisis y presentación como pueden serla derivación de un proceso valido legalmente, la recolección de datos que se brinda al perito para que pueda ser verificado por el mismo en el proceso pericia, además al ser este tipo de prueba sofisticada y con desarrollo y modificaciones constantes la informática debe preverse de los archivos necesarios para resolver el problema las cuales deben ser resguardado con determinados requisitos, ya que si no se realiza de esta forma podría contaminarse, además se debe hacer énfasis en que este tipo de pericias no siempre es verificable o puede llegar a demostrarse cuando es por medios informáticos debido a su complejidad, es por ello que toda evidencia por más mínima que pueda parecer debe mantenerse bajo un manejo y estudio forense con las medidas necesarias para no ser infiltradas. (Piro, 2016)

2.2.3.2. Tipos o clases de peritajes informáticos.

Dentro de la clasificación de pruebas se cuenta con un listado de pericias informáticas constando de una serie de resguardo por ser clasificadas como tal, teniendo en cuenta que para hacer constar su veracidad debe conllevar una serie de pasos mediante el análisis y la recolección de evidencias e información como antes se ha mencionado, es por ello que este tipo o clases de peritajes informáticos se basan en el desarrollo principalmente en el estudio del peritaje forense digital o tecnológico.

A continuación se presentan los tipos de peritajes informáticos según (Clérigues, 2015-2016):

-Forense Digital o Tecnológico: consiste en obtener evidencias digitales que se encuentren en dispositivos físicos o virtuales. Se realiza un análisis forense en busca de indicios y así aportar como resultado de su investigación un dictamen pericial.

En el peritaje digital o tecnológico se pueden realizar las siguientes actuaciones: identificación y recopilación de evidencias, análisis forense de dispositivos TI, análisis de la información y contenido, trazas y rastros de los ficheros, falsedad y

manipulación de los ficheros, recuperación y reconstrucción información, tratamiento de imágenes y multimedia, ciberseguridad y hacking ético.

-De Gestión o de Management: consiste en la obtención de la información, evaluación y constatación de la misma para poder establecer las relaciones y compromisos contractuales que se originan entre las partes.

-Tasador Tecnológico: consiste en la tasación informática de valorar económicamente determinados activos informáticos mediante distintas técnicas que incluyen el cálculo del retorno de la inversión para algún proyecto informático.

-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, generar un balance de los riesgos en TI (Tecnologías de la Información) y realizar un control de la inversión en un entorno de TI.

-Mediador: Este consiste en permitir el realizar un acercamiento entre las partes en un determinado conflicto para ahorrar tiempo y costos. (p. 31)

2.2.3.3. Herramientas de análisis forense digital.

Ahora en día existen una variedad de herramientas que sirven de apoyo para el análisis a profundidad de los medios informáticos, como pueden ser discos duros, memorias de almacenamientos, infraestructuras de red, software, aparatos móviles con acceso a internet, dispositivos portátiles como Tablet o incluso SmartWatch (reloj digital), entre otros.

Dentro de las herramientas más difíciles que se pueden tener son las de software mediante unidades externas, esto debido al cuidado que se maneja al momento de introducirlas a manera de ejemplo estas pueden ser, memorias USB, DVD, debido a que al ser instaladas en medios portátiles como pueden ser computadoras, Tablet o teléfonos celulares la introducción

del software puede llegar a contaminar la evidencia que contiene el o los dispositivos a analizar.

Pero al lograr sustraer la evidencia es más factible analizar mediante Hardware forenses de tipo sofisticado, estos utilizados en laboratorios tecnológicos forenses por expertos en la materia como peritos informáticos o ingenieros informáticos.

> Dentro de las herramientas más utilizadas en el análisis forense son aquellas que se ocupan de la recopilación de evidencias en la escena del algún delito informático, así mismo el análisis, investigación y presentación de los resultados mediante los siguientes puntos: softwares portables, hardware tecnológico sofisticado, laboratorios forenses, preservación, cadena de custodia, documentación (Clérigues, 2015-2016).

Es por ello que se presenta una serie de herramientas que le sirven de apoyo al perito experto en el tema, para lograr buscar en las evidencias obtenidas y poder así encontrar los hechos bajo el análisis que se realiza durante este proceso; Como antes se ha relacionado este tipo de herramientas son las que trabajan bajo un sistema de actualizaciones constantes que ayudan al perito forense a realizar su investigación.

2.2.3.4. Proceso de obtención.

Uno de los pasos más importantes en el entorno judicial, es la recolección de evidencias y conservación de las mismas, en el caso particular de las evidencias digitales la información almacenada en archivos electrónicos hace que dicha labor sea compleja, ya que por medio de esta se puede llegar a aclarar los hechos, por lo que es necesario saber cuál es el proceso a seguir para su correcta extracción.

Cuando se habla de sustraer la evidencia, en ella se debe llevar un orden adecuado de recopilación sobre la información, si la recolección de datos se realiza de manera correcta y ordenada, es mucho más útil en la detención del ciberdelincuente y, como tal, tiene una posibilidad mucho mayor de ser admisible en un proceso penal.

El procedimiento para la recolección de evidencia varía en cada país, no obstante, se encuentra una guía que puede ayudar a un investigador forense, por lo que para el proceso

obtención se tomará como referencia básica, el modelo de actuación definido por M. Reith y otros. En el cual se deben cumplir los siguientes pasos.

Identificación del incidente.

Consiste en detectar la existencia de un incidente constitutivo de delito producido en un dispositivo digital a través de los indicios existentes (Reith, Carr, & Gunsch, 2002, pág. 13).

Este paso inicial no forma parte del campo forense, pero es importante por su influencia siguientes pasos a seguir.

Preparación del análisis.

Se necesita disponer de herramientas y técnicas necesarias con las que el perito realizará el análisis forense, así como en la obtención de las autorizaciones judiciales que se requieren para ir en búsqueda de la evidencia necesaria. (Reith et al, 2002).

Estrategia de aproximación.

Es la manera de abordar el análisis mediante una buena comprensión de la situación, que permita definir la mejor estrategia de definición de fuentes y procedimientos, teniendo en cuenta la tecnología especifica de qué se trata (Reith et al, 2002, pág. 13).

Cabe mencionar que la estrategia debe tener como finalidad, maximizar la recogida de evidencias digitales que no hayan sufrido alteraciones después del cometimiento de un hecho delictivo.

Preservación de las evidencias.

Su objetivo es asegurar y preservar el estado original de la evidencia existente que se quiere recolectar como los ordenadores y su contenido digital (Reith et al, 2002, pág. 14).

La actividad que se lleva a cabo impide el uso de cualquier dispositivo digital que contenga evidencias, idealmente desde el momento en que se haya producido el incidente digital, evitando su apagado, como el uso de otros dispositivos electromagnéticos, como es el caso de equipos con interfaz WiFi.

Recopilación de evidencias.

Su finalidad es llevar a cabo la grabación de la escena física y el duplicado de las evidencias digitales, por lo que se utiliza para ello procedimientos que hayan sido aceptados y estandarizados, de forma que los jueces puedan confiar en que son fiables y satisfacen los requisitos exigidos. (Reith et al, 2002, pág. 14)

El propósito es preservar las evidencias originales inalteradas y manipular únicamente los duplicados durante su posterior examen y análisis.

Examen.

Se trata de realizar una búsqueda profunda de evidencias que estén relacionadas con el delito cometido que se ha identificado previamente durante el reconocimiento llevado a cabo en el primer paso.

Las evidencias más comunes son, por ejemplo, contraseñas, archivos borrados, tráfico de red, registros del sistema, etc. Suele ser fundamental el establecimiento del timeline (línea de tiempo) de estas evidencias para permitir la reconstrucción histórica de los hechos" (Reith et al, 2002, pág. 15).

Análisis.

En este paso se debe determinar la importancia de cada una de las evidencias sustraídas y establecer las conclusiones basadas en las evidencias encontradas. "La adopción de una teoría que explique el incidente digital ocurrido, puede requerir varias iteraciones sucesivas de actividades de examen y análisis, para llevar a cabo la actividad de análisis puede que no se requieran grandes habilidades técnicas" (Reith et al, 2002, p. 15).

Presentación.

Consiste en detallar con la exhaustividad necesaria el proceso de análisis con los resultados obtenidos desde el punto de vista técnico, de forma que se dote al informe de tal manera que pueda repeler una posible futura impugnación (Reith et al, 2002, pág. 16).

Además, se debe de aportar un resumen, en las conclusiones, con la explicación en términos no técnicos, de los resultados extraídos del análisis de las evidencias y de la reconstrucción de los hechos digitales.

Devolución de las evidencias.

"Consiste en la devolución, en su caso, a los propietarios de los dispositivos físicos, así como de sus contenidos digitales, determinando qué evidencias generadas por el incidente deben ser eliminadas y cómo realizar dicha eliminación" (Reith et al, 2002, pág. 17). Esta devolución también puede ocurrir en el propio acto de adquisición de evidencias, ya que, en ocasiones, no se puede retirar la evidencia por afectar a sistemas de producción. Ejemplo: en el caso de la actividad de identificación el cual se realiza en el primer paso ya que no tiene carácter forense.

2.2.3.5. Protocolo de investigación y análisis de la pericia informática.

Evidencia Digital.

Dentro de la legislación penal salvadoreña, se habla sobre la pertinencia y utilidad de la prueba en su articulado y se establece lo siguiente:

> Art. 177.- Será admisible la prueba que resulte útil para la averiguación de la verdad y pertinente por referirse directa o indirectamente a los hechos y circunstancias objeto del juicio, a la identidad y responsabilidad penal del imputado o a la credibilidad de los testigos o peritos. (Código Procesal Penal, 1996, pág. 55)

La evidencia digital es una nueva modalidad de evidencia que surge por la necesidad actual de buscar la manera de procesar a aquellas personas que cometen delitos de naturaleza informática, ya que a través de esta que se averigua como ocurrió el hecho para contar con los suficientes elementos para enjuiciar a una persona, cumpliendo así con los preceptos del citado artículo 177 del Código Penal.

Tomando en cuenta que el Código Procesal cuenta con un catálogo de medios probatorios dentro de los cuales es posible encontrar la forma de probar los delito informáticos, pero de no ser posible probar un hecho con los medios regulados, el mismo Código da la pauta para probar un hecho delictivo con otro medio probatorio de los no reglados, cuando habla en el artículo 176 de la libertad probatoria (Código Procesal Penal, 1996, pág. 55) dejando en claro que los medios probatorios regulados por la Ley Penal no son taxativos.

Es sobre la base del principio de libertad probatoria, que la evidencia digital puede ser introducida a un proceso penal, aunado a ello, esta también cumple con los elementos de la pertinencia de la prueba en vista que es el medio idóneo para probar la existencia de un delito informático.

La Guía Integral de Empleo de la Informática Forense en el Proceso Penal elaborada por el Laboratorio de Investigación y Desarrollo de Tecnología Informática Forense (Info-Lab), incluye dentro de su texto el Protocolo de Actuación Informático Forense, cuya finalidad es ser un instrumento que cuente con "los aspectos básicos a considerar en las labores de búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales en el proceso penal, a fin de garantizar la validez y eficacia probatoria de dichas actividades" (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense InFo-Lab, Ministerio Público Fiscal Provincia de Buenos Aires. Universidad FASTA., 2016, pág. 9).

En ese mismo orden de ideas el Protocolo de Actuación Informático Forense, considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático (computadoras, celulares, aparatos de video digital, etc.). El referido protocolo también aclara que la evidencia digital es evidencia física, pues sostienen que técnicamente, "es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales" (InFo-Lab. Et al, 2016, Pág. 40).

Según la Constitución (1983), es la Fiscalía General de la República la institución encargada de investigar el delito, pero en una investigación donde el proceso sea de naturaleza informática, el fiscal del caso puede auxiliarse de un perito informático forense para realizar la investigación, en la investigación el perito informático es el especialista en la materia y según Info-Lab. (2016) este especialista puede tener o representar varios roles.

Estos roles según el protocolo son:

Rol de Asesoramiento: En ocasiones, el fiscal o el director de la investigación puede necesitar la opinión de un experto para desarrollar tareas investigativas o probatorias. Por ejemplo, planificar la ejecución de un registro domiciliario y/o evacuar consultas durante el procedimiento, precisar los datos que han de requerirse a un proveedor de servicios, fijar

puntos de pericia o interrogar al perito de la contraparte. Todas estas actividades requieren contar con asesoramiento técnico.

Rol Investigativo: En algunos casos y/o momentos de un proceso, suele requerirse la intervención de un especialista informático para ejecutar medidas de investigación (ej.: secuestro de equipos informáticos, volcados de memoria, obtención de imágenes de disco, etc.).

Rol Pericial: Bajo este rol, el experto aporta sus conocimientos especiales para conocer o apreciar algún hecho o circunstancia pertinentes a la causa.

El protocolo distingue cuatro tipos de especialistas forenses, esto en razón a que cada caso es distinto por consiguiente puede necesitarse de un especialista de distinta área, los especialistas según el protocolo son:

Responsable de Identificación (RI): Persona idónea para las tareas de identificación, no necesariamente es un especialista informático. **Especialista en Recolección (ER):** Persona autorizada, entrenada y calificada para recolectar objetos físicos pasibles de tener evidencia digital. Puede necesitar el auxilio de un Especialista en Adquisición. **Especialista en Adquisición (EA):** Está autorizado, entrenado y calificado para recolectar dispositivos y para adquirir evidencia digital de éstos (ej.: imágenes de disco, volcados de memoria). **Especialista en Evidencia Digital (EED):** Experto que puede realizar las tareas de un Especialista en Adquisición, y además tiene conocimientos específicos, habilidades y aptitudes que le permiten manejar un amplio rango de situaciones técnicas, tales como la realización de una pericia.

Principios generales en el manejo de la evidencia digital.

Los principios son la base que sostienen los cuerpos normativos que rigen los estados, Info-Lab. (2016). Considera dentro de su texto cuatro principios a tomar en cuenta a la hora de realizar una investigación puramente informática, principios que se muestran a continuación:

Relevancia. La evidencia debe ser útil para las necesidades investigativas y/o los puntos probatorios de cada caso concreto. Ha de revestir pertinencia respecto de dichos fines y no ser

sobreabundante o superflua. Este principio opera fundamentalmente como criterio de selección de evidencia. El experto debería saber qué lugar ocupa una determinada evidencia en el plan de investigación penal y/o en la actividad de litigación del Fiscal en cada caso concreto. Ante la duda, o si se estimara que podría ser útil, el especialista debe consultar con el director de la investigación, aportándole su opinión técnica.

Suficiencia. Este principio complementa al anterior. Las evidencias obtenidas y eventualmente analizadas deberían ser suficientes para lograr los fines investigativos buscados mediante ellas, y/o para convencer al tribunal acerca de los puntos para los cuales fueron ofrecidas como prueba. Frente a situaciones dudosas, deberá consultarse con el director de la investigación.

Validez legal. Para que la evidencia sea admisible, debe haber sido obtenida respetando las garantías y formas legales. Por ello el experto debe cumplir con las disposiciones legales y reglamentarias propias de su actuación, cuando una acción impliqué injerencia en derechos fundamentales (secuestro de dispositivos, análisis de comunicaciones personales, etc.), se deberá constatar la previa autorización judicial o la orden del director de la investigación, no debe adoptar decisiones ni llevar a cabo acciones que sean ajenas al área de la propia incumbencia.

Confiabilidad. La evidencia debe ser convincente, apta para probar lo que se pretende con ella. Esto se refiere no sólo a las características que una evidencia digital posee en sí misma, sino también a los procedimientos de obtención, preservación, análisis y presentación ante el tribunal.

Para asegurar que el principio de la confiabilidad se desarrolle correctamente, es preciso que en el proceso de manejo de evidencia digital tome en cuenta los siguientes elementos:

Justificable: Se debe poder justificar todos los métodos y acciones realizadas en el manejo de la posible evidencia digital. La justificación puede darse demostrando que las acciones y métodos utilizados son el mejor curso de acción posible, u otro especialista validar y verificar el proceso realizado.

Auditable: El Especialista en Adquisición (EA) y el Especialista en Evidencia Digital (EED) deben documentar todas las acciones que realizan y justificar todas sus decisiones en las etapas del proceso. Se busca que cualquier especialista externo (consultor o perito de parte)

pueda ser capaz de evaluar el proceso y determinar si se ha aplicado una metodología, técnica o proceso adecuado.

Repetible: Se deben obtener los mismos resultados si se aplica el mismo procedimiento, con las mismas herramientas, en las mismas condiciones, en cualquier momento. Si un EA o EED repite los procedimientos documentados, debe arribar a los mismos resultados que el Especialista que realizó el análisis.

Reproducible: Se deben obtener los mismos resultados si se aplica el mismo procedimiento, con herramientas distintas, en condiciones distintas, en cualquier momento.

De los principios citados y los conceptos extraídos del Protocolo de Actuación Informático Forense, es que se entiende que el procedimiento de actuación cuando se trata de un delito informático no es antojadizo, sino que debe sujetarse a ciertas reglas que orientan el proceder en cada caso concreto.

2.2.3.6. Fases de investigación en la pericia informática.

A través de la fase de investigación, los elementos que deben manejar el avance de la labor del perito son: la no alteración de la prueba y el principio de imparcialidad.

Las fases de la investigación pericial informática tienen mucha relevancia puesto que, a través de estas, se garantiza la prueba dentro de los procesos. Son cinco las fases de investigación de está, y están enfocadas primordialmente en la obtención, procesamiento, análisis y conclusiones de la evidencia digital, estas se desarrollan de forma sucesiva puesto que es preciso agotar una fase para pasar a la siguiente.

Fase de identificación.

> Se basa en la identificación de los equipos, dispositivos y todo otro tipo de medio de almacenamiento cuya obtención y/o examen se considere pertinente y útil para aspectos específicos del plan de investigación penal delineado en un caso concreto por el Fiscal y/o su equipo. Dicho proceso de trabajo suele ser necesario en investigaciones o etapas investigativas de carácter planificable.
>
> (Info-Lab. Et al, 2016, p.13).

En esta etapa se debe realizar la organización y determinación en cómo se orientará la misma, es por ello que el perito debe tomar en cuenta los siguientes elementos:

Revisar el contexto legal (ya que el hecho de que no se considere un proceso penal, no implica que se deba obviar que durante el proceso de investigación se pueda

vulnerar la legislación vigente) que afecta al escenario, dispositivo, elemento o información que se va a analizar. Solicitar las autorizaciones necesarias, así como información referente a cuáles son los prerrequisitos, sobre qué se debe actuar, quién debe intervenir, quién puede estar presente y cuál es el límite de la actuación.

Planificar la investigación e identificar las herramientas y los medios (hardware y software) así como los procedimientos, y los conocimientos necesarios para realizar una actuación profesional.

Identificar si la información existe en los dispositivos o debe ser capturada en el proceso de la investigación (por ejemplo el tráfico en la red 'online' origen y destino de las comunicaciones).

Identificar unitariamente los medios y bienes involucrados susceptibles de contener cualquier tipo de información o evidencia relevante. No solo los dispositivos telemáticos sino también aquella documentación que pudiera contener información susceptible o afín.

La descripción de los dispositivos: qué son cada uno de ellos, qué identificaciones existen en el dispositivo y cuáles proceden del fabricante o distribuidor, tipo de dispositivo, los posibles usos y utilidades de cada dispositivo para qué, quién, cuándo, dónde, con qué frecuencia, etc. (Jerez, 2015, pág. 24).

Es por ello, que para que se cumpla plenamente esta fase, el perito debe de tener en cuenta ciertos requisitos, considerando que esta etapa es fundamental ya que, dará apertura a la investigación, identificando todos aquellos dispositivos que han sido encontrado en la escena del hecho delictivo o que se tuviera sospecha que han sido un medio necesario para la realización de un delito.

Fase de recopilación.

En esta etapa estará sujeta:

Toda evidencia que se tome o incaute debe ir perfecta e individualmente identificada, y debe quedar perfectamente documentado el origen de cada elemento de la

> investigación. En ocasiones, la recopilación ha de hacerse utilizando medios especializados para garantizar que la información perdure en el tiempo y no sea destruida, como en el caso de las investigaciones forenses de la memoria RAM. (Aguilar, 2015, parrá 5).

Sin embargo, en los diversos casos existe tan solo una única ocasión de capturar la información, es por ello, que se debe perpetrar de forma oportuna y con suficiente reserva para comprobar su obtención, para el realizar dicha operación se debe que tomar en cuenta dos requisitos fundamentales:

1. Respetar la organización de privilegio según la volatilidad de la información.
2. Ser metódico, tomando en cuenta los procesos en la investigación.

Durante la recopilación se tiene que ser sumamente cauteloso y cerciorarse de trabajar internamente en los escenarios y requisitos de legales que requieren ciertas situaciones.

Fase de preservación.

El elemento principal en esta fase es:

> Realizar una imagen exacta del contenido de la evidencia, asignando un código único correspondiente a una combinación única de bytes que constituye la totalidad del medio en observación. Dicho código debe ser complejo para evitar que sea alterada la información rescatada; el código asignado solo el personal autorizado debe manipularlo para seguridad y protección del mismo, con el fin de crear una cadena de custodia consistente. (Jojoa, 2014, parrá. 3).

Las labores de preservación tienen como objeto la capacidad de una copia igual y completa de los datos incluidos en los dispositivos a investigar, también son llamadas imagen de disco.

Uno de los requisitos de una investigación plena es que debe de ser repetible, y si no se dispone de la posibilidad de reproducir la situación de partida de forma íntegra, es imposible cumplir con el requisito.

Fase de análisis.

Tiene como objetivo el de reformar todos los datos disponibles del ataque, estipulando la cadena de hechos es decir, desde el inicio del ataque, hasta el momento de su descubrimiento.

Por esa razón, se da la pauta de que "existen procedimientos genéricos para soportar las técnicas de análisis y búsquedas de evidencias particulares y específicas de la investigación que se esté llevando a cabo. Estos procedimientos técnicos facilitan las pautas para realizar el análisis" (Jerez, 2015, pág. 26)

Sin embargo, a través de esta fase se llega a sustraer los datos que integran la información que, a su vez, tras ser estudiada y situada, se da respuesta a los asuntos que plantean las investigaciones.

Por otro lado, otra de las funciones del análisis, es la obtención de la información que no es visible de los ficheros, como los metadatos, puesto que utilidad ha sido comprobada empíricamente en varios casos ya que ha permitido conocer cuál ha sido el ciclo de vida del mismo, fechas/horas, autoría de la creación, accesos, modificaciones entre otros datos.

Fase de presentación.

A través del análisis de la información y las evidencias, el perito informático deberá establecer una conclusión. Esta conclusión debe quedar plasmada en un informe claro, preciso y entendible por terceros que no son conocedores en la materia, con autodeterminación, es decir, que el informe tenga carácter judicial o extrajudicial.

> Durante que durante la reunión de entrega del informe al peticionario o gestor del encargo se da una explicación sobre el contenido del informe y se aclaran las dudas pertinentes, en caso de que surjan. Esto facilitará en gran medida la comprensión del contenido del mismo por los interesados. (Jerez, 2015, pág. 28)

Es por ello, que el informe deberá presentar las formalidades legales siendo riguroso, previsor y sobre todo dando el razonamiento respectivo. Sin embargo, es responsabilidad del perito informático conservar copia de todo lo necesario, manipulando los medios que garanticen la integridad y confiabilidad de estas para poder, en un momento, rememorar todo el proceso y las actuaciones, siendo capaz de realizar una exposición o dar las pertinentes explicaciones que le sean solicitadas.

2.2.3.7. Cadena de custodia de las evidencias digitales.

Por cadena de custodia se entiende a una serie de requisitos, que cuando sea procedente deben observarse para demostrar la autenticidad de los objetos y documentos relacionados a

un hecho delictivo que inicia a partir de la recolección de las evidencias, embalaje, transporte, análisis y su custodia, hasta su valoración en el juicio (Sandoval, 2018).

Sin embargo, este tipo de proceso se llevara a cabo en el transcurso de los juicios penales, tomando mayor importancia cuando en la escena del delito se encuentran las evidencias y son embaladas para su custodia y transporte conforme se desarrollen las etapas del proceso y para la práctica de las experticias o pericias que deba practicársele a la evidencia, la cadena de custodia toma relevancia por el resguardo que se le da a la evidencia y su finalidad primordial es garantizar que la evidencia encontrada en la escena del delito es la misma que se vierte en juicio.

De tal forma que, para que este proceso sea válido la evidencia debe ser recogida, embalada y etiquetada adecuadamente, tener una conservación adecuada, un transporte idóneo y que la entrega de la misma sea apropiada (Sandoval, 2018).

Es por ello, que para que se dé la validez de la cadena de custodia no solo se debe de cumplir con los requisitos antes mencionados, sino que también realizar todos los pasos para la plena ejecución de está, siendo su primer paso los hallazgos y la protección en la escena del delito, la búsqueda mediante la inspección preliminar, la fijación mediante acta, fotografía, croquis o video, recolección, embalaje, custodia de evidencias, transporte y entrega, análisis pericial, presentación en juicio, devolución, destrucción o comiso para fines de beneficio de instituciones.

A pesar del desenvolvimiento de cada una de las fases de la cadena de custodia, los garantes de recoger los materiales y evidencias deben aprobar que estos sean enviados junto con el respectivo formato de cadena de custodia, además, deben efectuar el estudio del embalaje de los mismos con el único fin de observar si se muestra alguna alteración o modificación tanto en el embalaje como en los rótulos o etiquetas, donde consta la evidencia.

2.2.3.8. Pilares fundamentales para valorar la prueba pericial informática.

El Protocolo de Actuación Informático Forense ya abordado en la temática, habla sobre principios a tomar en cuenta para la obtención de la prueba, ahora bien cuando está ya se ha obtenido corresponde al juez su valoración y para realizar dicha acción este debe valerse de ciertos pilares que se consideran fundamentales porque no pueden faltar en ningún momento cuando se valore prueba digital.

Cuando corresponda al juzgador valorar, el juez aplicara la reglas de la sana critica para "determinar la credibilidad del testigo, la razonabilidad de las máximas de experiencia aportadas por el perito y su aplicación al caso concreto, o si el documento es auténtico y refleja los hechos ocurridos en la realidad". (Llunch, 2014, pág. 2). Es por ello, que a través de este sistema de valoración el juez deberá de motivar su decisión de su sentencia o su fallo, dando ventaja a las partes ya que podrán controlar el proceso.

Pese a que, "la ley no le exige al Juez a tener por comprobados los hechos que establece recoge una prueba electrónica (salvo en el supuesto de documentos públicos electrónicos)" (Signaturit, 2017, parrá 13). Sin embargo, está extenderá sus efectos para avalar el hecho que se discute, pero su validez será concedida por el juez bajo las reglas de la sana crítica. Por esa razón, en la evidencia digital para que el juez pueda valorar plenamente, está debe de contar con ciertos elementos de los cuales podemos mencionar la licitud, autenticidad, integridad y exactitud.

Licitud

Al momento de presentar la evidencia digital, esta no debe de transgredir derechos fundamentales como el derecho a la intimidad ya que, si los vulnerará estaríamos en presencia de una prueba nula de pleno derecho. (Guardiola, 2017)

Autenticidad

Es de suma importancia avalar la autenticidad de un instrumento, puesto que se debe mostrar que el supuesto autor es el que corresponde con el autor real, manifestando que se trata de la misma persona, legitimando el origen de los datos y el origen de los mismos. (Guardiola, 2017)

No obstante, cuando se diera indicio que llevan a poner en tela de juicio al Juez en su autenticidad, este tendrá la potestad de negar la fuerza probatoria de la misma, puesto que, existe la duda.

Integridad y exactitud

La integridad se refiere que la prueba no ha sido adulterada, desde el momento de su sustracción hasta el momento de su atribución en juicio.

Es por ello, que para cumplir este elemento, se debe de respetar la cadena de custodia ya que, a través de esta se garantizara su identidad, integridad y autenticidad de la evidencia puesto que, por medio de esta estableceremos el hecho que se pretende probar.

Sin embargo, "el juez la estudiará según su libre valoración**,** aunque siguiendo las reglas del criterio racional. Este es el sistema establecido para la prueba electrónica" (Signaturit, 2017, parrá. 12). Si surgen sospechas de la autenticidad y/o integridad de los datos es posible que el juez termine entorpeciendo la eficacia de ella.

Por lo tanto, en la valoración el juez este debe tener en cuenta el aporte de las partes en relacionadas con la prueba electrónica incluida en el proceso, especialmente si la parte contraria refuta su validez, esta impugnación deberá tener un argumento, es decir no se impugnará solo porque la resolución dictada por el juez afecta a los intereses de la parte, sino porque existen elementos aptos para fundar el recurso que se pretenda presentar.

En consecuencia, si no se manifiesta tal impugnación el juez podrá considerarla como autentica y exacta.

2.2.3.9. Proceso de validación.

Si bien, "la validez de la prueba tiene íntima relación con el debido proceso" (Molina, 2008, pág. 168). Para que esta sea admitida dentro del proceso está, debe de respetar las garantías procesales y los requisitos legales que establece en la ley secundaria.

No obstante, al momento de la valoración, los que intervienen en un proceso, tienen la posición ius fundamental de instar que la prueba relacionada tenga validez y que después el juez instituya su cabida demostrativa.

> La parte que se ve afectada ya sea en su interés o en sus derechos fundamentales con algún medio probatorio, le asiste el derecho de solicitar los mecanismos procesales de exclusión de las que no cumplan con los presupuestos de validez. (Molina, 2008, pág. 169).

Sin embargo, en la pericia informática para que esta obtenga su validez plena debe de cumplir no solo con los requisitos legales si no también al momento de la realización de la cadena de custodia esta no debe ser vulnerada en el acto de recolectar la evidencia digital puesto que, corre el riesgo de ser manipulada ya que, es realizada a dispositivos informáticos y a los datos contenidos en ellos.

Es por ello, que para que se cumpla de forma correcta la cadena de custodia, se estudiara su integridad, y para eso el equipo de investigación deberá de ver la validez de la prueba desde tres puntos:

a) Validez técnico-informática: trata de estudiar el control, revisión y auditoría de las operaciones técnicas informáticas, que son realizadas desde la identificación de la evidencia digital recolectada hasta la fase del análisis.

b) Validación técnico-criminalística: es el aquel control, revisión y auditoría de todas las operaciones técnicas relacionada con la criminalística, elaboradas desde la toma de contacto, de los actores participantes en la tarea analizada, es decir desde que se involucran con la problemática pericial propuesta.

c) Validación técnico-legal: se trata del análisis integrador de la prueba indiciaria informática recolectada y disponible, a efectos de determinar su confiabilidad probatoria legal. (Info-Lab. Et al, 2016, p.72).

Por lo tanto, si dentro de la elaboración de la cadena de custodia se respeta con todo el procedimiento que se establece con antelación, acatando la garantías y derechos procesales para evitar que manen irregularidades probatorias que puedan poner no solo en riesgo la validez de dicha prueba si no fundar consecuencia sobre la errónea valoración del funcionario judicial dictando una sentencia inexacta y aplicando una equivocada administración de justicia.

2.2.3.10. Problemas de la cadena de custodia en la pruebapericial informática.

La cadena de custodia, tiene como finalidad, no viciar el manejo de los medios probatorios obtenidos, y de esta forma evitar la manipulación, contaminación, alteración, daños, reemplazos, o destrucción.

Al visualizar este tópico cómo problemas se pueden tomar como ejemplo: un ordenador o dispositivo incautado por la policía y encendido en el lugar que se llevó acabo la incautación para la sustracción de información, ya que no se está en presencia de un equipo que se encuentre en funcionamiento, donde la información está siendo procesada, pudiendo implicar la pérdida de información y la destrucción de la prueba informática pretendida (Arellano , 2012). Por lo que ya no es una prueba en la que se pueda considerar que se haya conservado la cadena de custodia, por no existir riesgo en la perdida de información, debido a que el sistema operativo pudo haber sido modificado así como accedido a determinados ficheros, puesto que cualquier fichero o documento informático es susceptible de ser alterado.

No embalar correctamente la evidencia recolectada, ni documentar que la evidencia digital en el momento de su resguardo o traslado sufrió alguna modificación o alteración, es una evidente vulneración a la cadena de custodia, asimismo delegar a un miembro que no presenció la forma de obtención de la evidencia, a elaborar el acta y que este firme dando fe del contenido de la misma; esto no solo es ilegal, además rompe la cadena; así mismo con esta acción se encuentra en las fronteras de la falsedad ideológica (Sandoval, 2018) .

Problemas en cuanto al transporte de la evidencia digital.

Al momento de transportar la evidencia, algunos de los problemas que se pueden presentar son como el transporte de las evidencias al Laboratorio Forense sin embalajes externos, sellado o rotulado y el traslado de la evidencia en medios inadecuados ya que de esta forma se puede dañar el ordenador o dispositivos y perder así la evidencia (Sandoval, 2018).

Problemas en razón al almacenaje de la evidencia digital.

Almacenamiento de la evidencia en lugares no controlados, es decir en lugares de acceso libre. Entrega no controlada: en el proceso de transporte o traslado no se logra determinar a donde estuvo la evidencia, en que tiempo y por qué, aquí podría cuestionarse si estuvo perdida, si fue alterada entre otros.

La forma más frecuente de romper la cadena de custodia es violando los sellos del embalaje de las evidencias recolectadas (antes de ser analizadas) y las ya analizadas, que en los formatos no se encuentran descritas las evidencias o que no coinciden con la descripción

del acta policial, entre otros. De acuerdo a especificaciones técnicas, el romper la Cadena de Custodia con lleva desestimar la prueba científica, es decir que no se toma como elemento probatorio de un hecho delictivo. Respecto al quebrantamiento de la cadena de custodia existe pronunciamiento por los tribunales de sentencia, que él no dejar constancia que quienes y como se protegió la evidencia es conducente del rompimiento de cadena y en consecuencia improductivo valorar la prueba (Sandoval, 2018).

Problemas en la obtención de la evidencia digital.

Mantener la integridad de la evidencia digital a lo largo de un proceso presenta diferentes problemas en el manejo de equipos de hardware y sus correspondientes archivos de datos, siendo uno de los problemas la extremada complejidad de las redes de computo, el alarmante tamaño de los archivos de computo tanto de datos como multimedia así como las bases de datos (Buriticá, 2003).

Los problemas que surgen desde el momento de la recolección de la evidencia informática pueden ser: la Volatilidad de la evidencia digital dado que la prueba se puede borrar, perder y alterar, esta incluso antes de recolectar la evidencia, ya que pudo haber sido modificada por el autor, se han visto casos en que se ha alterado la información de la maquina portadora de la prueba después de que se ha obtenido la evidencia, perdiendo la garantía que no ha sido manipulada, por lo que se dificulta corroborarla con el original, teniendo como consecuencia que el juzgador no puede estar completamente seguro de que el archivo o mensaje de datos que se le muestra no ha sido manipulado por el receptor (Buriticá, 2003).

El almacenamiento del medio electrónico, ya que el documento o archivo al que se quiere ingresar puede que contenga en ella códigos encriptados lo que conlleva a que no se pueda conocer su contenido y si se logra ingresar no es suficiente para determinar la integridad de la información obtenida en un estudio de ciencias forenses (Buriticá, 2003).

Problemas en el transporte que podrían alterar la evidencia recolectada, debido a que este tipo de evidencia es delicada y puede darse el caso que al momento de incautar un ordenador o dispositivo, este se encuentre en funcionamiento dificultando el resguardo e integridad de la prueba, ya que al momento de trasladar el ordenador o dispositivo electrónico, la información se puede perder o sufrir cambios, el mismo riesgo se presenta si se apaga el dispositivo, haciendo que la prueba carezca de veracidad (Buriticá, 2003).

Identificación del autor, ya que puede darse el caso que el hecho delictivo se realice dentro de un centro de computación y por ser de libre acceso para todas las personas se dificulta en individualizar al autor. (Buriticá, 2003)

Por último la falta de expertos versados en dicho campo teniendo como consecuencia el desconocimiento de las técnicas utilizadas para la intrusión a sistemas de información o inscripción de datos. Cuando los peritos de los organismos encargados de la aplicación de la ley acceden directamente a las pruebas electrónicas decomisadas sin hacer en primer lugar una copia imagen de los datos, el acceso a las pruebas y su visualización quedan registrados. El acceso directo puede complicar en gran medida el proceso de validación de las pruebas para presentarlas ante los tribunales, porque en este caso los funcionarios de las fuerzas del orden deben demostrar o probar que el acceso directo que efectuaron no afectó materialmente a la finalidad de las pruebas. (Buriticá, 2003)

Debido a lo anterior resulta relevante el análisis de legalidad de obtención de evidencias digitales, pues permite considerar que la evidencia digital pudo ser modificada. En este sentido, se podría decir que hubo un rompimiento de la cadena de custodia y en consecuencia, se vulneró el principio de legalidad de la prueba, lo que debería conllevar a la exclusión probatoria de todos los elementos probatorios así obtenidos y los derivados de estos.

2.2.3.11. Problemas sobre valoración de la pericia informática, como prueba.

Teniendo en cuenta que la prueba como tal, consiste en la búsqueda de la verdad real y objetiva, con la que se confirma o desvirtúa una hipótesis o una afirmación, siendo este el medio pertinente y útil para descubrir la verdad y así tener una garantía contra la arbitrariedad de las decisiones judiciales, se sabe que la prueba surge de las evidencias que los hechos pudieron haber dejado ya sea en cosas o personas, buscando con ella es la reconstrucción de los hechos que son objeto de investigación para lograr que sea comprobable y demostrable, por lo que será relevante y útil cuando produzca certeza de la existencia o no del hecho que se pretende acreditar, como cuando sea utilizada como fundamento para una resolución.

El primer principio del derecho procesal penal es el de Juicio Previo, el cual sostiene que ninguna persona puede ser condenada a una pena ni sometida a una medida de seguridad sino mediante una sentencia firme, por lo que debe existir un justo juicio, el cual se logra en gran parte gracias a la prueba aportada (Vélez, 2001). En ese sentido y teniendo establecido la

importancia de la prueba dentro de un proceso, se hace entonces necesario establecer con qué problemas se puede encontrar a la hora de valorar la pericia informática como prueba ya que esto influye en gran magnitud a la hora de resolver en una Sentencia Judicial.

Los problemas se amplían en el análisis de las evidencias digitales recolectadas, ya que al momento de hacer el informe pericial, pueda ser que contenga buenos fundamentos los cuales van acompañados de unas malas conclusiones por parte del perito informático o si el perito no parece seguro de sus conclusiones, el dictamen no puede tener eficacia probatoria, esto influenciado por la poca formación de profesionales en esta área haciendo que sea más fácil que esto suceda (Vélez, 2001).

Es posible que el juez, a quien le corresponde apreciar estos aspectos de la prueba, no tenga una preparación adecuada para la valoración de este tipo de evidencias, por lo que el juzgador utiliza la experiencia y la lógica para valorar la prueba incorporada, por tal razón si considera que las conclusiones del perito contrarían normas generales de la experiencia o de lógica, o que son contradictorias, o que no encuentran respaldo suficiente en los fundamentos del dictamen, puede rechazarlo, aunque emane de dos peritos en perfecto acuerdo.

Por otra parte, no basta que el informe de los peritos sea claro y firme, como consecuencia lógica de sus fundamentos o motivaciones, porque el perito puede exponer con claridad y firmeza una tesis equivocada, por lo que debe estar debidamente entrenado para sustraer y manejar la evidencia que se pretende incorporar obteniendo una valoración adecuada, ya que en este tipo de pericias existe también la facilidad de modificar la prueba.

Debido a lo anterior existe un verdadero problema al momento de evaluar el informe otorgado por un perito informático, ya que ni el perito como el Juzgador están debidamente capacitados y preparados para dar plena seguridad y garantía que se valorara la prueba informática de manera adecuada volviéndolo atentatorio para las partes que intervienen en un proceso penal.

2.2.3.12. Consecuencias de la falta de homogeneización sobre protocolo de investigación en la sentencia.

La evidencia digital está sujeta a riesgos específicos de posibles alteraciones, debido a su fragilidad es necesario un protocolo de investigación, donde se integre la dimensión técnica en sus contextos jurídico, estratégico y organizacional. En El Salvador no existe un protocolo público aceptado, en cuanto a las actuaciones que se realizan al momento de investigar un delito informático y el tratamiento de la evidencia digital, por lo que la falta de homogeneización sobre protocolo de investigación genera las siguientes consecuencias:

Incertidumbre sobre aspectos técnicos en el proceso de recuperación de la información.

No existe ninguna garantía sobre si el proceso o método que se utiliza en la recuperación de la información en los medios de almacenamiento sea el correcto, tampoco se puede asegurar que se han realizado todas las tareas posibles con los mecanismos adecuados.

A ejemplo de esto se puede mencionar lo sucedido en el caso donde se procesó al ex Fiscal General de la Republica y 3 personas más, por los delitos de fraude procesal y falsedad ideológica, a quienes se les incautaron una laptop, celular y Tablet en 2016, y a más de un año de haber incautado esos medios de almacenamiento el perito de la Policía Nacional Civil no presento informe de vaciado de los dispositivos electrónicos. Por lo que el juez cita al perito y este al momento de presentarse manifiesta que no pudo extraer la información debido a que el software utilizado en la PNC era 2008 y no era compatible con algunos dispositivos incautados, y que la laptop lanzaba alerta de virus en el momento del procedimiento.

El juez octavo de instrucción amplió el plazo para que peritos de la FGR, extrajeran la información de los dispositivos y en efecto una perito si pudo realizarlo sin encontrar los problemas de virus o de compatibilidad con el software, quedando en evidencia el informe presentado por el perito de la PNC. (La Prensa Grafica, 2018)

Dudas sobre la validez legal de las actividades investigativas y periciales en los delitos informáticos.

Debido a que no existe un protocolo de investigación público en El Salvador, los peritos utilizan otra metodología, que podría cumplir o no, con los estándares legales del país. “Son muchos los derechos y garantías que pueden verse afectados mediante la labor informático forense” (InFo-Lab. Et al, 2016, p. 64-65) y por esta razón es que se debe minimizar las afectaciones de derechos de las partes al momento de investigar, y esto se lograría creando un

protocolo que vaya de la mano con los estándares adoptados por los organismos de justicia del país.

Inadecuada administración de justicia penal.

Si existe incertidumbre sobre los aspectos técnicos en el proceso de recuperación de la información y también dudas sobre la validez legal de las actividades investigativas y periciales lo más probable es que el juzgador realice una inadecuada administración de justicia penal. Esto es porque el juez no tendrá la certeza de que la prueba es verosímil, y existirán problemas al momento de valorarla, lo que podría arribar en absolver un culpable, o condenar a un inocente.

Cabe mencionar que la validez legal y la calidad técnica son condiciones necesarias, pero no suficientes, para lograr las metas buscadas. La dimensión estratégica no debe dejarse de lado.

El Estado debe organizarse para articular un sinnúmero de actividades en las que suelen intervenir diversos actores como: la priorización de determinados tipos de problemáticas político criminales (que se traduce en la asignación diferencial de recursos), la elección de la modalidad de abordaje más adecuada a cada caso, la planificación y ejecución eficaz de las variadas labores de investigación y litigación, (Aquí es donde debe integrarse la actividad informático forense.) capacitación y aprendizaje organizacional. (InFo-Lab. Et al, 2016)

Por estas razones es necesario un protocolo de investigación, que sea público, aplicado por peritos de PNC Y FGR, y que los abogados defensores y jueces también conozcan de este, así el juez podría cuestionar el curso de la investigación, o determinar con certeza si la prueba se preservo correctamente. Un protocolo de investigación brindará la garantía sobre el proceso técnico, y buscaría la aplicación de estrategias organizativas es decir, no habría dudas sobre si los mecanismos o herramientas utilizadas fueron las correctas, y la fase de identificación de la evidencia digital recolectada, hasta el análisis seria del conocimiento de los sujetos determinantes.

2.3 Marco normativo.

2.3.1. Marco jurídico nacional.

2.3.1.1. Definición de Constitución.

Según el diccionario de Guillermo Cabanellas (1993) Constitución es "Acto o decreto fundamental en que están determinados los derechos de una nación" (Pág. 71) es sobre la base de lo dicho por Cabanellas que se sostiene que Constitución es la ley fundamental donde radican una serie de principios fundamentales que rigen el derecho, asimismo esta contiene las garantías mínimas y derechos fundamentales de todos los salvadoreños que se deben respetar en todo momento.

Según el Art. 1 de la Constitución, el Estado reconoce a la persona humana como aquella en base a quien se creó la ley, y asimismo menciona que es la persona humana el fin de la ley, en otras palabras el Estado se creó por y para la persona humana (Constitución, 1983). El Estado debe garantizar según el artículo citado la Justicia, Seguridad Jurídica y el Bien Común, y es por ello que se sostiene que protección de la persona humana la finalidad del Estado.

2.3.1.2. Garantías constitucionales.

Juicio previo: La Constitución de El Salvador reconoce esta garantía fundamental en el artículo 12, en esencia nadie puede ser declarado culpable sin antes haber sido oído y vencido en juicio (Constitución, 1983). Es decir que previo a la declaratoria de culpabilidad de una persona esta debe ser sometida a un proceso penal donde se le aseguren los elementos mínimos para su defensa, esto le permitirá contrariar o expresar su oposición frente a aquel que lo acusa.

Esta garantía constitucional también es desarrollada en el Art.1 del Código Procesal Penal y está orientada en el sentido que para que a una persona se le imponga una pena o medida se seguridad primero se deben haber probado los hechos y circunstancias que se alegan en su contra, en un proceso penal donde sea asistido ya sea de un abogado particular o un defensor público de la Procuraduría General de la República que ejerza su defensa técnica en el juicio (Código Procesal Penal, 1996).

Obligación de probar: Por mandato constitucional es la Fiscalía el ente encargado de investigar y promover la acción penal (Constitución, 1983), asimismo como consecuencia de

los primeros le nace la obligación de probar los hechos que alega en un juicio, esto sobre la base del art 193 numerales 3 y 4 Cn.

"La obligación de probar lo alegado, corresponde a la parte que afirma, en virtud del principio latino actori incumbit onus probandi" (al actor le incumbe la carga de la prueba) (Caballena de Torres, 1993, pág. 48). Hay que tener claro que la carga de la prueba corresponde a la parte que acusa, pero para que el procesado se encuentre verdaderamente en igualdad de condiciones con el acusador, se le permite aportar pruebas a través de su defensa técnica y también en el ejercicio de su defensa material (Código Procesal Penal, 1996).

Hábeas data: El hábeas data nace sobre la base del Art. 2 inc. 2 Cn., "viene a ser un término relativamente reciente en El Salvador, naciendo como consecuencia del sostenido avance de las nuevas tecnologías y particularmente de la Informática, configurándose como un mecanismo consagrado como garantía Constitucional" (Herrera Mejía, 2012, pág. 39).

Tomando en cuenta que la disposición citada anuncia la protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen, el habeas data se enfoca en asegurar cumplir estos preceptos constitucionales, pudiendo ser procesable vía amparo según el Art. 247 Cn, en vista que es procedente solicitar el amparo por violación a los derechos que la constitución reconoce (Constitución, 1983). Y siendo el habeas data un derecho fundamental es tutelable el amparo.

En ese orden de ideas con la creación de la Ley Especial Contra los Delitos Informáticos y Conexos, en el salvador se busca crear otra forma de protección para los derechos de la intimidad y el honor. Esto en razón a que este cuerpo legal considera las infracciones contra estos derechos como delitos.

Comunicaciones: Cuando se habla de la intervención de las llamadas telefónicas que regula el artículo 24 inc. 2 Cn., esto solo puede ocurrir en casos excepcionales pues por regla general están prohibidas por ir en contra del derecho a la intimidad personal que regula el Art. 2 Cn.

En ese mismo orden de ideas cuando se pretenda realizar una intervención telefónica se debe solicitar por escrito al juez competente su autorización, dicho escrito debe contener las razones que motivan la intervención (Ley Especial para la Intervención de las Telecomunicaciones, 2010), es decir se deben expresar los argumentos y fundamentos que

justifiquen dicha acción, tomando en cuenta que esta no podrá ser de carácter permanente sino temporal sobre la base del artículo 1 de la LEIT.

2.3.1.3. Leyes secundarias.

Código penal.

El aumento de los ciberdelitos es incuestionable que ha llegado hasta nuestras fronteras, sin embargo, lo que hizo necesaria la regulación de este tipo de conductas delictivas, fue hasta finales de los años 90 que El Salvador a través de la creación del Código Penal publicado en el Diario Oficial No. 105 Decreto 1030 emitida el 26 de abril de 1997, empezó a regular estos tipos de delitos de forma genérica, algunos delitos que contempla hasta hoy en día son: La Injuria, La Calumnia, La Difamación, La pornografía, La estafa y los delitos contra la Intimidad. (Fundación Salvadoreña para el Desarrollo Económico y Social [FUSADES], 2016 p. 1). Cometidos a través de los medios informáticos.

En relación de lo anterior, se promovieron otras leyes como de la Ley de Telecomunicaciones "Decreto Legislativo No. 142. Diario Oficial No. 218, Tomo 337, 21/11/1997" (SIGET, 2014, parrá. 12) y la Ley de Acceso a la Información Pública normas que iban de la mano con dicho código para poder regular de forma plena estos delitos.

A pesar de ello, estos instrumentos jurídicos no fueron lo suficiente para poder normar la ciberdelincuencia puesto que, el Código Penal no lograba cumplir su función de sancionar tales conductas ya que, no las contemplaba en su totalidad convirtiéndolas en conductas atípicas surgió entonces la necesidad de crea una ley especial que pudiera abarcar no solo los delitos ya regulados por la ley penal si no, aquellos delitos cometidos por medio de las Tecnologías de la Información y la Comunicación (TIC) que habían quedado por fuera del ordenamiento jurídico ante la evolución de las Tecnologías.

Ley Especial Contra los Delitos Informáticos y Conexos.

La Ley Especial Contra los Delitos Informáticos y Conexos (LEDIC) fue aprobada "el 04 de febrero del año 2016" (Asamblea Legislativa de la República de El Salvador, 2016, pág. 13). Ante la creación de esta ley surgieron demasiados retos ya que, si bien la referida norma acoge la mayoría de los ciberdelitos, no cuenta con la parte procedimental dejando un gran vacío legal respecto al tratamiento de estas conductas, referente a las pruebas con los cuales

se demostrará el hecho delictivo, trayendo como consecuencias no solo la impunidad de los delitos si no la mala administración judicial, si el Estado no hace un esfuerzo por divulgar dicha ley, ésta corre el riesgo de ser letra muerta.

Código Procesal Penal.

A pesar de la falencia que contiene la Ley Especial al no establecer el proceso de los de los delitos informáticos, hoy en día estas conductas se procesan a través de lo que regula el Código Procesal Penal a pesar de lo dicho, se sabe que la prueba idónea para estos tipos de delitos es la prueba pericial informática, que el Código no regula de forma expresa los requisitos fundamentales para la validez de la pericia, ya que, solo se manifiesta en el capítulo IV "peritos" del Código Procesal Penal , no hace mención especial de los peritos informáticos es por ello, que la referente ley queda corta para la aplicación en un delito informático ya que, tampoco no cuenta con una sección especial en la que establezca los parámetros legales para la obtención, preservación y tratamiento en relación a la evidencia digital.

Aunado a lo anterior, ante la falta de regulación de los delitos informáticos esto trae aparejada no solo arbitrariedades sino posibles irregularidades procesales puesto que se sabe, que la cadena de custodia juega un papel importante procesalmente pues por medio de esta como lo establece el artículo 250 Pr.Pn., se puede demostrar "… la autenticidad de los objetos y documentos relacionado en un hecho delictivo" (PR.PN, 1996, p.269). La cadena de custodia en relación a la ciberdelincuencia comprende otros aspectos técnicos más específicos que no está contenida en el Código Procesal Penal. (Medrano, 2017).

Es por ello, que por todos estos vacíos legales se dan caso como el de "troll center" en las que fueron atacados los sitios web de los principales periódicos del El Salvador y al curso del proceso judicial se demostró las debilidades al no valorar pruebas que indican la comisión del delito. (La prensa Grafica, 2018). Casos como estos reflejan la realidad en El Salvador en cuanto al mal tratamiento de los ciberdelitos por la falta de conocimiento técnico por parte de los funcionarios además, la carencia de un ordenamiento jurídico especial que regule el proceso y las herramientas para poder resolverlos y así dar una buena administración de justicia.

2.3.2. Marco jurídico internacional.

En el artículo 144 de la Constitución de la República, expresa:

> Los Tratados Internacionales celebrados por El Salvador con otros estados o con organismos internacionales, constituyen leyes de la República al entrar en vigencia, conforme a las disposiciones del mismo tratado y de esta Constitución. La ley no podrá modificar o derogar lo acordado en un tratado vigente para El Salvador. En caso de conflicto entre el tratado y la ley, prevalecerá el tratado. (Constitución de la República de El Salvador, 2014, art. 144).

Por lo tanto los tratados que el país suscribe y posteriormente ratifica se vuelven leyes de la República.

Convención Americana sobre Derechos Humanos.

También se conoce como "PACTO SAN JOSE", suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos, realizada en San José Costa Rica, del 7 al 22 de noviembre de 1969.En El Salvador esta convención entró en vigencia el 15 de junio de 1978. En ella se reconocen y se protegen derechos esenciales del hombre.

En el artículo 8 se regulan las Garantías Judiciales, y se establece que:

> 1. Toda persona tiene derecho a ser oída, con las debidas garantías y dentro de un plazo razonable, por un juez o tribunal competente, independiente e imparcial, establecido con anterioridad por la ley en la sustanciación de cualquier acusación penal formulada contra ella, o para la determinación de sus derechos y obligaciones de orden civil, laboral, fiscal o de cualquier otro carácter.
>
> 2. Toda persona inculpada de delito tiene derecho a que se presuma su inocencia mientras no se establezca legalmente su culpabilidad. (Convención Americana Sobre Derechos Humanos, 1969, art. 8)

Reconociendo el debido proceso legal, como una garantía judicial, de igual manera el derecho a la defensa que es irrenunciable, y a la vez regula que el defensor podrá interrogar a testigos o peritos.

Pacto Internacional de Derechos Civiles y Políticos.

Este fue adoptado por la Asamblea General de las Naciones Unidas de acuerdo a la resolución de 16 de diciembre de 1966; en El Salvador entró en vigencia el día 23 de marzo de 1976.

En el artículo 14 reconoce que todas las personas son iguales ante los tribunales y cortes de justicia, a la vez el derecho a ser oídos públicamente y enmarca garantías como la presunción de inocencia, y el principio "ne bis in ídem", entre otras garantías mínimas.

En el artículo 19 inciso segundo expresa "Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección" (Pacto Internacional de Derechos Civiles y Políticos, 1976, art. 19). En el inciso 3 del mismo artículo reconoce que el ejercicio de este derecho entraña obligaciones y deberes especiales, por consiguiente está sujeto a restricciones establecidas en la ley con el fin de asegurar el respeto a los derechos o a la reputación de los demás y de la misma manera garantizar la protección de la seguridad nacional, el orden público o la salud o la moral pública.

Convenio de Budapest sobre la ciberdelincuencia.

Suscrito por los Estados miembros del Consejo de Europa el 23 de noviembre de 2001. Actualmente sigue siendo un referente para la creación de cualquier marco legal sobre cibercriminalidad. Una de las razones de la creación del convenio fue por la preocupación de los Estados acerca del uso de las redes informáticas, o del manejo de la información electrónica para cometer delitos. Por lo que uno de los fines del Convenio es luchar contra la ciberdelincuencia.

Más de 56 países de todo el mundo se han adherido, entre ellos Costa Rica, Chile, República Dominicana, Panamá y Argentina, sin embargo El Salvador no se encuentra suscrito al Convenio de Budapest así lo confirmó el Jefe de la Unidad de Asesoría Técnica Internacional de la Corte Suprema de Justicia, mediante memorándum con referencia UAIP-M708-2436-2017(2), en el cual se le solicitó la siguiente información:

> "Si la CSJ ha recibido consultas de adhesión al convenio sobre ciberdelincuencia de BUDAPEST del año 2001 u otros instrumentos internos de la materia, según los

> mecanismos legales correspondientes"(sic), quien respondió que en los registros de su Unidad no consta que se haya recibido consulta al respecto y que consultó vía telefónica, con la Dirección Jurídica del Ministerio de Relaciones Exteriores, sobre el tema en comento y le confirmaron que nuestro país no se ha adherido a dicho Convenio, ni tampoco está previsto o en estudio la adhesión al mismo." (Res. UAIP-2436-RR-884-2017(2), 2017).

En consecuencia en el país, no se hace uso de esta que podría ser una herramienta muy importante para la lucha contra el cibercrimen.

En el artículo 14 de la sección ll del Convenio Contra el Cibercrimen titulada "Derecho procesal", establece la obligación a los estados de adoptar medidas legislativas o de cualquier otro tipo con el fin de establecer el procedimiento de investigación de los delitos (Convenio Sobre la Ciberdelincuencia, 2001). De manera que si el país se hubiera suscrito y posteriormente ratificado, hoy sería una obligación para El Salvador adoptar ciertas medidas y no habría vacíos en la Ley Especial Contra Delitos Informáticos y Conexos, con respecto a la investigación de los delitos.

2.3.4. Marco conceptual.

En este apartado se presentan las definiciones de la mayor parte de los conceptos utilizados a lo largo del desarrollo de la investigación, con la finalidad de dar a conocer su significado en vista que se cuentan con algunos conceptos utilizados por los peritos informáticos, que es preciso conocer y manejar para entender el enfoque de la presente investigación.

Arquitectura de Von Neumann:

La arquitectura Von Neumann, también conocida como modelo de Von Neumann o arquitectura Princeton, es una arquitectura de computadoras basada en la descrita en 1945 por el matemático y físico John Von Neumann y otros, en el primer borrador de un informe sobre el EDVAC.

Este describe una arquitectura de diseño para un computador digital electrónico con partes que constan de una unidad de procesamiento que contiene una unidad aritmético lógica

y registros del procesador, una unidad de control que contiene un registro de instrucciones y un contador de programa, una memoria para almacenar tanto datos como instrucciones, almacenamiento masivo externo, y mecanismos de entrada y salida. El significado ha evolucionado hasta ser cualquier computador de programa almacenado en el cual no pueden ocurrir una extracción de instrucción y una operación de datos al mismo tiempo, ya que comparten un bus en común. Esto se conoce como el cuello de botella Von Neumann y muchas veces limita el rendimiento del sistema.

Arpanet:

Fue una red de computadoras creada por encargo del Departamento de Defensa de los Estados Unidos para utilizarla como medio de comunicación entre las diferentes instituciones académicas y estatales. El primer nodo fue creado en la Universidad de California en Los Ángeles, y fue la espina dorsal de Internet hasta 1990.

Activos informáticos:

Son aquellos recursos de software y hardware con los que puede contar una empresa, es decir todo elemento que compone el proceso completo de comunicación partiendo desde la información, el emisor, el medio de transmisión y el receptor.

Biotecnología:

Se denomina biotecnología al uso de células vivas para la producción y la optimización de medicamentos, alimentos y otros productos de utilidad para el ser humano. La noción también se refiere al estudio de esta técnica y a sus aplicaciones.

Dicho de otro modo la biotecnología consiste en aplicar los conocimientos de la ingeniería y de otras ciencias para usar agentes biológicos en el tratamiento de recurso orgánico, inorgánico, Esto permite obtener o modificar diferentes tipos de productos.

Ciberseguridad:

La ciberseguridad se define como una capa de protección para los archivos de información, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.

La ciberseguridad trata de trabajar en robustos sistemas que sean capaces de actuar antes, durante y después, no sirve solo para prevenir, sino también dar confianza a los clientes y al mercado, pudiendo así reducir el riesgo de exposición del usuario y de los sistemas.

Cracker:

Se aplica a quien, además de ser capaz de entrar en sistemas ajenos, lo hace con fines delictivos, como señala el diccionario de Oxford.

Por lo que se puede decir que un crackers es un programador malicioso, ciberpirata bandido virtual, el cual utiliza sus conocimientos con el objetivo de violar ilegal o inmoralmente sistemas cibernéticos para cometer ilícitos informáticos.

Un uso adecuado de ambos términos es el que figura en el siguiente ejemplo: Las empresas necesitarán 825 000 hackers para frenar a los crackersen 2025.

Copyright:

Es una palabra de origen inglés que traducido al español sería derechos de autor. Esto le proporciona al responsable de un contenido artístico o de una obra intelectual un derecho de autor cada vez que sea reproducido o utilizado, participando por ley en los posibles beneficios que genere su trabajo.

El significado de copyright engloba los reglamentos jurídicos que protegen los derechos morales y patrimoniales de los autores, simplemente por el hecho de haber realizado una obra artística, musical, científica, didáctica o literaria, entre otras. Se trata de un derecho humano esencial reconocido por la Declaración Universal de los Derechos Humanos.

Dispositivos electromagnéticos:

Son todos aquellos aparatos que permiten el paso o la interrupción del flujo de corriente a una determinada carga, esta puede ser motores, bobinas resistencias entre otras.

Edvac:

Se describe en inglés por sus siglas como (Electronic Discrete Variable Automatic Computer), fue una de las primeras computadoras electrónicas binaria, y tuvo el primer programa diseñado para ser almacenado. Este diseño se convirtió en estándar de arquitectura para la mayoría de las computadoras modernas. El diseño de la EDVAC es considerado un éxito en la historia de la informática.

Hacker:

Es el término utilizado para calificar a una persona que accede ilegalmente a portales ajenos, por lo que, es una persona con grandes habilidades para el manejo informático que decide orientar sus talentos a fines delictivos.

Hacking ético:

Es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas sin hacer daño.

La idea es tener el conocimiento de cuales elementos dentro de una red son vulnerables y corregirlo antes que ocurra hurto de información.

Hardware:

Es el conjunto de los componentes que conforman la parte material (física) de una computadora, a diferencia del software que refiere a los componentes lógicos (intangibles). Sin embargo, el concepto suele ser entendido de manera más amplia y se utiliza para denominar a todos los componentes físicos de una tecnología.

Memoria RAM:

La memoria de acceso aleatorio (RAM, por sus siglas en inglés) es uno de los elementos más importantes de los ordenadores convencionales y los dispositivos móviles, ya que la CPU hace uso de ella para guardar los datos y las instrucciones que está ejecutando en un momento determinado.

Metadatos:

La definición más concreta de los metadatos es qué son "datos acerca de los datos" y sirven para suministrar información sobre los datos producidos. Los metadatos consisten en información que caracteriza datos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos.

Los Metadatos permiten a una persona ubicar y entender los datos, incluyen información requerida para determinar qué conjuntos de datos existen para una localización geográfica particular, la información necesaria para determinar si un conjunto de datos es apropiado para fines específicos, la información requerida para recuperar o conseguir un conjunto ya identificado de datos y la información requerida para procesarlos y utilizarlos.

Los Metadatos proveen un inventario estandarizado de los datos georreferenciados existentes en una organización, proveen un gran potencial para usuarios que buscan cerciorarse si un dato o conjunto de datos georreferenciados son apropiados para su necesidad o si necesitan localizar datos en bases de datos de diferentes organizaciones.

NFSNET:

La Red de la Fundación Nacional para la Ciencia (NSFNET, de sus siglas del inglés National Science Foundation Network) fue un programa creado y financiado por la Fundación Nacional para la Ciencia para coordinar y promover investigación y educación avanzada en trabajo en redes en los Estados Unidos, y fue reemplazo de ARPANET Desde entonces ha sido reemplazada por las redes comerciales**.**

Nodo:

En informática y en telecomunicación, de forma muy general, un nodo es un punto de intersección, conexión o unión de varios elementos que confluyen en el mismo lugar. Ahora bien, dentro de la informática la palabra nodo puede referirse a conceptos diferentes según el ámbito en el que nos movamos:

En redes de computadoras cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo.

En estructuras de datos dinámicas un nodo es un registro que contiene un dato de interés y al menos un puntero para referenciar (apuntar) a otro nodo. Si la estructura tiene sólo un puntero, la única estructura que se puede construir con él es una lista, si el nodo tiene más de un puntero ya se pueden construir estructuras más complejas como árboles o grafos.

Pulsos eléctricos:

Son un tratamiento no térmico para la conservación de alimentos el cual se coloca un alimento fluido, semifluido o solido en una solución electrónica entre dos electrodos por periodos cortos de tiempo (menos de un segundo) y se le aplica un determinado número de pulsos de alto voltaje que varía según la inactivación que se desea conseguir.

Red:

Una red de computadoras (también llamada red de ordenadores, red de comunicaciones de datos o red informática) es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo. Un ejemplo es Internet, el cual es una gran red de millones de ordenadores ubicados en distintos puntos del planeta interconectados básicamente para compartir información y recursos.

Software:

Es un término informático que hace referencia a un programa o conjunto de programas de cómputo que incluye datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.

Comúnmente se utiliza este término para referirse de una forma muy genérica a los programas de un dispositivo informático.

Tecnologías de la información y comunicación:

Es un conjunto de técnicas y equipos informáticos que permiten comunicarse a distancia por vía electrónica.

De todos los elementos que integran las tecnologías de la informaticen y comunicación, sin duda el más poderoso y revolucionario es Internet, que nos abre las puertas de una nueva era, la Era Internet, en la que se ubica la actual Sociedad de la Información. Internet nos proporciona un tercer mundo en el que podemos hacer casi todo lo que hacemos en el mundo real y además nos permite desarrollar nuevas actividades.

Tecnología informática:

Se refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones.

Geofeedia:

Es una herramienta de geolocalización y rastreo en redes sociales, esta herramienta permite acceder a las noticias por medio de la ubicación, conocer y hacer monitoreo de los contenidos que son tendencias en redes sociales. Los resultados son en tiempo real, permitiendo localizar fotos en Instagram, mensajes en Twitter, videos en YouTube, entre otros servicios. La aplicación tarda aproximadamente 30 segundos en determinar qué información se encuentra en el lugar seleccionado.

Copia bit a bit:

Es una forma de clonación de archivos utilizando un método forense, este clonado forense se practica en discos duros y consiste en copiar todo el contenido de un disco duro, bit a bit, en otro dispositivo de almacenamiento o fichero de imagen obteniendo la firma hash de los bits leídos durante el proceso.

Perito informático:

Es el especialista forense que tiene conocimientos en informática, se encarga de ilustrar al juez en aquellos hechos que requieren los conocimientos especiales, científicos y técnicos relacionados a la informática. Asimismo es quien practica los peritajes informáticos.

CAPITULO III

MARCO METODOLÓGICO

3.1. Tipo de investigación.

Para llevar a cabo el trabajo de investigación, se utilizó el enfoque del método cualitativo, que consiste en "…examinar la forma en que los individuos perciben y experimentan los fenómenos que los rodean, profundizando en sus puntos de vista, interpretaciones y significados" (Hernández Sampieri, Collado, & Baptista Lucio, 2014, pág. 358), de modo que, puedan causar un significado sobre el fenómeno y contribuir para la orientación teóricas jurídicas.

En esta investigación se utilizó un tipo de estudio explicativo ya que, "este estudio va más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre

conceptos" (Franco, 2013, parrá. 3). Asimismo, dichos estudios también fueron encaminados a responder aquellas fuentes u orígenes de eventos físicos o sociales.

Es por ello, que su interés estaba focalizado en explicar por qué ocurre cierto fenómeno y las condiciones en que se da éste.

3.2. Sujetos de investigación.

El sujeto de investigación "Es la persona con formación científica que es capaz de pensar, investigar, un objeto de investigación, en relación con un problema de investigación" (Carvajal, 2013, parrá. 5).

Es por ello, que los sujetos de investigación que integraron las unidades de análisis se determinaron en relación al problema y a los objetivos que se establecieron al principio de la investigación. Sin embargo, se necesitó de la población y esta se definió como: "conjunto finito o infinito de elementos con características comunes, para los cuales serán extensivas las conclusiones de la investigación. Esta queda limitada por el problema y por los objetivos del estudio". (Tesis de Investigadores, 2012, parrá. 1).

3.2.1 Unidades de análisis.

La unidad de análisis se definió como "elementos en los que recae la obtención de información y que deben de ser definidos con propiedad, es decir precisar, a quien o a quienes se va a aplicar la muestra para efectos de obtener la información". (Centty, 2010, parrá. 1).

Al hablar de unidad de análisis se hizo referencia a un dominio limitado y diferenciable con propiedades inseparables, en tanto se adquirió perfilar un tipo que individualizo un conjunto que pueda ser distingo de otras entidades. Por otro lado, al referirse al análisis es porque se presumió que la unidad estuvo definida, es susceptible de conocerse al seguir un procedimiento de búsqueda. Por lo tanto, el tipo de muestreo estuvo dirigido a sujetos conocedores de la materia, que a través de su experiencia profesional brindaron la información para la edificación del estudio, por ende las unidades de análisis fueron las siguientes:

- Defensores Públicos y Particulares
- Fiscalía General de la República, Santa Ana
- Jueces de Instrucción y Sentencia de Santa Ana

- Laboratorio Técnico Científico de la Policía Nacional Civil.

3.2.2. Técnicas para la recolección de datos.

La recolección de datos ocurrió en los ambientes naturales y cotidianos de los participantes o unidades de análisis. Cabe decir, que el investigador fue el principal agente en la recolección de datos, ya que es quien colecciona los fundamentos mediante diferentes métodos y técnicas. Es decir que no sólo analiza si no que es el medio de obtención de la información. (Hernández Sampieri et al, 2014).

Observación:

En este tipo de investigación la observación es un elemento importante por lo tanto se necesitó realizarla de la mejor manera. Cabe mencionar que, observar es diferente a ver (lo cual hacemos cotidianamente). Es por ello que, no sólo se limitó al sentido de la vista sino a todos los sentidos (Hernández Sampieri et al 2014).

Ahora bien, observación según Juan Herrera files "es aquella que nos permite obtener información sobre un fenómeno o acontecimiento tal y como este se produce" (Herrera files, 2008, pág. 13). Es decir, que consistió en observar detenidamente los elementos que están dentro de nuestro campo de estudio y por lo tanto recopilar todo aquello que beneficiara a la investigación.

En cuanto al tipo de observación que se utilizó, fue la observación participante. Acordé con ello Galan Amador, en el artículo la observación como método de investigación, menciona que:

> Es indicada para propósitos exploratorios, y forma parte del proceso de familiarización del investigador en el estudio de la situación. Aquí, el análisis de los datos es simultáneo a la recolección de los mismos. El investigador determina que se debe observar y como va registrar esas observaciones. De igual manera, debe plantearse una estrategia anticipadamente, así como establecer listas y registros de la observación de manera que la observación sea selectiva, concentrándose esta en los detalles relevantes.

3.2.3 Muestreo cualitativo.

Es común que en la investigación cualitativa el diseño del estudio se desarrolle conforme a la plena determinación. Sin embargo, en el caso del muestreo sucede lo mismo, ya que, se tomó la mejor decisión de cómo obtener los datos y de quién o quiénes obtenerlos, determinaciones que fueron realizadas en el campo, pues se pretendió manifestar la situación actual y los numerosos puntos de vista de los colaboradores, los cuales resultaron desconocidos al iniciar el estudio.

> En los estudios cualitativos casi siempre se emplean muestras pequeñas no aleatorias, lo cual no significa que los investigadores naturalistas no se interesen por la calidad de sus muestras, sino que aplican criterios distintos para seleccionar a los participantes (Martín- Crespo & Salamanca , 2007, pág. 1).

Sin embargo, para realizar el muestro cualitativo hay una diversidad de este tipo de muestra pero debido a la orientación de la investigación se utilizó el **muestreo por conveniencia,** ya que.

> Es una técnica de muestreo no probabilístico donde los sujetos son seleccionados dada la conveniente accesibilidad y proximidad de los sujetos para el investigador (Explorable, 2019, parrá. 1).

Es decir las personas disponibles en la investigación fueron seleccionadas por su fácil disponibilidad, no porque hayan sido seleccionados mediante un criterio detallado. Esta conveniencia, se puedo establecer por su simplicidad al momento de ser ejecutada y en bajos costes de muestreo.

Es por ello, que para esta investigación se seleccionaron 6 personas conocedoras de la ley como lo son el Juez, Procurador, Abogado Particular, Fiscal y Perito con el único objeto de efectuar las entrevistas y así hacer el estudio de los datos recolectados referente a la problemática que existe actualmente en la pericia informática referente al proceso penal salvadoreño.

3.2.4 Determinación de las categorías de análisis.

Esta investigación estuvo orientada a considerar los objetivos planteados y todos aquellos elementos teóricos analizados es por ello, que se estudiaron las siguientes categorías de análisis:

- La pericia Informática: "se refiere a los estudios e investigaciones orientados a la obtención de una prueba o evidencia electrónica, de aplicación en un asunto judicial o extrajudicial, para que sirva para decidir sobre la culpabilidad o inocencia de una de las partes" (Investigacion Informatica, 2012, párr.1), realizadas por quienes poseen conocimientos especializados en informática, de manera que está ilustra al juez sobre los hechos relevantes en el proceso. (LLUCH, 2014)

- Problemas probatorios: uno de los aspectos importante lo constituye el hecho de como probar los delitos informáticos, para ello el Dr. Riquent señala: "las dificultades que se producen en materia probatoria en el proceso penal, es una de las cuestiones que debería preverse de lege ferenda ya que no bastara el adecuar la legislación de fondo si la forma permanece atada al estado". (ResearchGate., 2014)

- La administración de justicia penal en los delitos informáticos es: "una función pública derivada de la soberanía del Estado, que se atribuye a los jueces y magistrados" (Guias Juridicas, 2019, párr. 5), quienes son los encargados de absolver o condenar a quien se le imputa el cometimiento de un delito informático.

3.2.5. Criterios de inclusión.

En vista que la investigación estuvo enfocada en el tema probatorio de la pericia informática, fue necesario que las personas que participaran aportando sus conocimientos fueran profesionales del derecho y especialistas informáticos, es por ello que fueron objeto de estudio aquellas personas especialistas en derecho que cumplieron con las siguientes características:

- Juez de instrucción

- Juez de sentencia
- Fiscal
- Perito informático del Laboratorio Técnico Científico de la Policía Nacional Civil
- Abogado defensor público
- Abogado defensor particular.

3.3. Instrumentos.

A través del proceso de la investigación cualitativa se hizo necesario utilizar instrumentos que ayudaron a conocer precisamente el problema de la investigación es por ello que para alcanzar los objetivos planteados se requirió utilizar los siguientes:

Entrevista semiestructurada.

La entrevista semiestructurada, consistió en realizar una comunicación con una persona o varias, y profundizar en el tema de interés; es decir, se dirigió un interrogatorio progresivo y fluido, y se buscó hacer que la persona entrevistada o grupo entrevistado se expresara; de esta manera la entrevista utilizada permitió obtener todos los datos importantes para la investigación.

> Juan Herrera Files aporta que: "es una técnica en la que una persona solicita información de otra o de un grupo, para obtener datos sobre un problema determinado, presupone pues la existencia al menos de dos personas y la posibilidad de interacción verbal" (Pág, 15).

En ese mismo orden de ideas tomando en cuenta que el tipo de entrevista que se utilizó en esta investigación es la entrevista semiestructurada, Sampieri considera que "estas se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener mayor información" (Hernández Sampieri et al 2014).

El instrumento anteriormente descrito, se utilizó para entrevistar a profesionales del derecho que trabajan en instituciones públicas, ya sea un Juez, Fiscal y/o Defensor Público, asimismo a Defensores Particulares, por lo cual pretendió con este instrumento obtener información amplia sobre cuáles son los problemas difíciles de vencer con los que se enfrentan dichos profesionales a la hora de actuar en un Proceso Penal de naturaleza informática, así

como también se utilizó con el Perito Informático del Laboratorio Técnico Científico de la Policía Nacional Civil, a quien se le dirigió con el objetivo de que brindara información acerca de las dificultares con las que se enfrenta a la hora de extraer una prueba informática vinculada a un proceso penal.

3.3.1 Validación de instrumentos.

La validez de los instrumentos "…en términos generales se refiere al grado en que un instrumento mide la variable que quiere medir." (Blogspot, 2012).

Los instrumentos utilizados en la investigación fueron validados a través del sometimiento a un análisis, realizado por profesionales del derecho, quienes conocieron de primera mano la temática abordada para que fueran estos quienes puedieran definir si los instrumentos en cuestión cumplían con los elementos mínimos para poder ser utilizados para recabar información.

3.4. Procedimiento de aplicación.

Se acudió a tribunales, instituciones y oficinas jurídicas de personas que cumplieran con las características profesionales relacionadas al derecho como jueces, fiscales, defensores públicos y defensores particulares, así como también peritos informáticos del Laboratorio Técnico Científico de la Policía Nacional Civil.

Al llegar a esta etapa ya se tenían definidos los personajes a quienes se les realizaron las entrevistas, tomando en cuenta que estas fueron formuladas con el fin de obtener puntos claves sobre el tema planteado, enfocadas en darle respuestas concretas a las preguntas de investigación que se plantearon al inicio de la investigación.

Se dirigió un escrito con fines académicos a cada institución, escrito a través con el que se logró el acceso a la información que se solicitó en especial al personal del Laboratorio Técnico Científico de la Policía Nacional Civil debido al manejo forense que estos le dan a las evidencias informáticas en los procesos penales de este tipo.

En los párrafos anteriores se expresó, que se entrevistó a abogados particulares, a ellos se les realizó una serie de preguntas sobre el manejo que tienen en un proceso penal a la hora de hacer valer la prueba informática, así como también sobre las dificultades que se les

presentan al momento de ejercer la defensa técnica de una persona que está siendo procesada por un delito informático.

Se abordó a jueces desde la etapa de instrucción hasta la etapa de sentencia dentro del territorio occidental del país y se logró extraer información sobre cómo ellos valoran la prueba pericial en los procesos penales que tienen relación con los delitos informáticos.

Se indagó a los peritos informáticos del Laboratorio Técnico Científico de la Policía Nacional Civil, sobre el manejo que se le puede dar a una prueba que provenga de medios informáticos y cómo es la forma más adecuada de proteger su veracidad sin que esta sea contaminada o pierda la cadena de custodia en un determinado proceso penal.

3.5. Procesamiento y análisis de la información.

En la investigación cualitativa la recolección de datos fue una de las partes fundamentales de la investigación debido a que se trató de buscar los datos más importantes que permitieran obtener la información necesaria sobre las personas que se investigaron, así, se pudo llegar al objetivo planeado. De modo que la información obtenida se trató de analizar y comprender para dar respuesta a las preguntas de investigación (Baptista Lucio, Fernández Collado & Hernández Sampieri, 2010).

Asimismo, son los investigadores el medio que se utilizó para que se encargaran de recolectar la información que se necesitaba, considerando que ellos fueron los encargados de aplicar todos los instrumentos para adquirir los datos y analizarlos. A continuación se presenta una figura que detalla el proceso utilizado para la recolección de datos de la investigación:

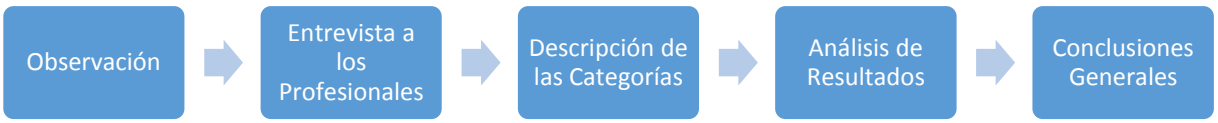

Figura 1

Proceso de recolección de datos.

Fuente: Elaboración Propia.

Con respecto al proceso de recolección de datos que se muestra en la figura 1, se inició con la técnica de la observación a los diferentes profesionales objeto de estudio, luego se aplicó las entrevistas semiestructuradas para posteriormente describir las categorías de análisis

que fueron producto de los diferentes objetivos de investigación, a continuación se analizaron los datos obtenidos de acuerdo a las categorías y por último se presentaron las conclusiones generales.

Posterior a la recolección de la información se realizó el procesamiento de la misma, procesando dicha información a través del vaciado de las entrevistas realizadas a las distintas unidades de análisis, esta información fue recabada en matrices cualitativas, lo cual facilitó el posterior análisis de dicha información.

Para la elaboración del vaciado de la información se utilizó las matrices de vaciado, para poder valorar los datos aportados por los partícipes y así tener elementos para el ordenamiento de las categorías de análisis.

Para el análisis de los resultados se elaboró una matriz de análisis a partir de las categorías planteadas en la investigación. Con dicha matriz se buscó especificar criterios particulares, en vista que en ella se vaciaron las distintas respuestas de los sujetos de investigación entrevistados.

El llenado de la matriz de análisis, partió de la transcripción de las diferentes entrevistas a través de un análisis de la prueba semáforo, a través de los diferentes criterios que muestren los instrumentos para poder explicar los principales hallazgos que se obtuvieron de la recolección de los mismos.

Vaciada la información se procedió a analizar los datos, para ello se trabajó con una matriz de análisis de resultados, que dependió de la aplicación de una entrevista semiestructurada integrando seis instrumentos, ya que es esta la cantidad de sujetos a entrevistados; de igual forma se tomaron como base las categorías de análisis que se encuentran en los objetivos de estudio.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS DATOS

4.1. Matriz de vaciado de información.

Cuadro 1 Transcripción de entrevista semiestructurada dirigida a Procuraduría General de la República, Santa Ana.

ENTREVISTADO: RAE

FECHA: 30/05/2019 **HORA:** 3:30 pm.

N.º	PREGUNTA	REPUESTA
1	¿Qué estudio posee sobre pericia informática?	Sobre eso lo que le puedo contestar es que hemos recibido una capacitación sobre delitos informáticos y dentro de los delitos informáticos hemos analizado la prueba informática.
2	¿Qué capacitaciones recibe sobre actualización en tecnología de la información?	Actualmente sobre esa capacitaciones ninguna, solo lo que yo puedo hacer particularmente.
3	¿Cuál es el procedimiento para realizar un peritaje o un contraperitaje informático?	El procedimiento normal, depende de a quien le interesa, si es a la defensa que le interesa lo solicita la defensa al juez, y si es a fiscalía será el ente público quien lo solicite al juez, y hay casos donde el juez autoriza al fiscal que realice la prueba informática, y le pide al ente fiscal que comunique o notifique a la parte contraria la diligencia a realizar, cabe destacar que no se realiza el mismo día la pericia, sino que se va a las oficinas de la policía en San Salvador, haya se constituyen las partes y se entrega el aparato, el perito lo toma y se compromete en otra fecha en enviar el resultado.

4	¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje?	Podemos decir que en un 75% o 90% que se cuentan con los recursos posiblemente, pero hay limitantes que nos impiden hablar de un 100%.
5	¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?	Eso es lo discutible, que nos lleva a una discusión donde la prueba no le refleja los hechos reales sino que le va a reflejar que existe una información en un medio informático, pero que no precisamente este medio dirá que el hecho es real, en esencia la pericia informática dirá que sucedió una alteración pero no definirá quien la realizó.
6	¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?	No hay un procedimiento establecido, va dependiendo de cuál prueba informática se trate, porque pueden haber otras; para el caso de las extorciones intervienen las llamadas, y cuando se incautan objetos el fiscal hace una petición al juez que le autorice el vaciado de la información a través del perito, es entonces que el juez ordena la práctica de esta diligencia y hay casos donde se constituyen las partes en el juzgado, se juramenta al perito y este se lleva el aparato y posteriormente él hace llegar esa información al juzgado, esto nos demuestra que quien ejerce la cadena de custodia sobre los objetos secuestrados es el perito, y cuando este no puede entregar la información se la da a otro compañero que casualmente se dirige para el lugar donde se tiene que entregar esta y con dicha acción rompe la cadena de custodia.
7	¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?	Digamos que si el peritaje informático si se hace dentro de un procedimiento normal y usando las herramientas idóneas, tiene un 100% de confiabilidad, aún más que el ADN porque este arroja un 99.99% y se da por establecida la paternidad, pero aunque este peritaje de un 100% hay que tomar en cuenta que la prueba está sujeta a manipulación y es entonces donde puede haber posibilidades de falsear una información.

8	¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?	Esto es lo discutible porque los verbos rectores de un tipo penal están establecidos legalmente y uno de los elementos de prueba es la prueba informática, pero no es solo esta sino que existen otros medios de prueba, incluso la ley permite la incorporación de otros medios de prueba al proceso penal siempre y cuando este dentro de las normas y requisitos de la prueba del Código Penal.
9	¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?	Lo normal es que no lo hacemos, porque delitos informáticos pocos estamos viendo, pero cuando es necesario si lo hacemos.
10	¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?	En algunos casos si, pues hay casos que por la misma situación que se da, porque hay un círculo vicioso que se da cuando se trata de justificar una prueba informática, esto nos lleva a decir que cada caso es distinto y se presenta de distinta manera
11	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	Dependiendo pero en un caso en concreto pueden haber variaciones, esto genera un problema de aplicación porque si tenemos un peritaje que la defensa prevé antes de la audiencia, ese peritaje que a criterio de la defensa no logra establecer el hecho, entonces no tiene caso peticionar otro cuando se está viendo la debilidad que tiene la prueba para desacreditarla, por eso reitera que dependiendo del caso se solicita o no, pues puede darse el caso que la defensa considere que necesita una prueba que establezca otro resultado, hay que valorar si se solicita o no.
12	¿Si el fiscal presenta peritaje informático es suficiente para probar el	No es suficiente, esto depende, pues partiendo de la fidelidad de la prueba posiblemente en algún caso va a ser suficiente o posiblemente en otros no porque pueden variar algunas

	hecho delictivo?	circunstancias.

Fuente: Elaboración Propia

Cuadro 2 Transcripción de entrevista semiestructurada dirigida a defensor particular, Santa Ana.

ENTREVISTADO: HUMR

FECHA: 07/05/2019 **HORA:** 10:43 am.

N.º	**PREGUNTA**	**REPUESTA**
1	¿Qué estudio posee sobre pericia informática?	Son mínimos estudios que dan sobre la pericia informática, yo realmente medio recibí una charla informativa sobre la pericia informática, acuérdese que la pericia son elementos de prueba anticipados o elementos de prueba que necesitan la autorización judicial, donde se nombre un perito conocedor del tema, o un perito de la Policía Técnica Científica que es la única que tenemos aquí porque peritos informáticos de donde vamos a traer, solo que vayamos a sacar a los técnicos de los ciber, pero ellos no saben nada de leyes y de pericia tampoco.
2	¿Qué capacitaciones recibe sobre actualización en tecnología de la información?	La verdad no he recibido capacitaciones meramente de los delitos informáticos por lo que se debería buscar una institución que este informando a los profesionales dando la información correcta o hiciera los estudios y actualizaciones tecnológicas de la informática, aquí no hay nadie que haga eso es mentira aquí solo se han metido que aquí hay delitos informáticos por unos dos o tres casitos ralos que se han dado, por eso, pero si actualizaciones en tecnologías de la información no, me atrevo a decir que Centroamérica no tiene nada de eso, incluso El Salvador es

		uno de los países de Centro América que va a veces un poquito avanzado en tecnología, pero por los piratas que aquí traen teléfonos y otras cuestiones.
3	¿Cuál es el procedimiento para realizar un peritaje o un contraperitaje informático?	Los procedimientos ya están establecidos en el código procesal penal, los procedimientos para realizar un peritaje ya sabemos que hay que hacer petición al órgano judicial en este caso al juez competente o un juez que en determinado momento tenga la causa, entonces a él se le pide los peritajes, lo que hace la fiscalía es que a veces de recoger los elementos indiciarios o las primeras investigaciones, pero cuando se trata de peritaje tendremos que hacerlo para fundamentar una determinada acusación o defensa técnica tendríamos que hacerlo con mediación judicial, cuando habla de contraperitaje es la defensa ya que esta puede proponer peritos y puede proponer puntos de peritaje, cuando la defensa pone puntos de peritajes también puede agregar un perito y en este caso en relación a los delitos informáticos, ahora bien donde encontrara a un perito eficientemente preparado para que le venga a hacer un contra peritaje, solo que esta persona tenga dinero y lo traiga del extranjero y diga si haremos un buen estudio para contrarrestar el peritaje que presenta la otra parte, en este país se presta y los abogados en el ejercicio libre re la profesión sabemos que en este país muchas pruebas de peritaje a veces vienen viciadas, las pruebas pre constituidas vienen un tanto viciadas.
4	¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje?	Cuando se trata de recursos tecnológicos idóneos en el país es bien escaso, aquí no hay una empresa que diga, nosotros somos la empresa informática en la cual vamos a la vanguardia con la información tecnológica y nosotros podemos dar peritajes, si yo quiero sacar los mensajes de un WhatsApp que han desaparecido o algo, nosotros somos especialistas en eso, nosotros hemos pagado aplicaciones para realizar esos procesos existe una aplicación rusa que anda por ahí que

		no se puede detectar nada incluso los muchachos de agrupaciones utilizan esa aplicación rusa para que no los detecten entonces en recursos tecnológicos idóneos el país está muy bajo, el país no tiene para hacer eso, la fiscalía tiene una herramienta que es la Policía Técnica Científica, pero de técnica y científica deja mucho en que dudar.
5	¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?	Mire, las herramientas de software si, el problema es aquí no las podemos utilizar aquí no utilizamos las herramientas de software, porque los softwares son creaciones de otros países más avanzados, pero hablando en sí de las herramientas si puede hacerse, pero aquí las utilizamos mal o no las tenemos.
6	¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?	Cuando habla de protocolo es el procedimiento que se hace, el procedimiento de extracción y transporte es a través de una solicitud que se hace primeramente al tribunal para nombramiento de un perito, de ahí se le da la comisión al perito para que vaya hacer la extracción, el Órgano Judicial en ese aspecto esta corto porque tiene medicina legal y otros, pero que bien es que se desprendiera de la policía lo que es la Policía Técnica Científica, se desprendiera de la policía y existiera una institución autónoma que fuera tecnologizada y pudiera decirse en un determinado momento, aquí tenemos esta institución que aporta a los peritajes y los contra peritajes, que bien que existiera la estatal y existiera una privada, para que la privada a solicitud del abogado defensor dijera vamos a ver si comprobamos lo mismo, ahí ya estaríamos equilibrando esta situación, volviendo, el proceso de extracción ya está establecido, nombramiento al perito se manda a que haga el peritaje con los elementos que él tiene por allá va, no sé cuáles son los que tenga, es el que menos sabe que software tiene, hoy últimamente para observaciones de firma

		tienen la lupa, la lupa y la lupa y a eso le dan fe, una lupa cualquiera la puede tener pero no un buen conocimiento y en cuanto a los software debe tener conocimiento tecnológico sobre eso y aquí fallamos en ese punto.
7	¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?	Mire probabilidades son muchas pero muchas, el problema aquí es que el defensor no se da cuenta que lo han falseado, si aquí vienen caso donde dicen lo reconoció una persona por q se lo mostramos en una base de datos y yo tengo unos donde han mostrado bases de datos pero el testigo dice otra cosa ah presumen que esta es, la prueba presuntiva no la admite nuestro código aquí o se prueba o no se prueba.
8	¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?	Dentro del tipo penal tenemos elementos subjetivos del tipo como elementos objetivos del tipo penal y esos hay que establecerlos, los elementos subjetivos habría que determinarlos, cuáles de los elementos subjetivos de los tipos penales se pueden estar comprobando con lo que es el peritaje informático y extraerlos, ejemplo mire aquí dijo esto y lo dijo esta persona, ese es el elemento subjetivo ahora bien vamos a los elementos objetivos a ver si esos también se pueden establecer eso se determinara a través del medio probatorio que tengamos en ese momento.
9	¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?	Le vuelvo a repetir la nueve se la está contestando con la ocho y la diez en el sentido de que como si el cliente es el que menos tiene, tras que le decomisan todo lo que tiene por diferentes delitos que supuestamente cometió el imputado queda sin el poder económico, si hay un imputado que tiene plata volvemos a la situación de donde va agarrar?, a que institución se va acercar para hacer un contraperitaje informático?, no hay ninguna institución donde pueda hacer contraperitaje informático, ese es uno de los grandes obstáculos que tiene la defensa, en ese

		aspecto considero que se pone bien difícil la situación.
10	¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?	A veces claridad aquí es bien difícil, si al Juez a veces con que le cuesta manejar el teléfono táctil IPhone que tiene o Samsung o Huawei, entonces dirá si dice tal cosa en el peritaje informático, pero como la defensa esta corta en esa cuestión, ¿porque la defensa esta corta? Porque a veces su cliente no tiene dinero y como va a acceder a un peritaje o contraperitaje en esa situación queda desnivelada la defensa, entonces el juez se va ir con lo que le diga el perito de la Policía Técnica Científica, si ahí dice fulano fue y aquí está el número, el juez dirá si aquí está el numero pero el juez no sabe si el investigador o perito le dijeron este número es y a saber si no es ese , ahí es donde se empieza a contaminar lo dicho desde que el agente policial captura al imputado, desde ahí viene la contaminación de todo y ahí es donde existen problemas para el defensor, el juez quien toma como claro la situación esa y así condenan a las personas y eso lo sufrimos todos los abogados defensores.
11	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	Para mi si porque si vienen al defensa y presenta un buen peritaje informático y el imputado dice tengo dinero contratare a unas personas de una empresa norteamericana que me venga a hacer un contraperitaje, y lo certifique con toda la documentación legal en el trámite correcto que se tiene que hacer, y decir este es un perito informático de primera, y viene a desvirtuar todo el peritaje que hacen la Policía Técnica Científica si nosotros no tenemos técnicos, entonces si viene a desacreditar todo eso y lo admite el juez y sigue todos los procedimientos perfectamente puede desvirtuar la participación del imputado, pero el hecho de que aquí en el país es bien difícil y otra cosa sabemos la situación económica financiera y la situación delincuencial que hay en el país, aquí si pelean dos personas grandes siempre van con el temor de que les pueda suceder algo, entonces se pone bien complicado porque la balanza se inclina a veces a favor de la fiscalía por

		que el defensor no tiene las armas pertinentes, lo único que le toca a uno es estar atento para cuando el fiscal cometa el error o fajarse en el contrainterrogatorio, eso le queda a uno no más.
12	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	Habría que ver cómo viene el peritaje informático, todo es de análisis, a veces por poner una cuestión más adelante se puede contradecir, ahí es donde puede entrar en función algo que es el consultor técnico a la hora de la vista pública, si yo vengo y digo el fiscal presento peritaje informático ¿es suficiente para probar el hecho delictivo? Vengo yo y digo no hay medios en el país, no tengo una persona que sea experta para que me haga un peritaje o mi cliente no puede cubrir un peritaje, como defensor debo de buscar las armas que tengo para defenderme, lo que o haría es contratar un consultor técnico que conozca sobre informática y lo tengo en vista pública y le doy copia del peritaje informático presentado por el fiscal para efecto que el fiscal no pueda el hecho delictivo, otro perito dice esto no es así como lo ha puesto en el peritaje informático, ya con una cosa que diga que no es así, ya me da un elemento para decirle al Juez que hay un error en el peritaje informático por lo tanto no lo podemos tener como un elemento para probar el hecho delictivo, pero si yo no pruebo absolutamente nada sobre el peritaje informático a lo mejor el Juez sentenciador pueda decir es suficiente y va tener como probados los hechos delictivos, podría ser, como le digo los elementos del tipo penales son los q hay q probar tanto objetivos como subjetivos pero hay otras cuestiones que ustedes como estudiantes de derecho saben lo q son la teoría del delito y saben la fase intermedia y toda esa cuestión, ustedes lo tienen más fresco y ahí verán ciertos elementos que hay que probar para establecer el tipo penal pero probar el hecho delictivo así yo estaría dudoso en esa cuestión, tendríamos que ver en concreto ciertos casos para determinar si fiscalía pudo haber probado el hecho delictivo. En ese aspecto va el

		análisis de lo que es los delitos informáticos, que le soy sincero gran conocimiento de los delitos informáticos no tengo pero si del proceso penal.

Fuente: Elaboración Propia.

Cuadro 3 Transcripción de entrevista semiestructurada dirigida a Fiscalía General de La República, Santa Ana.

ENTREVISTADO: CERH

FECHA: 10/06/2019 **HORA:** 03:00 pm.

N.º	**PREGUNTA**	**REPUESTA**
1	¿Qué estudio posee sobre pericia informática?	Nosotros, como investigadores o como los encargados de investigar todos los delitos, nos corresponde obviamente conocer en principio como se investigan los hechos delictivos, por eso es de que en el caso del fiscal le corresponde saber y conocer cómo se investigan en este caso un delito informático, y por eso es que nosotros somos formados en diversos cursos sobre como investigar este tipo de delitos.
2	¿Qué capacitaciones recibe sobre actualización en tecnología de la información?	Bueno actualmente se realizan muchos cursos orientados a que los fiscales conozcan como investigar los delitos informáticos como, por ejemplo, Curso Especializado sobre Técnicas de Investigación del Delito Informático.
3	¿Cuál es el procedimiento para realizar un peritaje o un contraperitaje informático?	Ok, el procedimiento ya lo establece el Código Procesal Penal que es el mismo procedimiento en este caso en específico va depender o las leyes a fines va depender

		la pericia que se requiera pero generalmente una pericia se solicita la autorización del juez, el juez nombra los peritos, las dos partes tienen derecho a proponer y una vez se selecciona los peritos estos se juramentan, si no son peritos permanentes se juramentan y se les da un plazo para que emitan dictamen.
4	¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje?	Digamos que los recursos si existen, no son suficientes, pero si existen, las instituciones digamos tienen recursos, pero obviamente no son suficientes para las exigencias de los delitos que actualmente se cometen.
5	¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?	Si eso va a depender mucho del tipo de pericia que se está requiriendo porque generalmente nosotros encontramos evidencias, pero obviamente las evidencias hay que analizarlas o se les corresponde a las partes en este caso al fiscal examinar, analizar la evidencia y al juez obviamente valorarla.
6	¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?	Existe un capítulo específico en el Código Procesal Penal sobre cadena de custodia, cuando se extrae, se incauta cualquier evidencia se llena una cadena de custodia y esa cadena de custodia es la que nos da a nosotros fe de que la evidencia que se incauto es la misma que llegue al juico, de tal manera de que en cada eslabón que va pasando la evidencia se debe de dejar registro de quien tuvo la evidencia para que fines y obviamente eso le llega hasta el juez y por eso es que el juez puede al final dictaminar que la evidencia que se incautó y se analizo es la misma que haya llegado a juicio.
7	¿Qué probabilidades existen de falsear la información obtenida en un peritaje o	Probabilidades de falsear, bueno digamos que, en esta materia, en cualquier otra materia alguien puede falsear una evidencia, una prueba, pero para eso en estos casos

	contraperitaje informático?	en específico las partes tienen el derecho de proponer otros peritos que pueden realizar la pericia de manera conjunta. Y eso en cierta manera garantiza de que al final haya una fidelidad del dictamen o de la información aun y cuando las conclusiones sean diferentes, pero se garantiza que la información no esté falseada.
8	¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?	En el caso que sea contundente pues es claro que si verdad, pero como probar los hechos no depende solamente de una prueba en lo particular si no que una prueba en este caso una prueba una pericia tecnológica pues en un proceso puede ser una de una gama de evidencias que son sometidas a la valoración del juez.
9	¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?	Es su derecho, como parte técnica puede proponer perito, puede proponer la realización de una nueva pericia, claro que el por sí solo no lo puede presentar porque eso tiene que ser en este caso si él quiere una prueba pericial, pues obviamente tiene que pedirlo al juez y el juez juramentar los perito. Él (defensor) lo que puede hacer es proponer que se realice una prueba pericial y proponer los peritos que el piense que son los idóneos para la realización de esa prueba, claro que debe acreditar esa circunstancia.
10	¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?	Cuando uno analiza una sentencia puede uno en base a cierto grado de experiencia ya en este que hacer uno puede en cierta medida interpretar si el juez que conoció el caso es un juez con experiencia, un juez que conoce mucho, o es un juez que digamos le falta un poco, entonces este todo respeto verdad, pero un juez que conoce en principio como se redacta una sentencia y dos sabe trasladar la evidencia a esa sentencia verdad, claro que puede haber claridad al respecto verdad ahora, puede también conocer pero la redacción puede ser mala no la ha trasladado al documento.

		Entonces cuando uno lee una sentencia puede uno dictaminar si hizo una valoración completa y analítica del caso en específico y ahí es donde uno puede decir valoro bien esta prueba.
11	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	Nosotros tenemos vivimos y tenemos un sistema de pesos y contrapesos, es obvio de que la contraparte tiene derecho a presentar prueba de descargo verdad, entonces va a depender del tipo de peritaje que es lo que se pretende probar, eventualmente podría ser que si o podría ser que no, o simplemente confirmar la primer pericia.
12	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	Va depender del hecho que pretende probar, un delito puede tener diferentes digamos o varios elementos objetivos del tipo y cada uno de esos datos están sujetos a prueba, entonces va depender para que se realizó ese peritaje, si el peritaje es para probar uno de esos datos objetivos, pues habrá probado parcialmente digamos el tipo penal y obviamente complementado con otros electos de prueba, entonces esto depende mucho de que es específicamente lo que se pretenda probar, porque obviamente el tipo penal tiene elementos objetivos, subjetivos y normativos verdad entonces es casi imposible que con una sola evidencia se prueben todos los elementos del tipo penal.

Fuente: Elaboración Propia

Cuadro 4 Transcripción de entrevista semiestructurada dirigida al Juez de Instrucción de Metapán, Santa Ana.

ENTREVISTADO: MAUA

FECHA: 03/05/2019 **HORA:** 10:30 am.

N.º	**PREGUNTA**	**REPUESTA**
1	¿Qué estudio posee sobre pericia informática?	No una preparación intensiva, pero si cursos básicos orientados a valoración y admisión de prueba o incautación o al manejo de los mismos.
2	¿Qué capacitaciones recibe sobre actualización en tecnología de la información?	Si he recibido un par de cursos relacionados a la pregunta anterior sobre todo al manejo de leyes novedosas en el país como estas leyes especiales y estos delitos sobre todo como se debe manejar el ofertorio y la admisión de la prueba para no violentar derechos y garantías
3	¿Cuál es el procedimiento para realizar un peritaje o un contraperitaje informático?	El procedimiento para los peritajes es para el ente fiscal o ente acusador o parte interesada procede a señalar algún equipo o soporte técnico donde este contenida alguna información que se crea útil para alguna investigación el proceso es que se incauta y el fiscal solicita al juez la autorización para sustraer la información del lugar donde se crea que este para no violentar derechos y garantías si al juez le parece lo autoriza y se nombra perito con conocimientos en la materia.

4	¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje?	La PNC y fiscalía están en esta lucha de algún equipamientos así como algunas organizaciones internacionales, debido a que en el país no solo se necesita pruebas en los procesos penales como la confesión o pruebas testimonial sino también pruebas científicas y dentro de ella se entra lo que es la admisión de las pruebas tecnológicas en lo que parece que se empieza a entrar en transición en lo cual se encuentran de una manera en adquisición de los insumos necesarios para darles tramite a estos peritajes.
5	¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?	Si porque en un software queda la evidencia, porque si hay herramientas para sustraer la información real y veraz y puede depender en muchos casos en primer lugar del tipo de equipo que se trata en donde se encuentre el soporte del software y otro seria de la astucia de la persona que maneja la información llámese persona investigada o procesada, esto debido a que a la delincuencia que va a delante del sistema esto al momento de sustraer información vía peritaje no se pueda por la habilidad de la persona que lo ha manejado.
6	¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?	Por tener un sistema penal acusatorio esa carga corre por cuenta del fiscal por ser este el que investiga, ubica y señala, los equipos donde estén estas investigaciones, siendo este a través de la PNC y las unidades especializadas quien incauta luego de eso proceden a elaborar la cadena de custodia y la conservación de esos software o material sujeto a peritaje queda en poder del fiscal y este solicita al juez este peritaje y el juez lo autoriza y se nombra al perito designado por el fiscal quedándole a fiscal y a perito esta responsabilidad.
7	¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?	Yo creería que si esta un equipo que ha sido incautado respetando derechos y garantías hay una debida cadena de custodia hay una conservación y un perito calificado las posibilidades son mínimas pero en todo caso existen falencias que puedan permitir que esas debilidades vayan incrementando por el uso de las tecnologías de las herramientas

8	¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?	Si porque puede ser que el juez sentenciador pueda tener en su poder el analizar y valorar el contenido y si este contenido ha sido respetado todo lo anterior y si el peritaje arroja información positiva el juez podrá valorar en base al mismo.
9	¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?	La experiencia nos indica que los abogados somos acusocios e inteligentes lo cual crea las contraproponiendo los hechos al juez pero el fiscal está en la obligación de investigar lo que le afecte al acusado por el cual se encarga a las cosas de cargo pero es muy poco.
10	¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?	En un par de respuestas se hablaba de la existencia del delito pero para mí el juez debe ser más acusocio para la participación del procesado por el cual debe haber una individualización cierta de que esa información ese equipo o lo que arrojo ese peritaje fue manipulado por el procesado si es así puede valorar más allá de la existencia del delito la participación del delito
11	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	Si puede por la hipótesis fiscal es solo eso una relación de hechos que contiene una hipótesis estando sujeta a que lo corrobore un juez o el fiscal y si no lo logra el defensor puede demostrarle al juez que los hechos no fueron así y que fue diferente y si tal vez ocurrieron pero no es el acusado por el cual si puede desvirtuarse.
12	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	Nosotros tenemos en el sistema libertad probatoria lo cual un hecho puede probarse con diferentes medios de prueba, pero el juez cuando admite y valora una prueba lo hace en un marco legal respetando principios uno de estos es la pertinencia lo cual el peritaje resulta más que pertinente en un delito informático lo cual si puede valorar que ese peritaje es útil y pertinente el cual si se puede valorar

Fuente: Elaboración Propia.

Cuadro 5 Transcripción de entrevista semiestructurada dirigida al Juez Segundo de Sentencia de Santa Ana.

ENTREVISTADO: GLD

FECHA: 02/05/2019 **HORA:** 8:30 am.

N.º	**PREGUNTA**	**REPUESTA**
1	¿Qué estudio posee sobre pericia informática?	Tengo 21 años de analizar prueba pericial, tengo dos cursos que fueron dados por la escuela de capacitación judicial sobre delitos informáticos, impartidos por agentes federales colombianos y americanos.
2	¿Qué capacitaciones recibe sobre actualización en tecnología de la información?	El año pasado recibí dos cursos de delitos informáticos y está pendiente una más avanzada, a los jueces nos están actualizando sobre delitos informáticos, son impartidos por la Ilea sede que está ubicada en San salvador impartida por cuatro federales y agentes adoc en la investigación de este tipo de delitos y las otros impartidos por los colombianos.
3	¿Cuál es el procedimiento para realizar un peritaje o un contraperitaje informático?	Se establece en el Art. 186 y sig. Pr.Pn. Se debe verificar la condición del perito que realizo esa pericia informática, para

		cualificarlo se necesita que diga qué tipo de capacitaciones tiene, cuanto tiempo de ejercer ese tipo de pericia, y otras cosas por ahí, no necesita juramentación porque son peritos técnicos permanentes. El proceso penal se ha diseñado de la siguiente manera: recolección u observación de la evidencia, luego verificación (realizado por los jueces de paz e instrucción, en las respectivas audiencias) y luego viene la tercera fase de comprobación; (Porque hoy el silogismo de que canta como pato, vuela como pato, pía como pato, camina como pato, es pato. Falso, puede ser un robot, puede ser una persona que se ha puesto un disfraz de pato y no es pato, hoy ese silogismo de prueba ya está superado) Hoy la prueba científica se analiza de esta manera: Recolección primera fase, verificación segunda fase y tercera fase comprobación. ¿Cómo se va a comprobar? Se comprueba lo recolectado u observado en aquellas investigaciones, se comprueba con la declaración y el sometimiento de un contra interrogatorio del perito que practico esa pericia, porque el papel por sí solo no habla, (no es Harry Potter que el papel habla) aquí en nuestro medio la realidad es que el perito que practique esa pericia informática debe de ser cuestionado de como hizo para que esa pericia llegara a incorporarse al proceso, de cómo se incorporó, la circunstancias en las que se investigó, personales tanto como de funcionamiento de la institución para la cual trabaja, entonces es una cualificación que se hace del perito.
4	¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o	Si existen, ya que está establecido en al art. 186 Pr.Pn. sí existen herramientas tanto en leyes nacionales e internacionales, hay herramientas para investigarlo, nosotros los

	contraperitaje?	jueces debemos estar pendientes de esas herramientas, que está proporcionando no solo la ley misma si no que del avance tecnológico que está existiendo a cada rato en este tipo de delitos. El delito informático, su investigación y comprobación se basa más que todo en prueba indiciaria científica (pero es científica, pero es prueba indiciaria) porque exactamente prueba directa se atreve a decir sin temor a equivocarse que es posible que no existe en muchos casos. La prueba indiciaria científica hace que un hecho desconocido sea un hecho conocido para poder deducir la responsabilidad penal a la persona que comete el delito utilizando medios informáticos. Claro hay prueba directa pero también la prueba científica en estos casos de informática también puede darse más la prueba indiciaria, y este es el punto, los jueces deben de capacitarse en prueba indiciaria porque muchos jueces penalistas no la manejan. Se da mucha injusticia porque la prueba indiciaria los jueces no la manejan. La prueba indiciaria nos lleva a una presunción judicial que deviene de la prueba indiciaria y la prueba indiciaria es aquella operación intelectual de prueba de análisis de prueba que hace el juez de toda la prueba indirecta que lleva a un solo punto, a ¿cuál punto? A que fulano de tal fue el responsable de esa acción criminal. Esta prueba analizada se hace una presunción judicial; no hay presunción legal solo una que es la presunción de inocencia es la única presunción y es una garantía constitucional que a toda persona acusada de delitos se le presume inocente, no hay otra

		presunción legal solo judicial que deviene del análisis de la prueba indiciaria o circunstancial.
5	¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?	Si, porque una vez detectada la huella de esa información de que IP salió es imposible botar una prueba de esa, ahora bien es de ver quien fue el que la manipulo, y para ello pues hay formas de llegar a esa persona, toda computadora y toda IP está registrada a nombre de una persona, y podemos llegar a pensar que si es de ella pero que no lo hizo ella, y bien vamos a ver la persona incriminada tiene que decir quien tuvo acceso a su aparto informático, debe decirlo. Es parecido a un accidente de tránsito donde la persona golpea a la otra y se va, nadie sabe nada de esa persona, pero a través de la placa podemos investigar que el propietario es fulano de tal, entonces el tema de la flagrancia si hay lesionados se va a buscar a esta persona, ahora bien encontrando a esta persona esta va decir como alegatos, -no, no fui yo, no soy yo. Pero ¿usted es dueño del vehículo?, ah entonces díganos a quien se lo presto, -ah no que no se lo puedo decir, es un sujeto que no conozco. Entonces se le enchucha y se le lleva al banquillo de los acusados. Entonces es el mismo análisis analógicamente es parecido, muy bien ¿usted es el dueño de la IP de donde salió esta información? - aja, ¿quién la manipulo entonces? -mi hijo, ¿Dónde está su hijo? ¿Venga usted hizo esto? -Si miré yo lo hice. Se investiga bien y se comprueba que fue él niño, no el padre, pero como el padre tiene registrada la IP, es el primero que se le busca. Ósea que hay formas de investigar el

		delito, los jueces debemos de esforzarnos un poco en analizar lo que es la prueba indiciaria y directa que es recabada a través de las experticias que en determinado momento se hacen.
6	¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?	El procedimiento del secuestro, es el proceso que se sigue, fiscalía ordena el secuestro de la IP, este solo tiene acceso el perito hay una de cadena de custodia lo cual garantiza que es el mismo aparato incautado en tales fechas, tal lugar y tales horas es el mismo al que se le practicara la experticia al mismo aparato que se sustraerá la información entonces esto debe de ser garantizado en la cadena de custodia que se debe de implementar esto a nivel procesal a nivel de protocolo la Policía Nacional Civil el laboratorio tiene sus protocolo, eso Uds. pueden irlo a investigar.
7	¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?	Probabilidades son mínimas, por ejemplo se metió a tu computadora e hizo una ilegalidad siempre hay huella, ¿cuál es la huella que se deja? El IP que utiliza ese hurto de información, ese hurto de esa IP para ponerla en algún otro lugar deja siempre una huella es imposible diría yo el que exista la posibilidad de falsear una información sin que el peritaje se dé cuenta. Si existe la corrupción, la corrupción es de seres humanos no es de las maquinas, no son los medios de información los corruptos, sino que son los seres humanos quien la manipula… Y sí, Podría. Para eso están los jueces para analizar este tipo de prueba. O sea, si se puede detectar, que se pueda hacer si se puede hacer pero que no se detecte ojo si se detecta.
8	¿Al momento de valorar la pericia	Si, si porque la informática es difícil, sabe porque inclusive las grabaciones es

	informática es posible comprobar los elementos del tipo penal?	imposible que alguien diga no fui yo, si es posible que diga yo estaba drogado cuando dije eso, ahí sí, porque esto (la grabación) no lo puede detectar, pero que no dijo lo que dijo es bien imposible, es prueba contundente.
9	¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?	Puede ser, Puede ofrecer la defensa. El proceso penal se divide en presunción de inocencia, inviolabilidad al derecho de la defensa técnica y material del imputado, tercera la verdad real el derecho que el imputado se defienda es inalienable en otras palabras la defensa técnica puede ofrecer prueba pericial para desvirtuar la prueba pericial que ha devenido de la investigación o del ente acusador. El defensor solicita al juez que juramente a un perito. Cuando esta judicializado el caso se le pide al juez directamente, y el juez ordena que se practique, con el perito nombrado y juramentado por el juez, que ha sido ofrecido por el defensor, solo que se hace en sede fiscal, porque los fiscales jamás se van a desplazar a casa del imputado o casa del defensor, lo hará en sede fiscal. Ahora bien, la mayoría de defensores por ejemplo aquí en Santa Ana no son muy acuciosos en eso, hemos tenido pocas contrapericias.
10	¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?	Si, la certeza es una valoración que tiene en su mente el juez sentenciador, el juez que celebre la vista pública, porque si no existe certeza existe probabilidad y con probabilidad no se le puede deducir responsabilidad a nadie, debe haber certeza. Y los jueces en cuestiones de experticia valoran perfectamente y acordémonos que las pericias son realizadas por personal “cualificado” y esa cualificación solo se puede extraer de lo que es la vista pública cuando es contra interrogado el perito, entonces debe de

		haber certeza y si no hay certeza obviamente se deja libre al imputado. Porque los jueces de paz valoran y analizan prueba pericial a efecto de encontrar probabilidad positiva, ¿porque probabilidad? Porque ahí no declara el perito, entonces la certeza solo se puede extraer en vista pública cuando declara el perito. Entonces los jueces de paz analizan y valoran la prueba, pero a efecto de encontrar probabilidad positiva o negativa, si encuentran probabilidad positiva lo mandan a juicio y si encuentran probabilidad negativa sobreseen al imputado.
11	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	Si puede presentarla, y tiene derecho a presentarla, que no lo hagan de hecho es una cosa, pero eso es de hecho , pero si tienen el derecho de hacerlo, haya está el artículo sobre eso que le digo el derecho la inviolabilidad a la defensa técnica y material del imputado, es un derecho que tiene el imputado de ofrecer prueba de descargo, aunque sea obligación de la fiscalía comprobar que el imputado es culpable, porque ya se le presume inocente, pero eso no quita o no resta las facultades del imputado y su defensor de ofrecer prueba pericial como para desvanecer los hechos que se le acusen al imputado.
12	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	No, necesita de otros elementos periféricos o indirectos no solo de una prueba sino de otros medios probatorios, en este delito especialmente se prueba con la pericia.

Fuente: Elaboración Propia

Cuadro 6 Transcripción de entrevista semiestructurada dirigida a Perito Informático del Laboratorio Técnico Científico de la Policía Nacional Civil, San Salvador.

ENTREVISTADO: OAEM

FECHA: 3/06/2019 **HORA:** 3:30 pm.

N.º	PREGUNTA	REPUESTA
1	¿Qué estudio posee sobre pericia informática?	Nosotros hemos recibido diferentes capacitaciones a nivel de la informática forense, estas capacitaciones las he recibido desde la creación de la sección de delitos tecnológicos en el año 2009, entre ellas he recibido el "curso básico de informática forense", cursos avanzados y especialidades sobre la materia, cursos que he recibido sobre cuestiones que versan sobre redes sociales, otros que tratan sobre respuesta a incidentes informáticos, el curso básico que debemos tener como perito para poder trabajar en la sección de delitos tecnológicos, es una capacitación para convertirse en perito de delitos tecnológicos, fue diseñado internamente y es impartido por el personal de la sección, luego esta capacitación es reforzada por personal internacional, ya sea del FBI, la ONU, de ABAROLI que es un colegio de abogados internacionales, también vienen los de INTERPOL, ya que estas instituciones dan cursos de informática forense básicos, avanzados, como por ejemplo hay un curso especial sobre redes sociales donde se utiliza una herramienta llamada GEOFEEDIA, que es utilizada para la red social Twitter, habiendo recibido los cursos y capacitaciones corresponde acreditarse y es la Policía la que acredita al personal para que pueda realizar los peritajes.

2	¿Qué capacitaciones recibe sobre actualización en tecnología de la información?	Es relativo no hay una respuesta especifica porque la tecnología es dinámica, por ejemplo el año pasado recibimos en la sección un curso avanzado sobre delitos tecnológicos, siempre el año pasado en el mes de diciembre realice una pasantía con la policía cibernética de Colombia y hace como tres años fui con la policía cibernética de México, lo que me permite ver una brecha entre las tecnologías de aquellos años y las que hay en la actualidad, estos países sirven de referencia para actualizar nuestra tecnología y se toman como base para solicitar equipo y capacitaciones, por ejemplo una institución llamada Justice Education Society es la que apoya a la sección en todo lo relacionado a "video", la 1DC capacita en todas las cuestiones relacionadas con la informática, en cuestiones procedimentales está el colegio de abogados ABAROLI, el FBI capacita sobre respuesta de incidentes, o sea depende el enfoque así es la institución que apoya en capacitaciones y equipo.
3	¿Cuál es el procedimiento para realizar un peritaje o un contraperitaje informático?	En la sección tenemos establecidos procedimientos específicos a realizar dependiendo del área que se solicite, estos procedimientos han sido creados internamente basándose en procedimientos aceptados por la comunidad forense internacional, se toman como base los manuales de procedimientos creados por otros países y se adecuan a nuestra realidad y a nuestra legislación. La sección trabaja con 3 áreas: computo, video y telefonía, no trabajamos con "audio" porque no se cuenta con capacitaciones, equipo, ni software para ese tipo de análisis, por ejemplo para el caso de computo: el procedimiento consiste en recibir el video o archivos y realizar una copia bit a bit que básicamente es una copia íntegra del archivo y se trabaja en esta copia y la razón es porque el archivo original puede ser sometido a contraperitaje y así se evita que se dañe, ya en la copia se buscan los elementos peticionados por investigador, fiscalía o

		juzgado.
4	¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje?	Hay que hacer una diferencia entre la existencia de los recursos tecnológicos y que se cuente con ellos, en esencia no se cuenta con un 100% de equipo y aquellos que se tienen si bien es cierto permiten la práctica de un peritaje estos son lentos lo que genera una tardanza en el análisis, de modo que no se está actualizado con las últimas versiones en equipo en la sección.
5	¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?	En la sección no se identifican personas, sino que se identifican usuarios, y si bien es cierto en los delitos informáticos se realiza un método forense, también se utilizan los medios tradicionales de investigación, hay que ir al lugar y verificar que la persona con el usuario reside en cierta casa de habitación, por otro lado un hecho irrefutable sobre la criminalística es que ninguna evidencia por si sola resuelve un caso, por ejemplo se pueden encontrar huellas pero también algún video para demostrar que la persona estuvo ahí, testimonios o algún otro tipo de prueba y el conjunto de videncia es la que sirve para demostrar el hecho.
6	¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?	Los del laboratorio no concurrimos a la escena del delito sino que son los de criminalística de campo los que incautan la evidencia y realizan una recolección, hay casos especiales donde si vamos a la escena del delito pero son casos bien especiales por ejemplo cuando el servidor es demasiado grande, esto impide que puede ser incautado por ende nosotros como peritos vamos a la escena del hecho y hace una búsqueda de los datos específicos que se necesitan y se hace una extracción directa del servidor, pero la regla general es que primero se realiza una incautación y luego se aplican los protocolos y manuales de procesamiento de la escena del delito, luego se aplican los procedimientos de cadena de

		custodia, esto implica la identificación de la evidencia, el embalaje, va a trasladar la evidencia y llenara los formularios, lleva la evidencia a la sección de recepción de evidencia y esta verifica que cumpla con todos los requisitos y que se especifique el tipo de análisis, luego la recepción se comunica con la sección de delitos tecnológicos, aquí en la sección se delega a alguien para que recoja la evidencia, se ingresan todos los datos de la evidencia en el sistema, luego la evidencia va a bodega y se espera a que yo como jefe de sección asigno al perito que practicara el análisis, y será este el que pondrá en práctica los manuales y procedimientos de análisis para el caso específico del que se trate, luego de practicado el análisis se embala de nuevo y se reenvía a recepción de evidencia, ellos se ponen en contacto con el usuario que solicito el análisis y le devuelven la evidencia que posteriormente se presenta en juicio, en otros casos la evidencia no se devuelve sino que se destruye, esto depende del tipo de delito que se está investigando por lo general cuando se trata de droga se destruye, pero con la nueva ley de extinción de dominio lo que hacemos es repartir los objetos, pero los teléfonos y computadoras por lo general se destruyen, a menos que alguien lo solicite se devuelve.
7	¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?	Aclaro que luego de realizar todo el procedimiento de análisis encontrar los resultados a esa información se le genera un valor HASH, haciendo una analogía un valor hash podría ser como una firma digital, esto lo hacemos para garantizar que la información obtenida no ha sido alterada, y es en la vista pública donde se confronta ese valor hash con lo plasmado en el informe, si hay una diferencia en esos dato significa que a información fue alterada, nosotros como peritos garantizamos el trabajo a través de ese valor hash, pero puede darse el caso que en el transcurso de la evidencia esta sea alterada eso ya está fuera del alcance de nosotros, por ejemplo se realiza un allanamiento el 1 de junio, la maquina incautada se apaga ese día y se

		remite a la sección el día 4 y se le practican los análisis el día 6, pero cuando se le realiza la copia bit a bit a los archivos se verifica que tuvo ingreso la fecha 3 de junio, esto significa que tuvo manipulación posterior a su incautación, pero eso ya está fuera del alcance de nosotros como peritos y lo que se hace es plasmarlo en el informe, también puede darse el caso que cuando se envié la información y se confronte en la vista pública no sea la misma, la evidencia puede ser enviada en soporte digital ya sea CD o USB y se confirma que no es la misa evidencia porque los valores HASH no coinciden aunque el CD sea el mismo que el perito envió pero su contenido ya fue alterado y esto puede suceder en el traslado de la información, hasta el momento esto no se ha dado pero puede suceder.
8	¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?	Es relativo porque se puede determinar que un usuario ha ingresado a un sistema, si lo vemos desde el tipo penal estafa y viene alguien y quiere que en cierto equipo se ha dado el delito de estafa en contra de una persona, lo que en realidad la sección hace es recolectar información como fotos, correos o cualquier información que haya pasado por el equipo que compruebe que el usuario tal tuvo comunicación con otro usuario tal, para este caso específico el perito informático no puede decir que se cometió el delito de estafa, eso lo dirá el perito contable; para el caso de los amaños lo que va a determinar que se dio el delito puede ser alguna conversación que quedo registrada en algún aparato como una Tablet, pero será el juzgador quien defina si en esa conversación hablaba de que le daban cierta cantidad por fallar un gol y por ende será el juzgador quien defina si existió el delito, pero hay casos como el de Pornografía infantil donde el perito al realizar el análisis a la maquina encuentra imágenes y videos pornográficos y al mismo tiempo está identificando el delito, pero en otros casos no puede el perito informático identificar el delito sino que es otro perito especializado en la

		materia quien puede hacerlo.
9	¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?	No se da y del 100% de las vistas públicas a las que los peritos de la sección hemos asistido se ha dado un 10% se ha tenido un contraperitaje, y este no consiste en la entrega de la evidencia a una persona y esta realizara la práctica del análisis, sino que se coordina pidiendo un permiso y se asigna a un perito y la persona solicitante llega a la sección de delitos tecnológicos, la limitante de un defensor o un perito de la defensa son los software y los equipos puesto que son sumamente caros por ejemplo el de uso de la institución su valor es de 40000 dólares y pueda que la defensa no cuente con este equipo o pueda que no tenga el software y si lo tiene no está autorizado para usarlo, por lo general la defensa se limita a verificar los procedimientos realizados por la sección y si realiza el análisis con un software diferente obtendrá otros resultados mejores o más limitados, la sección utilizamos los lineamientos institucionales basados en los manuales de procedimientos aceptados por la comunidad forense y eso los lleva a obtener los resultados que se presentan, y por eso en la mayoría de casos la defensa llega a la sección observa los procedimientos y si tiene algo que refutar solo pregunta porque se hizo tal cosa, pero desde la formación de la sección en el año 2009 nunca se hemos tenido un contraperitaje, para que eso sucediera tendríamos que renunciar alguno de la sección y dedicarnos a eso, por ejemplo balística tiene IBIS cosa que nadie más tiene, por otro lado un perito dactiloscopista se forma en el laboratorio y en ningún otro lado y para que alguien se dedique a esto tendría que renunciar alguien de los dactiloscopistas que están en laboratorio y dedicarse a hacer ese tipo de peritajes.
10	¿Existe claridad en el juez al valorar la pericia informática	A veces los jueces no tienen bien clara la parte tecnológica, pero existen otros que se han comprometido bastante y tiene muy buen conocimiento y esto les ayuda a valorar, aunque

	sobre la certeza de participación del imputado?	según la postura del perito depende de la forma en la que fiscalía presenta la evidencia, por ejemplo el caso de feminicidio, el primer caso que se judicializo no fue tomado en cuenta como feminicidio por la forma en la que fiscalía lo presento, no presento la autopsia y para demostrar que había una mujer muerta había que presentarla, cosa que fue refutada por el juez, por otro lado en la pericia el perito puede obtener los mejores resultados pero si fiscalía no hace la presentación en tiempo y de la manera pertinente el juez no la va a valorar de la manera adecuada, si existe un buen número de jueces que hacen buenas valoraciones, por ejemplo en el área de videos ha habido condenas aun sin testigos o sea que han sido solo sobre la base de videos, en el caso de la informática el juez se auxilia de otra persona que le traduce de manera entendible la terminología para poder valorar la evidencia.
11	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	A través de la informática no se puede demostrar que la persona que ingresa a una maquina con un usuario y contraseña es la dueña del usuario o sea no se puede decir que la persona que utilizo el usuario es la autorizada para tal fin, solo se puede decir que el usuario tal fue quien realizo una modificación en el sistema y por eso en la sección solo se identifican usuarios no personas, por ende la defensa más que todo se debe enfocar en demostrar que si bien es cierto que el usuario de su cliente fue utilizado, no fue su defendido quien lo utilizo y para ello se debe apoyar en otras pruebas como por ejemplo videos o testigos que afirmen otros hechos contrarios a los que le acusan.
12	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?	No pues es necesario acompañarse de otras pruebas que valoradas en su conjunto llevan a generar la certeza en el juez para resolver el juicio.

Fuente: Elaboración Propia.

4.2. Matriz de análisis de resultados.

MATRIZ DE ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS **La información que se ha trasladado a esta matriz ya ha pasado por un proceso de depuración a través de la aplicación de la prueba semáforo sobre lo que han aportado los informantes con el propósito de desarrollar el análisis y llegar a las conclusiones respectivas.**				
N.º	PREGUNTA	REPUESTAS	CATEGORÍAS	ANÁLISIS
1	¿Qué estudios posee sobre pericia informática?	R/(1).- Sobre eso lo que le puedo contestar es que hemos recibido una capacitación sobre delitos informáticos y dentro de los delitos informáticos hemos analizado la prueba informática. R/(2).- Realmente medio recibí una charla informativa sobre la pericia informática, por los mínimos estudios que dan sobre la pericia informática. R/(3).- En el caso del fiscal le corresponde saber y conocer cómo se investiga un delito informático, y por eso es que nosotros somos formados en diversos cursos sobre como investigar este tipo de delitos.	Pericia Informática.	En cuanto a la pregunta ¿Qué estudios posee sobre pericia informática? Los informantes clave 1-3-5-6 expresan que han recibido capacitaciones sobre delitos informáticos, y los informantes clave 2 y 4 expresan el dos que medio recibió una charla y el cuatro dice que no. De las respuestas obtenidas se puede inferir que Fiscales y Jueces han recibido capacitaciones sobre delitos informáticos pero no específicamente sobre pericia informática, y en el caso del defensor particular no posee estudios sobre pericia informática, en consecuencia a cuatro años de que esta en vigencia la Ley Especial Contra los

		R/(4).- No una preparación intensiva, pero si cursos básicos orientados a valoración y admisión de prueba. R/(5).- Tengo dos cursos que fueron dados por la Escuela De Capacitación Judicial sobre delitos informáticos, impartidos por agentes federales colombianos y americanos. R/(6).- Nosotros hemos recibido diferentes capacitaciones a nivel de la informática forense, estas capacitaciones las hemos recibido desde la creación de la sección de delitos tecnológicos en el año 2009, entre ellas he recibido el "curso básico de informática forense", cursos avanzados y especialidades sobre la materia, cursos sobre redes sociales, otros sobre respuesta a incidentes informáticos, el curso básico que debemos tener como perito para poder trabajar en la sección de delitos tecnológicos,		Delitos Informáticos y Conexos, aún existen demasiadas dudas y desconocimiento sobre la pericia informática, no se han orientado capacitaciones sobre esta temática y si bien es cierto jueces y fiscales expresan haber recibido capacitaciones han sido estas sobre temas generales no han desarrollado lo medular de la ley que es la pericia informática.

		es una capacitación que fue diseñada internamente y es impartida por el personal de la sección, luego esta capacitación es reforzada por personal internacional, ya sea del FBI, la ONU, de ABAROLI, también vienen los de INTERPOL, ya que estas instituciones dan cursos de informática forense básicos y avanzados.		
2	¿Qué capacitaciones recibe sobre actualización en tecnología de la información?	R/(1).- Actualmente sobre esa, capacitaciones ningunas, solo lo que yo puedo hacer particularmente. R/(2).- No he recibido capacitaciones meramente de los delitos informáticos por lo que se debería buscar una institución que este informando a los profesionales dando la información correcta o hiciera los estudios y actualizaciones tecnológicas de la informática. R/(3).- Actualmente se realizan muchos cursos orientados a que los fiscales conozcan		En cuanto a la pregunta ¿Qué capacitaciones recibe sobre actualización en tecnología de la información? Los informantes claves 1-2 responden que ninguna, mientras que los informantes 3-4 y 5 responden que si reciben cursos sobre como ofertar la prueba o sobre delito informático y solo el informante 6 responde que ha recibido cursos avanzados por la Policía Cibernética de Colombia y México. De lo expuesto se concluye que tanto la Fiscalía y Jueces solo reciben capacitaciones generales sobre los

		como investigar los delitos informáticos por ejemplo el Curso Especializado sobre Técnicas de Investigación del Delito Informático. R/(4).- Un par de cursos sobre todo como se debe manejar el ofertorio y la admisión de la prueba para no violentar derechos y garantías. R/(5).- El año pasado recibí dos cursos de delitos informáticos y está pendiente uno más avanzado, a nosotros los jueces nos están actualizando sobre delitos informáticos, son impartidos por la Ilea sede que está ubicada en San salvador impartida por cuatro federales y agentes adoc en la investigación de este tipo de delitos y las otros impartidos por los colombianos. R/(6).- Es relativo no hay una respuesta especifica porque la tecnología es dinámica, por ejemplo el año pasado recibimos en la sección un curso avanzado sobre delitos		delitos informáticos, específicamente sobre el manejo de la prueba informática, pero no sobre actualización en las nuevas tecnologías, por otro lado los defensores públicos y privados no reciben cursos ni capacitaciones de parte de ninguna institución. El único que recibe capacitaciones sobre nuevas tecnologías es perito informático del Laboratorio Técnico Científico de la Policía Nacional Civil, esto implica que es el único que conoce las nuevas tecnologías y herramientas para el manejo de la evidencia digital producto de los delitos informáticos.

3	¿Cuál es el procedimiento para realizar un peritaje o un contraperitaje informático?	tecnológicos, siempre el año pasado en el mes de diciembre realice una pasantía con la policía cibernética de Colombia y hace como tres años fui con la policía cibernética de México, lo que me permite ver una brecha entre las tecnologías de aquellos años y las que hay en la actualidad, estos países sirven de referencia para actualizar nuestra tecnología y se toman como base para solicitar equipo y capacitaciones. R/(1).- El procedimiento normal depende de a quien le interesa, si es a la defensa que le interesa lo solicita la defensa al juez, y si es a fiscalía será el ente público quien lo solicite al juez, y hay casos donde el juez autoriza al fiscal que realice la prueba informática, y le pide al ente fiscal que comunique o notifique a la parte contraria la diligencia a realizar, cabe destacar que no se realiza el mismo día la pericia, sino que se va a las oficinas de la policía en San Salvador, haya se constituyen las partes y se entrega el aparato, el perito lo		En cuanto a la pregunta ¿Cuál es el procedimiento para realizar un peritaje o un contraperitaje informático? Los informantes claves 1-2-3-4-5 expresan que el procedimiento es el normal el que regula el Código Procesal Penal, en cambio para el informante 6 o sea para el perito informático explica en esencia cual es el procedimiento destacando que en el laboratorio trabajan con tres áreas siendo estas:

		toma y se compromete en otra fecha en enviar el resultado. R/(2).- Están establecidos en el Código PrPn, hay que hacer petición al juez competente, a él se le piden los peritajes, el contraperitaje es la defensa quien propone perito en este caso que sepa de delitos informáticos. R/(3).- El procedimiento ya lo establece el Código Procesal Penal, va depender la pericia que se requiera, se solicita la autorización del juez, el juez nombra los peritos, las dos partes tienen derecho a proponer y una vez se selecciona los peritos estos se juramentan, si no son peritos permanentes se juramentan y se les da un plazo para que emitan dictamen R/(4).- Para el fiscal o parte interesada procede a señalar algún soporte técnico donde este contenida alguna información, que se crea útil para una investigación el		computo, video y telefonía, explica cómo se realiza el peritaje informático. Con base a las respuestas de los informantes claves se puede concluir que tanto jueces, fiscales y defensores no conocen el procedimiento para realizar el peritaje o contraperitaje informático, incluso sostienen que cada parte tiene derecho a nombrar un perito, pero de dónde saca la defensa un perito informático si los únicos que desarrollan las pericias son los del laboratorio, es evidente que desconocen estas circunstancias tanto jueces como fiscales, el único que lo conoce detalladamente es el perito informático del Laboratorio Técnico Científico de la Policía Nacional Civil.

		procedimiento es que se incauta y el fiscal solicita al juez la autorización para sustraer la información del lugar donde se crea que este, para garantizar el debido proceso para no violentar derechos y garantías si al juez le parece lo autoriza y se nombra perito con conocimientos en la materia. R/(5).- Se establece en el Art. 186 y sig. Pr.Pn. El proceso penal se ha diseñado de la siguiente manera: recolección u observación de la evidencia, luego verificación (realizado por los jueces de paz e instrucción, en las respectivas audiencias) y luego viene la tercera fase de comprobación; Hoy la prueba científica se analiza de esta manera: Recolección primera fase, verificación segunda fase y tercera fase comprobación. ¿Cómo se va a comprobar? Se comprueba lo recolectado u observado en aquellas investigaciones, se comprueba con la declaración y el sometimiento de un contra		

		interrogatorio del perito que practico esa pericia, aquí en nuestro medio la realidad es que el perito que practique esa pericia informática debe de ser cuestionado de como hizo para que esa pericia llegara a incorporarse al proceso, de cómo se incorporó, la circunstancias en las que se investigó, personales tanto como de funcionamiento de la institución para la cual trabaja, entonces es una cualificación que se hace del perito. R/(6).- En la sección tenemos establecidos procedimientos específicos a realizar dependiendo del área que se solicite, estos procedimientos han sido creados internamente basándose en procedimientos aceptados por la comunidad forense internacional, se toman como base los manuales de procedimientos creados por otros países y se adecuan a nuestra realidad y a nuestra legislación.		

4	¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje?	La sección trabaja con 3 áreas: computo, video y telefonía, no trabajamos con "audio" porque no se cuenta con capacitaciones, equipo, ni software para ese tipo de análisis, por ejemplo para el caso de computo: el procedimiento consiste en recibir el video o archivos y realizar una copia bit a bit que básicamente es una copia íntegra del archivo y se trabaja en esta copia y la razón es porque el archivo original puede ser sometido a contraperitaje y así se evita que se dañe, ya en la copia se buscan los elementos peticionados por investigador, fiscalía o juzgado. R/(1).- Podemos decir que en un 75% o 90% que se cuentan con los recursos posiblemente, pero hay limitantes que nos impiden hablar de un 100%. R/(2).- En el país es bien escaso, aquí no hay	Problemas Probatorios	En cuanto a la pregunta ¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje? Los informantes clave 1-3 explican que si existen, en cambio el informante 2 dice que es escaso, el informante cinco confunde las herramientas que contempla la ley para procesar a una persona por un

		una empresa que diga, nosotros somos la empresa informática en la cual vamos a la vanguardia con la información tecnológica y nosotros podemos dar peritajes, somos especialistas en eso, nosotros hemos pagado aplicaciones para realizar esos procesos. El país no tiene para hacer eso, la fiscalía tiene una herramienta que es la Policía Técnica Científica, pero de técnica y científica deja mucho en que dudar. R/(3).- Los recursos si existen, pero obviamente no son suficientes para las exigencias de los delitos que actualmente se cometen. R/(4).- La Policía y fiscalía están en esa lucha en busca de un equipamiento, como algunas organizaciones, fundaciones internacionales, ya que acá, ya no solo necesitamos prueba en los procesos penales como la confesión o pruebas testimonial, sino que se ha ido		delito o falta, con los insumos necesarios para practicar un peritaje o contraperitaje informático, por su parte los informantes 4 y 6 responden que se está en un proceso de equipamiento de insumos suficientes y necesarios. De lo anterior se puede inferir que si existen recursos mínimos para practicar un peritaje informático.

		modernizando de las pruebas científicas y entramos hablar de la admisión de las pruebas tecnológicas en lo que parece que se empieza a entrar en transición, en lo cual se encuentran de una manera en adquisición y equipamiento de los insumos suficientes y necesarios para darles tramite a estos peritajes. R/(5).- Si existen, ya que está establecido en al art. 186 Pr.Pn. sí existen herramientas tanto en leyes nacionales e internacionales, hay herramientas para investigarlo, los jueces deben estar pendientes de esas herramientas, que está proporcionando no solo la ley misma si no que del avance tecnológico que está existiendo a cada rato en este tipo de delitos. El delito informático, su investigación y comprobación se basa más que todo en prueba indiciaria científica (es científica, pero es prueba indiciaria) .La prueba indiciaria científica hace que un hecho desconocido sea		

		un hecho conocido para poder deducir la responsabilidad penal de la persona que comete el delito utilizando medios informáticos. La prueba indiciaria nos lleva a una presunción judicial y la prueba indiciaria es aquella operación intelectual de análisis de prueba que hace el juez de toda la prueba indirecta que lleva a un solo punto, Esta prueba analizada se vuelve una presunción judicial; no hay presunción legal solo una que es la presunción de inocencia es la única presunción y es una garantía constitucional que a toda persona acusada de delitos se le presume inocente, no hay otra presunción legal solo judicial que deviene del análisis de la prueba indiciaria o circunstancial. R/(6).- Hay que hacer una diferencia entre la existencia de los recursos tecnológicos y que se cuente con ellos, en esencia no se cuenta con un 100% de equipo y aquellos que se tienen si bien es cierto permiten la práctica de		

5	¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?	un peritaje estos son lentos lo que genera una tardanza en el análisis, de modo que no se está actualizado con las últimas versiones en equipo en la sección. R/(1).- Eso es lo discutible, que nos lleva a una discusión donde la prueba no le refleja los hechos reales sino que le va a reflejar que existe una información en un medio informático, pero que no precisamente este medio dirá que el hecho es real, en esencia la pericia informática dirá que sucedió una alteración pero no definirá quien la realizó. R/(2).- Las herramientas de software si, el problema es aquí no las podemos utilizar, aquí no utilizamos las herramientas de software, porque los softwares son creaciones de otros países más avanzados, pero hablando en sí de las herramientas si puede hacerse, pero aquí las utilizamos mal o no las tenemos.		En cuanto a la pregunta ¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió? Al respecto los informantes clave 2-3-4 y 5 responden que si, en cambio el informante 1 dice que es discutible, y el informante 6 dice que ninguna evidencia por si sola resuelve un caso. El grupo investigador infiere que las herramientas de software en el peritaje o contraperitaje informático puede establecer que ha sucedido, es decir la pericia informática puede dejar claro que efectivamente ha existido una violación o transgresión a la ley en base a la evidencia encontrada en un medio o soporte informático, aclarando en todo caso que con ello no se está definiendo la

		R/(3).- Si eso va a depender mucho del tipo de pericia que se está requiriendo porque generalmente nosotros encontramos evidencias, pero obviamente las evidencias hay que analizarlas. R/(4).- Si porque en un software queda la evidencia, entonces me parece que si hay herramientas para sustraer la información real y veraz y puede depender en muchos casos, en primer lugar del tipo de equipo que se trate en donde se encuentre el soporte del software, en segundo lugar de la astucia de la persona que maneja la información llámese persona investigada o procesada. R/(5).- Si, porque una vez detectada la huella de esa información de que IP salió es imposible botar una prueba de esas, ahora bien es de ver quien fue el que la manipulo, y para ello pues hay formas de llegar a esa persona, toda computadora y toda IP está registrada a nombre de una persona, y		participación del imputado en vista que una evidencia por sí sola no resuelve el caso.

6	¿Cuál es el protocolo que se sigue en El Salvador para la extracción,	podemos llegar a pensar que si es de ella pero que no lo hizo ella, y bien vamos a ver la persona incriminada tiene que decir quien tuvo acceso a su aparto informático, debe decirlo. Ósea que hay formas de investigar el delito, los jueces debemos de esforzarnos un poco en analizar lo que es la prueba indiciaria y directa que es recabada a través de las experticias que en determinado momento se hacen. R/(6).- En la sección no identificamos personas, sino que identificamos usuarios, y si bien es cierto en los delitos informáticos se realiza un método forense, también se utilizan los medios tradicionales de investigación, hay que ir al lugar y verificar que la persona con el usuario reside en cierta casa de habitación, por otro lado un hecho irrefutable sobre la criminalística es que ninguna evidencia por si sola resuelve un		En cuanto a la pregunta ¿Cuál es el

	transporte y presentación de la pericia informática?	caso. R/(1).- No hay un procedimiento establecido, va dependiendo de cuál prueba informática se trate, porque pueden haber otras; para el caso de las extorciones intervienen las llamadas, y cuando se incautan objetos el fiscal hace una petición al juez que le autorice el vaciado de la información a través del perito, es entonces que el juez ordena la práctica de esta diligencia y hay casos donde se constituyen las partes en el juzgado, se juramenta al perito y este se lleva el aparato y posteriormente él hace llegar esa información al juzgado, esto nos demuestra que quien ejerce la cadena de custodia sobre los objetos secuestrados es el perito, y cuando este no puede entregar la información se la da a otro compañero que casualmente se dirige para el lugar donde se tiene que entregar esta y con dicha acción rompe la cadena de custodia.		protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática? El informante clave 1 dice que no hay un procedimiento establecido, en cambio los informantes clave 2-3-4-5-6 en esencia responden que es el procedimiento de extracción, embalaje y cadena de custodia regulado en el Código Procesal Penal, sin hacer alusión a los protocolos internacionales existentes para la práctica de una pericia informática. De las respuestas obtenidas se concluye que los informantes clave en realidad desconocen la existencia de esos protocolos, asimismo confirma que en el país no existe un protocolo que se utilice en los casos de delitos informáticos para el manejo, traslado y presentación de la evidencia digital, sino que se utiliza el procedimiento

		R/(2).- Cuando habla de protocolo es el procedimiento que se hace de extracción y transporte, que es a través de una solicitud que se hace primeramente al tribunal para nombramiento de un perito, de ahí se le da la comisión de extracción desde el nombramiento, al perito se manda a que haga el peritaje con los elementos que él tiene por allá, no sé cuáles son los que tenga, es el que menos sabe que software tiene, hoy últimamente para observaciones de firma tienen la lupa, la lupa y la lupa y a eso le dan fe, una lupa cualquiera la puede tener pero no un buen conocimiento y en cuanto a los software debe tener conocimiento tecnológico sobre eso y aquí fallamos en ese punto. R/(3).- Existe un capítulo en el Código Procesal Penal sobre cadena de custodia, cuando se extrae, se incauta cualquier evidencia se llena una cadena de custodia y		reglado en el proceso penal, aplican las normas del derecho común.

		esa es la que nos da a nosotros fe de que la evidencia que se incauto es la misma que llegue al juicio, de manera que en cada eslabón que va pasando la evidencia se debe de dejar un registro de quien tuvo la evidencia, para que fines y eso llega hasta el juez y por eso es que el juez puede al final dictaminar que la evidencia que se incautó y se analizo es la misma que haya llegado a juicio. R/(4).- Ahora tenemos un sistema acusatorio, esa carga corre por cuenta del fiscal por ser el que investiga, ubica y señala, los equipos donde estén estas investigaciones, entonces es el a través de la PNC y sus unidades especializadas de la policía quien incauta luego de eso procede a elaborar la cadena de custodia y la conservación de esos software o material sujeto a peritaje queda en poder del fiscal y él solicita al juez este peritaje y el juez lo autoriza y nombra al perito que haya propuesto la fiscalía, pero todo la incautación		

		y procedimiento de conservación y embalaje queda por cuenta de fiscal y perito. R/(5).- El procedimiento del secuestro, es el proceso que se sigue, fiscalía ordena el secuestro de la IP, este solo tiene acceso el perito hay una de cadena de custodia lo cual garantiza que es el mismo aparato incautado en tales fechas, tal lugar y tales horas es el mismo al que se le practicara la experticia al mismo aparato que se sustraerá la información, entonces esto debe de ser garantizado en la cadena de custodia que se debe de implementar esto a nivel procesal a nivel de protocolo la Policía Nacional Civil el laboratorio tiene sus protocolos. R/(6).- Los del laboratorio no vamos a la escena del delito sino que son los de criminalística de campo los que incautan la evidencia y realizan una recolección, hay casos especiales donde si vamos a la escena del delito pero son casos bien especiales por		

		ejemplo cuando el servidor es demasiado grande, esto impide que puede ser incautado por ende nosotros como peritos vamos a la escena del hecho y hacemos una búsqueda de los datos específicos que se necesitan y se hace una extracción directa del servidor, pero la regla general es que primero se realiza una incautación y luego se aplican los protocolos y manuales de procesamiento de la escena del delito, luego se aplican los procedimientos de cadena de custodia, se lleva la evidencia a la sección de recepción de evidencia y esta verifica que cumpla con todos los requisitos y que se especifique el tipo de análisis, luego pasa a la sección de delitos tecnológicos, se ingresan todos los datos de la evidencia en el sistema, luego la evidencia va a bodega y luego yo como jefe de sección asigno al perito que practicara el análisis, y será este el que pondrá en práctica los manuales y procedimientos de análisis para el caso específico del que se trate, luego de		

7	¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?	practicado el análisis se embala de nuevo y se reenvía a recepción de evidencia, ellos se ponen en contacto con el usuario que solicito el análisis y le devuelven la evidencia que posteriormente se presenta en juicio, en otros casos la evidencia no se devuelve sino que se destruye. R/(1).- Digamos que si el peritaje informático si se hace dentro de un procedimiento normal y usando las herramientas idóneas, tiene un 100% de confiabilidad, aún más que el ADN porque este arroja un 99.99% y se da por establecida la paternidad, pero aunque este peritaje de un 100% hay que tomar en cuenta que la prueba está sujeta a manipulación y es entonces donde puede haber posibilidades de falsear una información. R/(2).- Probabilidades son muchas pero muchas, el problema aquí es que el defensor no se da cuenta que lo han falseado, si aquí vienen caso donde dicen lo reconoció una persona porque se lo mostramos en una base		En lo que se refiere a la pregunta ¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático? Los informantes claves responden el 1 que si se hace dentro del procedimiento normal y con herramientas idóneas es confiable en 100% pero se puede falsear porque la prueba está sujeta a manipulación esto implica que en algún punto pueda ser alterada. En ese mismo sentido responde los informante 2-3-4 y 5, ya que consideran que existen posibilidades de falsear la pericia informática, por otro lado el informante 6 o sea el perito informático responde que ellos cuentan con las herramientas que les permiten garantizar la credibilidad de

		de datos y yo tengo unos donde han mostrado bases de datos pero el testigo dice otra cosa ah! presumen que esta es, pero la prueba presuntiva no la admite nuestro código aquí o se prueba o no se prueba. R/(3).- En esta materia, en cualquier otra materia alguien puede falsear una evidencia, una prueba. R/(4).- Si esta un equipo que ha sido incautado respetando derechos y garantías, hay una debida cadena de custodia, hay una conservación y un perito con habilidades y destrezas que maneje el tema, las posibilidades son mínimas pero en todo caso existen falencias que puedan permitir que esas debilidades vayan incrementándose por el uso de las tecnologías y de las herramientas. R/(5).- Probabilidades son mínimas por		la pericia informática, y es posible acreditar que el resultado de esta no ha sido alterado, el perito aclara que garantiza la pericia, pero agrega que si la información ya llego a sus manos alterada el resultado de la pericia no será el correcto y se plasmara en el dictamen pericial la alteración previa, por ende se concluye que la evidencia digital puede ser alterada antes o después de estar en las manos del perito, más tomando en cuenta que no se tienen definidos protocolos de manejo de la evidencia digital..

		ejemplo se metió a tu computadora e hizo una ilegalidad siempre hay huella, ¿cuál es la huella que se deja? El IP que utiliza ese hurto de información, ese hurto de esa IP para ponerla en algún otro lugar deja siempre una huella es imposible diría yo el que exista la posibilidad de falsear una información sin que el perito se dé cuenta. Si existe la corrupción, la corrupción es de seres humanos no es de las maquinas, no son los medios de información los corruptos, sino que son los seres humanos quienes los manipulan. Y sí, Podría. Para eso están los jueces para analizar este tipo de prueba. R/(6).- Aclaro que luego de realizar todo el procedimiento de análisis y encontrar los resultados a esa información se le genera un valor HASH, haciendo una analogía un valor hash podría ser como una firma digital, esto lo hacemos para garantizar que la información obtenida no ha sido alterada, y es en la vista pública donde se confronta ese		

	¿Al momento de	valor hash con lo plasmado en el informe, si hay una diferencia en esos datos significa que a información fue alterada, nosotros como peritos garantizamos el trabajo a través de ese valor hash, pero puede darse el caso que en el transcurso de la evidencia esta sea alterada eso ya está fuera del alcance de nosotros, por ejemplo se realiza un allanamiento el 1 de junio, la maquina incautada se apaga ese día y se remite a la sección el día 4 y se le practican los análisis el día 6, pero cuando se le realiza la copia bit a bit a los archivos se verifica que tuvo ingreso la fecha 3 de junio, esto significa que tuvo manipulación posterior a su incautación, pero eso ya está fuera del alcance de nosotros como peritos y lo que se hace es plasmarlo en el informe, también puede darse el caso que cuando se envié la información y se confronte en la vista pública no sea la misma, la evidencia puede ser enviada en soporte digital ya sea CD o USB y se confirma que no es la misa		

8	valorar la pericia informática es posible comprobar los elementos del tipo penal?	evidencia porque los valores HASH no coinciden aunque el CD sea el mismo que el perito envió pero su contenido ya fue alterado y esto puede suceder en el traslado de la información, hasta el momento esto no se ha dado pero puede suceder. R/(1).- Esto es discutible porque los verbos rectores de un tipo penal están establecidos legalmente y uno de los elementos de prueba es la prueba informática, pero no es solo esta sino que existen otros medios de prueba, incluso la ley permite la incorporación de otros medios de prueba al proceso penal siempre y cuando este dentro de las normas y requisitos de la prueba del Código Penal. R/(2).- Los elementos objetivos del tipo penal esos hay que establecerlos, los elementos subjetivos habría que determinarlos, cuáles de los elementos subjetivos de los tipos penales se pueden estar comprobando con lo	Administración de justicia.	En cuanto a la pregunta ¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal? Los informantes clave responden, el numero 1 dice que es discutible si se pueden comprobar o no los elementos del tipo penal además agrega que hay otros medios de prueba no solo este, en ese mismo sentido responde el informante 6 quien expresa que es relativo y aclara haciendo una diferenciación entre los casos que es posible definir con la pericia el tipo penal, cita el caso de la estafa donde no es posible, asimismo cuando se trata de amaños y a pesar que se encuentre información en un soporte electrónico no será el perito quien identifique el tipo penal sino que

		que es el peritaje informático y extraerlos, ejemplo: mire aquí dijo esto y lo dijo esta persona, ese es el elemento subjetivo ahora bien vamos a los elementos objetivos a ver si esos también se pueden establecer eso se determinara a través del medio probatorio que tengamos en ese momento. R/(3).- En el caso que sea contundente pues es claro que sí, pero como probar los hechos no depende solamente de una prueba en lo particular si no que una prueba en este caso una pericia tecnológica pues en un proceso puede ser una de una gama de evidencias que son sometidas a la valoración del juez. R/(4).- Si porque principalmente el juez sentenciador tenga en su poder el analizar y valorar el contenido, entonces si ese contenido ha sido analizado respetando el debido proceso, incautación, cadena de custodia y el peritaje fue capaz de arrojar una		será el juez quien defina si se configura el delito y menciona que en el caso de la pornografía es posible determinar en el mismo momento de la extracción los elementos del tipo penal. Los informantes 3 y 5 responden en el mismo sentido al manifestar que si es posible con la pericia informática establecer el tipo penal. El informante clave 4 responde en el mismo sentido pero incluso llega a considerar que no solo los elementos del tipo penal se pueden establecer con la pericia sino que incluso el juez sentenciador con base al peritaje puede determine la existencia del delito. El informante 2 solo responde que se pueden estar comprobando los elementos subjetivos del tipo penal. De las respuestas obtenidas se puede concluir que hay una opinión o criterio dividido entre los informantes, pero la

		información positiva a los fines de la investigación, el juez puede determinar que con ese peritaje se ha logrado acreditar la existencia de un delito. R/(5).- Si, si porque la informática es difícil, sabe porque inclusive las grabaciones es imposible que alguien diga no fui yo, si es posible que diga yo estaba drogado cuando dije eso, ahí sí, porque esto (la grabación) no lo puede detectar, pero que no dijo lo que dijo es bien imposible, es prueba contundente. R/(6).- Es relativo porque se puede determinar que un usuario ha ingresado a un sistema, si lo vemos desde el tipo penal estafa y viene alguien y quiere que en cierto equipo se ha dado el delito de estafa en contra de una persona, lo que en realidad la sección hace es recolectar información como fotos correos o cualquier información que haya pasado por el equipo que compruebe que el usuario tal tuvo comunicación con otro usuario tal, para este		mayoría considera que a través de la pericia informática si es posible comprobar los elementos del tipo penal pero deben vincularse esta con otros medios de prueba, más tomando en cuenta que habrá casos donde no sea posible con la sola pericia comprobar los elementos del tipo penal.

9	¿Si el abogado defensor presente contraperitaje informático para desvirtuar los elementos del tipo penal?	caso específico el perito informático no puede decir que se cometió el delito de estafa, eso lo dirá el perito contable; para el caso de los amaños lo que va a determinar que se dio el delito puede ser alguna conversación que quedo registrada en algún aparato como una Tablet, pero será el juzgador quien defina si en esa conversación hablaba de que le daban cierta cantidad por fallar un gol y por ende será el juzgador quien defina si existió el delito, pero hay casos como el de Pornografía infantil donde nosotros al realizar el análisis a la maquina encontramos imágenes y videos pornográficos y al mismo tiempo estamos identificando el delito. R/(1).- Lo normal es que no lo hacemos, porque delitos informáticos pocos estamos viendo, pero cuando es necesario si lo hacemos.		En cuanto ¿si el abogado defensor presente contraperitaje informático para desvirtuar los elementos del tipo penal? El informante clave uno manifiesta que normalmente no se presenta, pero que hay casos donde sí. Los informantes clave, 3, 4 y 5 hacen mención que los abogados defensores pueden presentar una contraperitaje porque es su derecho como defensa técnica, pero a pesar que tienen la facultad para hacerlo, en la práctica

		R/(2).- Cómo?, si el cliente es el que menos tiene, también a que institución se debe ir para que le realice contraperitaje informático?, no hay ninguna institución donde pueda hacer contraperitaje informático, ese es uno de los grandes obstáculos que tiene la defensa, en ese aspecto considero que se pone bien difícil la situación R/(3).- Es su derecho, como parte técnica puede proponer perito, puede proponer la realización de una nueva pericia. R/(4).- Los abogados son pocos acuciosos e inteligentes, que tratan de desvirtuar la hipótesis fiscal contraproponiendo al juez otra versión de los hechos, pero si es una facultad del defensor proponer contra peritaje pero es poco. R/(5).- Puede ser. La defensa técnica puede		casi no se da. Ahora bien los informantes 2 y 6, en sus respuestas dejan claro que es un derecho de la defensa solicitar y practicar un contraperitaje, pero no obstante la ley los faculte es prácticamente imposible realizar un contraperitaje informático, porque no se trata de cualquier tipo de pericia sino que de una donde las herramientas, el software y el recurso humano no se encuentra en cualquier lugar, aparte que los especialistas que practican este tipo de pericias solo están disponibles en el Laboratorio Técnico Científico de la PNC., y no hay en el país otra institución que pueda practicar este tipo específico de peritajes, ni hay más especialistas que se dediquen a practicar estas pericias solo los ya mencionados del Laboratorio, sin dejar de lado que tampoco hay una institución u

		ofrecer prueba pericial para desvirtuar la prueba pericial que ha devenido de la investigación o del ente acusador. El defensor solicita al juez que juramente a un perito. Cuando esta judicializado el caso se le pide al juez directamente, y el juez ordena que se practique, con el perito nombrado y juramentado por el juez, que ha sido ofrecido por el defensor, Ahora bien, la mayoría de defensores por ejemplo aquí en Santa Ana no son muy acuciosos en eso, hemos tenido pocas contrapericias. R/(6).- No se da y del 100% de las vistas públicas a las que los peritos de la sección hemos asistido se ha dado un 10% se ha tenido un contraperitaje, y este no consiste en la entrega de la evidencia a una persona y esta realizara la práctica del análisis, sino que se coordina pidiendo un permiso y se asigna a un perito y la persona solicitante llega a la sección de delitos tecnológicos, la limitante		organismo que forme especialistas en la materia, y en todo caso si un abogado particular quisiera por otros medios practicar una pericia informática, es bien difícil que cuente con el capital necesario para comprar el equipo mínimo pues por lo dicho por el perito el de uso del Laboratorio está valorado en 40,000 dólares, aunado a ello se compra el software y aun si adquiriera estos dos, necesitaría un especialista forense y de dónde saca uno si en el país los únicos peritos informáticos son los del laboratorio, esto limita en gran medida para este tipo de delitos a la defensa porque tiene el derecho subjetivo pero no tiene forma alguna de ponerlo en práctica no hay forma de ejercitar este derecho.

		de un defensor o un perito de la defensa son los software y los equipos puesto que son sumamente caros por ejemplo el de uso de la institución su valor es de 40,000 dólares y pueda que la defensa no cuente con este equipo o pueda que no tenga el software y si lo tiene no está autorizado para usarlo, por lo general la defensa se limita a verificar los procedimientos realizados por la sección y si realiza el análisis con un software diferente obtendrá otros resultados mejores o más limitados, la sección utilizamos los lineamientos institucionales basados en los manuales de procedimientos aceptados por la comunidad forense y eso los lleva a obtener los resultados que se presentan, y por eso en la mayoría de casos la defensa llega a la sección observa los procedimientos y si tiene algo que refutar solo pregunta ¿porque se hizo tal cosa?, pero desde la formación de la sección en el año 2009 nunca se hemos tenido un contraperitaje, para que eso		
10	¿Si existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?			En cuanto a ¿si existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del

		sucediera tendríamos que renunciar alguno de la sección y dedicarnos a este tipo de peritajes. R/(1).- En algunos casos si, pues hay casos que por la misma situación que se da, porque hay un círculo vicioso que se da cuando se trata de justificar una prueba informática, esto nos lleva a decir que cada caso es distinto y se presenta de distinta manera. R/(2).- A veces claridad aquí es bien difícil, si al Juez a veces con que le cuesta manejar el teléfono táctil, entonces se dejara llevar por lo que dice el peritaje informático, y como la defensa esta corta, porque su cliente no tiene dinero, como va acceder contraperitaje, el juez se va ir con lo que le diga el perito de la Policía Técnica Científica, si ahí dice fulano fue y aquí está el número, el juez no sabe si el investigador o perito le dijeron, este número es y a saber si no es ese , ahí es donde se		imputado?, los informantes 1, 3, y 5 manifiestan que en cierto casos si existe claridad al momento de valorar la pericia informática, el informante 4 no deja claro si existe o no claridad en el juez, solo menciona que debe haber una individualización y una identificación para que el juez pueda valorar más allá de la existencia del delito y deducir así la responsabilidad penal, tomando en cuenta a que los resultados que arrojó el peritaje sobre la participación de una persona en el delito que se investiga. Sin embargo los informantes clave 2 y 6 establecen que es difícil ya que el juez no es conocedor de los medios tecnológicos, esto en razón a la falta de capacitación y al desinterés de parte del Juez, en consecuencia existe una mayor posibilidad que la valoración sea errónea, por lo que se puede concluir

		empieza a contaminar lo dicho desde que el agente policial captura al imputado, desde ahí viene la contaminación de todo y ahí es donde existen problemas para el defensor, el juez quien toma como claro la situación esa y así condenan a las personas y eso lo sufrimos todos los abogados defensores. R/(3).- Un juez que conoce en principio como se redacta una sentencia y sabe trasladar la evidencia a esa sentencia, claro que puede haber claridad al respecto. Entonces cuando uno lee una sentencia puede uno dictaminar si hizo una valoración completa y analítica del caso en específico y ahí es donde uno puede decir valoro bien esta prueba. R/(4).- El juez tiene que ser más acucioso para establecer la participación del procesado luego de ese peritaje, porque para que el juez pueda atribuir ese hecho al procesado tiene que haber una individualización y una		que no todos los jueces están capacitados para valorar la pericia informática, existen algunos jueces que se han preocupado por el tema tecnológico y se han interesado en la materia, se han propuesto conocer del tema y se han preparado para valorar la pericia informática cuando a su conocimiento sea sometido un proceso informático, hay que tomar en cuenta que la valoración proviene no solo de lo escrito en la pericia si no del contra interrogatorio que se le hace al perito en vista pública, por lo cual la valoración está sujeta a varios factores no solo a la presentación de la pericia.

		identificación cierta de que esa información, ese equipo, lo que arrojo ese peritaje; si es así puede valorar más allá de la existencia del delito las probabilidades de participación de una persona luego del peritaje. R/(5).- Si, la certeza es una valoración que tiene en su mente el juez sentenciador, el juez que celebre la vista pública, porque si no existe certeza existe probabilidad y con probabilidad no se le puede deducir responsabilidad a nadie, debe haber certeza. Y los jueces en cuestiones de experticia valoran perfectamente y acordémonos que las pericias son realizadas por personal "cualificado" y esa cualificación solo se puede extraer de lo que es la vista pública cuando es contra interrogado el perito, entonces debe de haber certeza y si no hay certeza obviamente se deja libre al imputado. R/(6).- A veces los jueces no tienen bien clara la parte tecnológica, pero existen otros		

		que se han comprometido bastante y tiene muy buen conocimiento y esto les ayuda a valorar, aunque según la postura del perito depende de la forma en la que fiscalía presenta la evidencia, por ejemplo el caso de feminicidio, el primer caso que se judicializo no fue tomado en cuenta como feminicidio por la forma en la que fiscalía lo presento, no presento la autopsia y para demostrar que había una mujer muerta había que presentarla, cosa que fue refutada por el juez, por otro lado en la pericia el perito puede obtener los mejores resultados pero si fiscalía no hace la presentación en tiempo y de la manera pertinente el juez no la va a valorar de la manera adecuada, si existe un buen número de jueces que hacen buenas valoraciones, por ejemplo en el área de videos ha habido condenas aun sin testigos o sea que han sido solo sobre la base de videos, en el caso de la informática el juez se auxilia de otra persona que le traduce de manera		
11	¿Si la defensa presenta contraperitaje informático se podría desvirtuar la participación del imputado en el hecho que se le atribuye?			En cuanto a la pregunta ¿Si la defensa presenta contraperitaje informático se podría desvirtuar la participación del imputado en el hecho que se le

		entendible la terminología para poder valorar la evidencia. R/(1).- Dependiendo de que se trate pero en un caso en concreto pueden haber variaciones, esto genera un problema de aplicación porque si tenemos un peritaje que la defensa prevé antes de la audiencia, que no logra establecer el hecho, entonces no tiene caso peticionar otro cuando se está viendo la debilidad que tiene la prueba para desacreditarla, es por eso que dependiendo del caso se solicita o no, pues puede darse el caso que la defensa considere que necesita una prueba que establezca otro resultado, hay que valorar si se solicita o no. R/(2).- Sí, porque si viene la defensa y presenta un buen contraperitaje informático y se contratara a unas personas de una empresa norteamericana que me venga a hacer un contraperitaje, y lo certifique con toda la		atribuye? El informante clave 1 expresa que eso depende de cada caso en concreto, se debe valorar si se solicita o no, los informantes claves 2 y 4 expresan que con el contraperitaje si se puede desvirtuar la participación del imputado, mientras que él infórmate clave 5 dijo que eventualmente podría ser que si o que no, y el informante clave 6 expreso que la informática solo identifica usuarios no personas , y que la defensa debe apoyarse en otras pruebas como videos o testigos para desvirtuar la participación del imputado, de las respuestas obtenidas se concluye que con el contraperitaje informático no es suficiente para desvirtuar la participación del imputado debido a que es necesario apoyarse de otros medios de pruebas.

		documentación legal en el trámite correcto y lo admite el juez y sigue todos los procedimientos perfectamente puede desvirtuar la participación del imputado. R/(3).- Es obvio de que la contraparte tiene derecho a presentar prueba de descargo, entonces va a depender del tipo de peritaje que es lo que se pretende probar, eventualmente podría ser que si o podría ser que no, o simplemente confirmar la primer pericia. R/(4).- Si puede porque la hipótesis fiscal es solo eso, esa está sujeta a que la corrobore frente al juez el mismo fiscal, pero si no ha sido capaz de poderla demostrar, obviamente con un peritaje el defensor puede demostrarle al juez que los hechos no ocurrieron en la forma como se plantearon, entonces si puede desvirtuarse mediante un peritaje la hipótesis del fiscal.		

12	¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?,	R/(5).-Si puede presentarla, y tiene derecho a presentarla, que no lo hagan de hecho es una cosa, pero eso es de hecho , pero si tienen el derecho de hacerlo, es un derecho que tiene el imputado de ofrecer prueba de descargo, aunque sea obligación de la fiscalía comprobar que el imputado es culpable, porque ya se le presume inocente, pero eso no quita o no resta las facultades del imputado y su defensor de ofrecer prueba pericial como para desvanecer los hechos que se le acusen al imputado. R/(6).- A través de la informática no se puede demostrar que la persona que ingresa a una maquina con un usuario y contraseña es la dueña del usuario, solo se puede decir que el usuario tal fue el que realizo una modificación en el sistema y por eso en la sección solo identificamos usuarios no personas, por ende la defensa más que todo se debe enfocar en demostrar que si bien es		En lo que se refiere a la pregunta, ¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?, los informantes claves 1, 3, 4, 5 y 6 manifiestan que no es posible

		cierto que el usuario de su cliente fue utilizado, no fue su defendido quien lo utilizo y para ello se debe apoyar en otras pruebas como por ejemplo videos o testigos que afirmen otros hechos contrarios a los que le acusan. R/(1).- No es suficiente, esto depende, pues partiendo de la fidelidad de la prueba posiblemente en algunos casos va a ser suficiente o posiblemente en otros no porque pueden variar algunas circunstancias. R/(2).- Habría que ver cómo viene el peritaje informático, todo es de análisis. Vengo y digo peritaje informático que presento el fiscal es suficiente para probar el hecho delictivo? si yo no pruebo absolutamente nada sobre el peritaje informático a lo mejor el Juez sentenciador pueda decir es suficiente y va tener como probados los hechos delictivos, podría ser, como le digo los elementos del tipo penal son los que hay que		que una sola prueba se dejen establecidos los elementos del tipo penal y el 6 agrega que es necesario acompañarse de otras pruebas, que en su conjunto generen la certeza en el juzgador, mientras que el informante 2 dice que esta dudoso de eso, tendría que ver en concreto, casos en los que la fiscalía pudo haber probado el hecho delictivo. De las respuestas se puede inferir que tanto procuradores, defensores particulares, fiscales, jueces de instrucción, jueces de sentencia y peritos tienen la convicción que una prueba no es suficiente para demostrar tanto el elemento objetivo como el elemento subjetivo del tipo penal mientras que los defensores particulares tienen duda si es posible o no probar el hecho delictivo solo con el peritaje informático.

		probar tanto objetivos como subjetivos, yo estaría dudoso en esa cuestión, tendríamos que ver en concreto ciertos casos para determinar si fiscalía pudo haber probado el hecho delictivo. R/(3).- Va depender del hecho que pretende probar, un delito puede tener diferentes elementos objetivos del tipo y cada uno está sujeto a prueba, entonces va depender para que se realizó ese peritaje, si es para probar uno de esos datos objetivos, pues habrá probado parcialmente el tipo penal y obviamente complementado con otros elementos de prueba, porque el tipo penal tiene elementos objetivos, subjetivos y normativos entonces es casi imposible que con una sola evidencia se prueben todos los elementos del tipo penal. R/(4).- Tenemos en el sistema libertad probatoria es decir que un hecho puede		

		probarse con diferentes medios de prueba, pero el juez cuando admite y valora una prueba lo hace en un marco legal respetando principios, uno de esos es la pertinencia de la prueba para poder demostrar existencia de un delito y participación de un procesado en un delito informático. R/(5).- No, necesita de otros elementos periféricos o indirectos no solo de una prueba sino de otros medios probatorios, en este delito especialmente se prueba con la pericia. R/(6).- No pues es necesario acompañarse de otras pruebas que valoradas en su conjunto llevan a generar la certeza en el juez para resolver el juicio.		

Fuente: Elaboración Propia.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones.

La creación de la Ley Especial Contra los Delitos Informáticos y Conexos el 26 de febrero de 2016, implicó un desafío nuevo para jueces, fiscales y defensores por ser estas las partes procesales que desarrollan los procesos penales, asimismo involucró la necesidad de actualizarse en el dominio de las TICs y conocer sobre estas temáticas, ya sea a través de cursos y capacitaciones, ahora bien durante el desarrollo de la investigación se ha sostenido que la pericia informática es la llave sobre la cual versan los procesos penales de naturaleza informática, por ser esta la que tiene como objetivo ilustrar al juez sobre lo que sucede cuando se comete un delito informático, durante el periodo de entrevistas y con los resultados obtenidos de las respuestas de los sujetos de investigación como grupo investigador se realizaron las siguientes conclusiones:

1. El conocimiento sobre pericia informática únicamente lo poseen los peritos informáticos del Laboratorio Técnico Científico de la Policía Nacional Civil, ellos han sido capacitados por instituciones internacionales como la ONU, ABAROLI, e INTERPOL. En consecuencia las pericias son realizadas por especialistas con conocimientos forenses.

2. Las capacitaciones sobre actualización de las nuevas Tecnologías de Información y comunicación desde el año 2009 hasta la fecha han sido impartidas únicamente para peritos del Laboratorio Técnico Científico de la Policía Nacional Civil. Como grupo investigador diagnosticamos que efectivamente las pericias son practicadas por un profesional con conocimientos en las nuevas TICs.

3. La Fiscalía General de la República para acreditar la tipicidad de un delito informático, tendrá que utilizar otros medios de prueba aparte del peritaje informático, debido a que este último únicamente establece el usuario que ha cometido el delito, mas no la persona, por lo que esta prueba per se, no logra comprobar los elementos objetivos y subjetivos del tipo penal, y tendrá que utilizar otros medios de prueba como videos, o testigos.

4. Se determinó que los recursos tecnológicos idóneos para realizar un peritaje existen, pero no son suficientes. Las TICs, están en constante evolución, y el hecho de no tener los recursos necesarios es uno de los problemas probatorios de los delitos informáticos.

5. Jueces, fiscales, y abogados desconocen el procedimiento para realizar un peritaje informático, no reciben capacitaciones sobre tecnologías de la información, pericia informática y peritaje informático.

6. No existe un protocolo especial para la extracción transporte y presentación de la pericia informática. La Ley Especial Contra Los delitos Informáticos y Conexos tampoco lo regula.

7. La defensa tiene el derecho de solicitar y presentar contraperitaje, no obstante es algo que en la práctica no se da y en caso que el abogado defensor solicite un contraperitaje no se cuentan con las herramientas, ni el equipo necesario para practicarlo, tampoco existen más peritos informáticos a parte de los del Laboratorio Técnico Científico de la PNC, por lo tanto no hay ninguna otra institución que pueda practicar peritajes aunque un abogado defensor lo solicite.

8. Jueces, fiscales y defensores públicos han recibido capacitaciones sobre delitos informáticos por parte del Consejo Nacional de la Judicatura y UTE, contrario al defensor privado que no recibe ninguna.

9. De las respuestas recabadas se diagnosticó que los Jueces tanto de instrucción y sentencia consideran que la verdad material principalmente se acredita con la pericia informática, pero no es suficiente, para acreditarse debe vincularse con otros medios de prueba.

10. La evidencia digital puede ser alterada o falseada desde el momento de la incautación, o en el traslado de la información, la principal característica de esta es la fragilidad que posee y debido al desconocimiento de jueces, fiscales y abogados, la falta de recursos necesarios y un protocolo que garantice su credibilidad y certeza, será casi imposible para los sujetos determinantes del proceso percatarse y /o probar, que la evidencia ha sido alterada.

5.2 Recomendaciones

1. Crear una institución especializada a nivel de informática forense, con el fin de capacitar continuamente a todos los sujetos procesales determinantes los cuales son jueces, magistrados, fiscales, peritos del Laboratorio Técnico Científico y abogados públicos y privados.

2. Equipar con las suficientes herramientas tecnológicas al Laboratorio Técnico Científico de la policía Nacional Civil, y a la unidad especializada de investigación de delitos informáticos de la Fiscalía General de la Republica.

3. Crear un protocolo para el tratamiento de estos delitos informáticos, de manera que genere credibilidad y certeza en la extracción, transporte y cadena de custodia, y que llegue hasta la presentación de la evidencia. El objetivo de esto es reducir las posibilidades de falsear la evidencia digital y conservar su integridad.

4. Que el Estado a través de la instancia que corresponda implemente una medida para la creación de un organismo que otorgue certificaciones de informática forense, para que los profesionales en esta área puedan acreditarse como expertos autorizados, de esta manera se contaría con el recurso humano necesario e idóneo.

5. Crear una institución especialista y a la vanguardia con la información y herramientas tecnológicas para realizar contraperitajes, y orientar al público en general cuando necesiten una opinión o asesoría sobre el tema.

6. Hacer del conocimiento público los profesionales que estén certificados en informática forense, para que tanto defensores públicos y privados y la sociedad en su conjunto sepan a quienes pueden acudir cuando necesiten los servicios de un experto.

7. Aperturar en el Consejo Nacional de la Judicatura espacios para instruir e informar a los defensores públicos y privados sobre los Delitos Informáticos, que el CNJ trabaje en coordinación con la Unidad Técnica Ejecutiva del Sector Justicia (UTE), con el objetivo de brindar cursos y capacitaciones al público, no limitarlo solo a jueces, magistrados y fiscales.

8. Abordar y culturizar a la comunidad Universitaria sobre Delitos informáticos, e informática forense ya que esta es la herramienta con la cual se investigan estos delitos.

9. Brindar charlas informativas y definidas como políticas públicas sobre la Ley Especial Contra los Delitos Informáticos y Conexos, a toda la sociedad en general, de manera que los ciudadanos conozcan a que instituciones acudir si son víctimas de estos delitos y también que se manifiesten los conocimientos y medidas de ciberseguridad necesarias para prevenirlos.

10. Preparar a la corporación Policial en el ámbito de la informática forense, por ser quienes intervienen en primera instancia en conjunto con la Fiscalía General de la Republica en la investigación del delito, ya que son los sujetos que tienen un primer contacto con la evidencia y tratamiento de la misma.

Bibliografía

Grupo Arga Detectives Privados. (21 de Febrero de 2018). *El Papel del Perito Informatico Forense*. Obtenido de El Papel del Perito Informatico Forense: https://argadetectives.com/blog/el-papel-del-perito-informatico-forense-que-es-la-informatica-forense-historia-y-evolucion.html

ABEL LLUCH, X. (2012). *Derecho Probatorio.* Barcelona,: J. M. Bosch.

Aguilar, M. (09 de 08 de 2015). *La informática forense dentro de la investigación pericial.* Obtenido de Metodologñia de la investigación en informática forense: http://informaticaycriminalistica.blogspot.com/2015/08/investigacion-pericial-en-informatica.html

Ampuero, I. H. (2016). Reglas de Prueba Legal y Libre Valoracion de la Prueba. *Revista IUS et Praxis, año 23, n° 1*, 26.

Anónimo. (01 de 09 de 2014). *Medicina Legal, Autopsia, Necropcia*. Obtenido de Blogspot: https://karinalistica.blogspot.com/2014/09/medicina-legal-autopsia-necropsia.html

Areitio, G., & Areitio, A. (2009). *Informacion, informatica e internet: del ordenador personal a la empresa 2.0.* España: Vision Libros.

Arellano , L. (3 de Enero de 2012). La Cadena de Custodia Informatica Forence. *ACTIVA, ISSN (3)*, 67-81. Medellin, Colombia. Obtenido de file:///C:/Users/Conchy%20Pint%C3%ADn/Downloads/45-Texto%20del%20art%C3%ADculo-85-1-10-20140521.pdf

Aroche, S. (14 de Febrero de 2006). *Maestro de Web by platzi (historia del internet)*. Obtenido de Maestro de Web by platzi (historia del internet): http://www.maestrosdelweb.com/internethis/

Asamblea Legislativa de la República de El Salvador. (1983). Código Procesal Penal. En A. L. Salvador, *Código Procesal Penal* (pág. 253). El Salvador: Lis.

Asamblea Legislativa de la República de El Salvador. (04 de 02 de 2016). Diario Oficial. *Ley Especial Contra los Delitos Informáticos y Conexos*. San Salvador, El Salvador: Diario Oficial.

Balsera, J. A. (2014). *Tratado Pericial Judicial.* Barcelona, España.: La Ley.

Barceló, M. (2008). *Una historia de la informática.* Barcelona: UOC.

Baytelman , A. (2008). *Litigacion Penal, Juicio Oral y Prueba.* Mexico: Inacipe.

Bogdan, T. (1992). *Introduccion a los Metodos Cualitativos en Investigacion* . España: Paidos.

Buriticá, G. (2003). *Como Obtener y Presentar Evidencia Digital.* Colombia: procedu.

Caballena de Torres, G. (1993). *Diccionario Jurídico Elemental.* Madrid: Heliasta S.R.I.

Caballenas, G. (1989). *Diccionario de Derecho Usual* (2° edición ed.). Buenos Aires-Republica Argentina, Colombia, Colombia: l Heliasta S.R.

Cafferrata, N. (1998). *La prueba en el proceso penal.* Buenos Aires: DEPALMA.

Carvajal, L. (01 de 06 de 2013). *Lizardo Carvajal*. Obtenido de Sujeto de Investigación: https://www.lizardo-carvajal.com/sujeto-de-investigacion/

Casado Pérez, J. M. (2000). *La Prueba en el Proceso Penal Salvadoreño.* San Salvador: LIS.

Centty, D. B. (12 de 06 de 2010). *Biblioteca virtual de derecho, economía y ciencias sociales*. Obtenido de Manual Metodológico para el investigador científico: http://www.eumed.net/libros-gratis/2010e/816/UNIDADES%20DE%20ANALISIS.htm

Clérigues, J. N. (2015-2016). Guía actualizada para futuros peritos informáticos Ultimas herramientas de análisis Forense digital. *Pensamiento Penal* , pág. 31.

Código Procesal Penal. (04 de 12 de 1996). Diario Oficial. San Salvador, El Salvador: LIS.

Comisión Económica para America Latina y el Caribe. (2016). *Estado de la banda ancha en América Latina y el Caribe 2016.* Santiago: Naciones Unias.

Constitución. (16 de Diciembre de 1983). Diario Oficial. *DECRETO N1 38*.-. San Salvador, El Salvador: Lis.

Constitución de la República de El Salvador. (12 de Junio de 2014). DIario Oficial. (L. V. Lopez, Ed.) San Salvador, El Salvador: Asamble Legislativa de El Salvador.

Convencion Americana Sobre Derechos Humanos. (22 de Noviembre de 1969). Convención Americana Sobre Derechos Humanos. *Convención Americana Sobre Derechos Humanos*. San José, San José, Costa Rica: desconocido.

Convenio Sobre la Ciberdelincuencia. (23 de Noviembre de 2001). *Convenio Sobre la Ciberdelincuencia.* Obtenido de Convenio Sobre la Ciberdelincuencia: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Couture J, E. (2010). *Fundamentos del Derecho Procesal Civil.* Buenos Aires: B de F de Ltda.

Dirección General de Apoyo a la Investigación Penal . (25 de 08 de 2013). *Ministerio Público*. Obtenido de Críminalistica de la República Bolivariana de Venezuela : http://criminalistica.mp.gob.ve/balistica-forense/

Echandía, D. (1981). *Compendio de Pruebas Judiciales.* Bogotá: Temis.

Echandía, D. (1994). *Teoria General de la Pueba* . Buenos Aires: Victor P.

Eduardo J. Piro. (2016). *Informática Forense Pericias Informáticas.* Obtenido de Informática Forense Pericias Informáticas: https://es.scribd.com/document/298023333/Pericias-Informaticas

Escobar, C. D. (24 de octubre de 2017). *Historia del Internet en El Salvador*. Obtenido de Medium: https://medium.com/@carl.d/historia-del-internet-en-el-salvador-53fc94ba508c

Explorable. (26 de 02 de 2019). *Muestreo por coveniencia*. Obtenido de Explorable: https://explorable.com/es/muestreo-por-conveniencia

Franco, P. (20 de 03 de 2013). *Tipos de estudio según Sampieri*. Obtenido de Blogspot: http://paulafrancocpf.blogspot.com/2013/03/tipos-de-estudios-segun-sampieri.html

Fundación Salvadoreña para el Desarrollo Económico y Social FUSADES. (2016). *Una ley contra los delitos informáticos que respete la libertad de expresión.* San Salvador: Estudios Legales.

Garcia Gomez, J. L. (2015). Informe sobre el Peritaje Informático. *Informe sobre el Peritaje Informático*. Madrid, España.

Garciandía, P. (2008). *La Peritacion Como Medio de Prueba.* Panplona: Arazandi.

Gissel, R. (2005). *Digital Underworld.* United Estates: Macrotech press.

Guardiola, M. (07 de 09 de 2017). *Law & trends*. Obtenido de Cómo evitar que se impugne la prueba digital: https://www.lawandtrends.com/noticias/tic/como-evitar-que-nos-impugnen-la-prueba-digital-1

Guias Juridicas. (06 de 03 de 2019). *Guias Juridicas*. Obtenido de Administracion de Justicia: http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAUNDE0tjtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAcT-CIjUAAAA=WKE

Hernández Sampieri, R., Collado, C. F., & Baptista Lucio, P. (2014). *Metodología de la Investigación.* México: McGRAW-HILL / INTERAMERICANA.

Herrera Mejía, S. E. (Marzo de 2012). LA EFICACIA DEL HABEAS DATA EN LA LEGISLACION SALVADOREÑA. San Salvador, El Salvador.

I Casadevall, I. T., & Vilaseca i Requena, J. (2005). *Sociedad del conocimiento.* Barcelona: UOC.

Ibarra, R. (27 de Abril de 2002). *Historia del internet en El Salvador.* Obtenido de https://nsrc.org/regions/CENTRAM/SV/Internet-SV-04-2002.PDF

Informático Forense Madrid. (03 de 05 de 2018). *¿Qué es el peritaje informático y comó llegar a ser perito?* . Obtenido de Informático Forense Madrid: https://informatico-forense-madrid.es/peritaje-informatico-ser-perito

Jerez, J. L. (2015). *Investigación Informática Forense basada en Emacs.* Madrid, España: Creative Commons.

Jinde, T. (12 de 01 de 2012). *Blogspot*. Obtenido de Dactiloscopía: http://dactiloscopiapenal.blogspot.com/p/concepto-de-dactiloscopia.html

Jojoa, D. (28 de 11 de 2014). *Fases de la Informática forense*. Obtenido de Blogspot: ttp://notasinformaticaforense.blogspot.com/2014/11/fases-de-la-informatica-forense.html

La prensa Grafica. (11 de Abril de 2018). *La prensa Grafica*. Obtenido de La prensa Grafica: https://www.laprensagrafica.com/elsalvador/FGR-tribunal-no-valoro-106-pruebas-en-caso-troll-center-20180410-0124.html

La Prensa Grafica. (7 de Noviembre de 2018). Perito mintio sobre dificultades para sacar informacion de computadora del exfiscal Martinez. *La Prensa Grafica*.

Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense InFo-Lab, Ministerio Público Fiscal Provincia de Buenos Aires. Universidad FASTA. (desconocido de Abril de 2016). *GUÍA INTEGRAL DE EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL.* Buenos Aires: Mar de Plata. Recuperado el 23 de Enero de 2019, de GUÍA INTEGRAL DE EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL: http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf?sequence=1

LEGISLATIVO, O. (2008). *CODIGO PROCESAL PENAL.* San Salvador: Diario Oficial.

Ley Especial Contra los Delitos Informáticos y Conexos. (02 de 2016). Diario Oficial. San Salvador, El Salvador: Diario Oficial.

Ley Especial para la Intervención de las Telecomunicaciones. (12 de Marzo de 2010). Diario Oficial. *DECRETO Nº 285*. San Salvador, El Salvador: Lis.

LLUCH, X. A. (2014). *Tratado Pericial Judicial.* Madrid.: La Ley.

Llunch, X. A. (2014). Distinción entre intepretar y valorar. En X. A. Llunch, *Valoración de los medios de prueba el el proceso civil* (pág. 22). Barcelona: La ley.

Luján, J. (14 de 09 de 2010). *La Críminalistica y Otras Ciencias*. Obtenido de Odontología Forense: http://www.mailxmail.com/curso-criminalistica-ciencias-forenses/odontologia-forense

Martín- Crespo, M., & Salamanca , A. (2007). El muestreo en la investigación cualitativa. *nure investigación*, 4.

Medrano, C. (23 de Febrero de 2017). *Universidad Luterana Salvadoreña*. Obtenido de Universidad Luterana Salvadoreña: https://www.uls.edu.sv/sitioweb/component/k2/item/551-a-un-ano-de-la-aprobacion-de-la-ley-de-delitos-informaticos-en-el-salvador-retos-y-desafios

Mixan, F. (2003). *Categoría y Actividad probatoria.* Peru: Hammurabi.

Molina, V. (2008). La validez de la prueba judicial. En L. B. Ruíz Jaramillo, *Valoración de la validez y de la eficacia de la prueba* (pág. 168). medellín: Estudio de Derecho.

Moraga, A. L. (1995). Historia e Internet: aproximación al futuro de la labor investigadora. En L. A. BARATAS DÍAZ, *"Internet: un recurso imprescindible para historiadores de la ciencia y la tecnología"* (págs. 667-675). Madrid, España: Lull: Revista de la Sociedad española de las Ciencias y de las Tecnicas.

Morales, M. A. (01 de 10 de 2013). *Universidad Rafael Landívar Facultad de Ciencias Jurídicas y Sociales.* Obtenido de Docplayer: https://docplayer.es/18741029-Universidad-rafael-landivar-facultad-de-ciencias-juridicas-y-sociales-licenciatura-en-investigacion-criminal-y-forense-fds.html

Octavio, I. (2011). Los primeros años de internet en america latina. *Razon y Palabra*, 9.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNDOC). (s.f. de s.f. de 2018). *Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos.* Obtenido de

Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos: http://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-de-los-capitulos-I-II-III-V.pdf

Ortiz Rodríguez, A. (1982). *Tratado de Derecho Procesal Penal.* Buenos Aires: Astrea.

Pacto Internacional de Derechos Civiles y Politicos. (23 de marzo de 1976). Pacto Internacional de Derechos Civiles y Politicos. *Pacto Internacional de Derechos Civiles y Politicos*. desconocida, desconocida, Naciones Unidas: desconocida.

Picón, E. (11 de febrero de 2019). *Peritos Ingenieros informáticos*. Obtenido de peritoinformatico.es: www.peritoinformatico.es

Proyecto de Justicia. (24 de 03 de 2016). *La cadena de custodia*. Obtenido de Proyecto de justicia: http://proyectojusticia.org/la-cadena-de-custodia/

Puente, D. (30 de 08 de 2014). *El Peritaje Psiquiátrico*. Obtenido de Psiquiatría Integral: http://psiquiatriaintegral.com.mx/principal/?p=678

Puig Faura, S. (2015). *La Prueba Pericial Informática en el Procedimiento Civil.* Madrid, España: La Ley.

Reith, M., Carr, C., & Gunsch, G. (2002). *Examinación de la evidencia Digital Internacional.* Madrid: Junin.

Res. UAIP-2436-RR-884-2017(2), 2436-2017 (Unidad de Acceso a la Información Pública del Órgano judicial 19 de Julio de 2017).

Roque, C. I. (2016). La toxicología Forense. *Revista de Ciencias Forenses de Honduras*, 5.

Sain, G. (2018). La Estrategia Gubernamental Frente al Cibercrimen: la importancia de las politicas preventivas mas alla de la solucion penal. En R. Parada, J. Errecaborde, & (coords), *Cibercrimen y delitos informáticos suplemento especial.* (págs. 7-32). Argentina: BluePress S.A.

Sandoval, R. I. (2018). *Codigo Procesal Penal (comentado).* San Salvador: Liz.

Scotti, L. (2016). El impacto de internet en el mundo juridico: una mirada desde el derecho internacional privado. *Foro Juridico*, 191.

Sendra, G. (1981). *Fundamentos del Derecho Procesal.* Madrid: S.L. CIVITAS EDICIONES.

Signaturit. (07 de 09 de 2007). *La prueba electrónica y su valoración por un juez o tribunal*. Obtenido de Signaturit: https://blog.signaturit.com/es/la-prueba-electronica-y-su-valoracion-por-un-juez-o-tribunal

Superintendencia General de Electricidad y Telecomunicaciones. (s.f de s.f de 2014). *Las telecomunicaciones en EL Salvador*. Obtenido de Superintendencia General de Electricidad y Telecomunicaciones: https://www.siget.gob.sv/temas/telecomunicaciones/resena-historica/las-telecomunicaciones-en-el-salvador/

Tesis de Investigadores. (01 de 09 de 2012). *Tesis de Investigación*. Obtenido de Blogspot: http://tesisdeinvestig.blogspot.com/2012/01/poblacion-y-muestra.html

Tünnermann, C. (2003). *La universidad latinoamericana ante los retos del siglo XXI.* Mexico: desconocido.

Union Interamericana de Telecomunicaciones (ITU). (2015). *Global Security Index & cyberwellness profiles.* Desconocida: ITU.

Vargas, I. (2012). *La Entrevista en la Investigación Cualitativa.* Heredia: Carc.

Vazquez, C., Regalado, J., & Guadron, S. (Diciembre de 2017). Cibercrimen e informática forense: introducción y análisis en El Salvador. *Escuela Especializada en Ingenería ITCA-FEPADE(10)*, 63-68. El Salvador. Obtenido de http://www.redicces.org.sv/jspui/bitstream/10972/3029/1/Articulo11.pdf

Vélez, A. (2001). *Derecho Procesal Penal.* Cordoba: Lener.

ANEXOS.

CUADRO NÚMERO 1: MATRIZ DE ENTREVISTAS.

Categoría	Indicador	Unidad de Análisis	Ítems
Pericia Informática. **Problemas Probatorios.** **La administración de justicia penal en los delitos informáticos.**	Conocimiento de pericia informática. Experiencia en peritaje y contra peritaje informático. Herramientas tecnológicas. Materia probatoria pericial en delitos informáticos. Embalaje y cadena de custodia de la pericia informática. Prueba Pericial del Delito Informático. Prueba Pericial de Participación en el Delito Informático.	Juez de Sentencia I Juez de Instrucción II Fiscal III Defensor Público IV Defensor Particular V Perito PNC VI	¿Qué estudios posee sobre pericia informática? ¿Qué capacitaciones recibe sobre actualización en tecnologías de la información? ¿Cuál es el procedimiento para realizar un peritaje o contraperitaje informático? ¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje informático? ¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió? ¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática? ¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático? ¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal? ¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal? ¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado? ¿Si la defensa presenta contraperitaje informático se podría desvirtuar la participación del imputado en el hecho que se le atribuye? ¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?

Fuente: Elaboración Propia

Anexo 1: Instrumento de investigación: Entrevista Semiestructurada.

"Universidad de El Salvador

Facultad Multidisciplinaria de Occidente"

Entrevista dirigida a Juez de Instrucción y Sentencia.

TEMA: "PROBLEMAS PROBATORIOS DE LA PERICIA INFORMÁTICA EN EL DERECHO PENAL SALVADOREÑO"

OBJETIVO: Obtener información real sobre los problemas que se pueden presentar en la pericia informática dentro del proceso penal salvadoreño, analizando si dichos problemas afectan o inciden en la administración de justicia.

GENERALIDADES:

Nombre: _____ Sexo: M ☐ F ☐

Edad: _____

Lugar: _____

Profesión: _____

Ítems a responder.

1) ¿Qué estudios posee sobre pericia informática?
2) ¿Qué capacitaciones recibe sobre actualización en tecnologías de la información?
3) ¿Cuál es el procedimiento para realizar un peritaje o contraperitaje informático?
4) ¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje informático?
5) ¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?
6) ¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?
7) ¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?
8) ¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?
9) ¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?
10) ¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?
11) ¿Si la defensa presenta contraperitaje informático se podría desvirtuar la participación del imputado en el hecho que se le atribuye?
12) ¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?

Anexo 2: Instrumento de investigación: Entrevista Semiestructurada.

"Universidad de El Salvador

Facultad Multidisciplinaria de Occidente"

Entrevista dirigida a Defensores Públicos y Particulares.

TEMA: "PROBLEMAS PROBATORIOS DE LA PERICIA INFORMÁTICA EN EL DERECHO PENAL SALVADOREÑO"

OBJETIVO: Obtener información real sobre los problemas que se pueden presentar en la pericia informática dentro del proceso penal salvadoreño, analizando si dichos problemas afectan o inciden en la administración de justicia.

GENERALIDADES:

Nombre: _____ Sexo: M ☐ F ☐

Edad: _____

Lugar: _____

Profesión: _____

Ítems a responder.

1) ¿Qué estudios posee sobre pericia informática?
2) ¿Qué capacitaciones recibe sobre actualización en tecnologías de la información?
3) ¿Cuál es el procedimiento para realizar un peritaje o contraperitaje informático?
4) ¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje informático?
5) ¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?
6) ¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?
7) ¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?
8) ¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?
9) ¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?
10) ¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?
11) ¿Si la defensa presenta contraperitaje informático se podría desvirtuar la participación del imputado en el hecho que se le atribuye?
12) ¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?

Anexo 3: Instrumento de investigación: Entrevista Semiestructurada.

"Universidad de El Salvador

Facultad Multidisciplinaria de Occidente"

Entrevista dirigida a Fiscalía General de la República.

TEMA: "PROBLEMAS PROBATORIOS DE LA PERICIA INFORMÁTICA EN EL DERECHO PENAL SALVADOREÑO"

OBJETIVO: Obtener información real sobre los problemas que se pueden presentar en la pericia informática dentro del proceso penal salvadoreño, analizando si dichos problemas afectan o inciden en la administración de justicia.

GENERALIDADES:

Nombre: _____ **Sexo: M** ☐ **F** ☐

Edad: _____

Lugar: _____

Profesión: _____

Ítems a responder.

1) ¿Qué estudios posee sobre pericia informática?
2) ¿Qué capacitaciones recibe sobre actualización en tecnologías de la información?
3) ¿Cuál es el procedimiento para realizar un peritaje o contraperitaje informático?
4) ¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje informático?
5) ¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?
6) ¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?
7) ¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?
8) ¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?
9) ¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?
10) ¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?
11) ¿Si la defensa presenta contraperitaje informático se podría desvirtuar la participación del imputado en el hecho que se le atribuye?
12) ¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?

Anexo 4: Instrumento de investigación: Entrevista Semiestructurada.

"Universidad de El Salvador

Facultad Multidisciplinaria de Occidente"

Entrevista dirigida a Perito informático del Laboratorio Técnico Científico de la Policía Nacional Civil.

TEMA: "PROBLEMAS PROBATORIOS DE LA PERICIA INFORMÁTICA EN EL DERECHO PENAL SALVADOREÑO"

OBJETIVO: Obtener información real sobre los problemas que se pueden presentar en la pericia informática dentro del proceso penal salvadoreño, analizando si dichos problemas afectan o inciden en la administración de justicia.

GENERALIDADES:

Nombre: _____ Sexo: M ☐ F ☐

Edad: _____

Lugar: _____

Profesión: _____

Ítems a responder.

1) ¿Qué estudios posee sobre pericia informática?
2) ¿Qué capacitaciones recibe sobre actualización en tecnologías de la información?
3) ¿Cuál es el procedimiento para realizar un peritaje o contraperitaje informático?
4) ¿Existen los recursos tecnológicos idóneos para elaborar un peritaje o contraperitaje informático?
5) ¿Las herramientas de software permiten dictar en el peritaje informático o contraperitaje lo que realmente sucedió?
6) ¿Cuál es el protocolo que se sigue en El Salvador para la extracción, transporte y presentación de la pericia informática?
7) ¿Qué probabilidades existen de falsear la información obtenida en un peritaje o contraperitaje informático?
8) ¿Al momento de valorar la pericia informática es posible comprobar los elementos del tipo penal?
9) ¿El abogado defensor presenta contraperitaje informático para desvirtuar los elementos del tipo penal?
10) ¿Existe claridad en el juez al valorar la pericia informática sobre la certeza de participación del imputado?
11) ¿Si la defensa presenta contraperitaje informático se podría desvirtuar la participación del imputado en el hecho que se le atribuye?
12) ¿Si el fiscal presenta peritaje informático es suficiente para probar el hecho delictivo?