



**Tratamiento de la prueba digital ofrecida por las partes
en el Proceso Penal del Ministerio Público de Ventanilla,
Callao -2017**

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

Maestro en Derecho Penal y Procesal Penal

AUTOR:

Br. Edgardo Simón Zarzosa Cadillo

ASESOR:

Dr. Edwin Alberto Martínez López

SECCIÓN:

Derecho

LÍNEA DE INVESTIGACIÓN:

Maestro en Derecho Penal y Procesal Penal

PERÚ – 2018

DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL / LA BACHILLER (ES): **ZARZOSA CADILLO, EDGARDO SIMON**

Para obtener el Grado Académico de *Maestro en Derecho Penal y Procesal Penal*, ha sustentado la tesis titulada:


TRATAMIENTO DE LA PRUEBA DIGITAL OFRECIDA POR LAS PARTES EN EL PROCESO PENAL DEL MINISTERIO PÚBLICO DE VENTANILLA, CALLAO -2017

Fecha: 14 de agosto de 2018

Hora: 7:15 p.m.

JURADOS:

PRESIDENTE: Dr. Mitchell Alarcón Diaz

Firma: 

SECRETARIO: Dra. Yda Rosa Cabrera Cueto

Firma: 

VOCAL: Dr. Edwin Alberto Martinez Lopez

Firma: 

El Jurado evaluador emitió el dictamen de:

Aprobar por unanimidad

Habiendo encontrado las siguientes observaciones en la defensa de la tesis:

.....
.....
.....
.....

Recomendaciones sobre el documento de la tesis:

- Estilo APA (citas y referencias)

.....
Nota: El tesista tiene un plazo máximo de seis meses, contabilizados desde el día siguiente a la sustentación, para presentar la tesis habiendo incorporado las recomendaciones formuladas por el jurado evaluador.

Página del Jurado

Dr. Mitchell Alarcón Díaz
Presidente

Dra. Cabrera Cueto Yda Rosa
Secretario

Dr. Edwin Alberto Martínez López
Vocal

Dedicatoria

El presente trabajo lo dedico a mis queridos padres especialmente a mi Madre Nona Rosa Cadillo Sánchez. A mi Hermano Rubén Zarzosa Cadillo, quien fue mi inspiración para el logro de mi objetivo.

Agradecimiento

Agradezco a la Universidad Privada Cesar Vallejo de Lima Norte por haberme brindado la oportunidad de continuar mis estudios de posgrado. A mi asesor de tesis Dr. Edwin Alberto Martínez López, quien con la paciencia y experiencia que lo caracteriza ha permitido pueda concluir este trabajo de investigación.

Declaración de Autoría

Yo, Edgardo Simón Zarzosa Cadillo, estudiante de la Escuela de Posgrado, Maestría en Derecho Penal y Procesal Penal, de la prestigiosa Universidad César Vallejo de la Sede Lima Norte; declaro, el trabajo académico que presentado es “Tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017” conformada por 188 folios, cuya finalidad es la obtención del grado académico de Maestro en Maestría en Derecho Penal y Procesal Penal, el mismo que corresponde a mi autoría.

Por consiguiente, declaro lo siguiente:

He consignado las fuentes del autor que corresponde en el presente trabajo de investigación, identificando la cita textual y de paráfrasis correspondiente a las fuentes de origen o cita de citas, de acuerdo a la normatividad y protocolo del sistema APA.

No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinen el procedimiento disciplinario.

Lima, 18 de agosto del 2018

Edgardo Simón Zarzosa Cadillo
DNI. N°32033544

Presentación

Señores miembros del jurado calificador

Tengo el honor de presentarles a ustedes mi tesis titulada “Tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao 2017”, cuyo objetivo fue: Describir el tratamiento legal de la prueba de digital en el Ministerio Publico de Ventanilla, Callao - 2017, en cumplimiento del Reglamento de grados y Títulos de la Universidad César Vallejo, para obtener el Grado Académico de Maestro.

En el presente trabajo, se investigó el tratamiento legal y los procedimientos adecuados que debe tener la prueba digital para su valoración en el proceso judicial. Del mismo modo el trabajo está estructurado por los siguientes capítulos: el capítulo I contiene la introducción; el capítulo II contiene al Marco metodológico; el capítulo III contiene los Resultados; el capítulo IV contiene Discusiones; el capítulo V contiene conclusiones. Por último, el capítulo VI menciona las referencias bibliográficas y los anexos respectivos.

Los resultados obtenidos en la presente investigación son “la prueba digital no tiene un tratamiento especial en el Nuevo Código Procesal Penal, dado que el tratamiento se lleva a cabo bajo la observancia del Artículo 185º del Código Procesal Penal como prueba documental”.

Respetable miembros del jurado calificador esperamos que este trabajo investigación sea evaluada y merezca un criterio de aprobación.

Los Olivos, 18 de agosto de 2018

Edgardo Simón Zarzosa Cadillo
DNI. N°32033544

Índice	Página
Página del Jurado	ii
Dedicatoria	iv
Agradecimiento	v
Presentación	vii
Índice	vii
Resumen	xi
Abstract	ixii
I. Introducción	13
1.1 Trabajos Previos	14
1.2 Marco Teórico Referencial de la Prueba Digital	19
1.3 Marco Espacial	79
1.4 Marco Temporal	79
1.5 Contextualización: Histórica, Política, Cultural, Social.	79
1.6 Supuestos teóricos	81
II. Problema de Investigación	82
2.1. Aproximación temática	83
2.2. Formulación del Problema de Investigación	83
2.3. Planteamiento del Problema	84
2.4. Justificación	85
2.5. Relevancia	87
2.6. Contribución	88
2.7. Objetivos	88
2.7.1. Objetivos específicos	89
III. Marco Metodológico	90
3.1. Categorías y categorización	91
3.2. Metodología	96

3.2.1. Respuestas de los estamentos, triangulación de datos, y conclusiones por cada pregunta:	96
3.3. Metodología	103
3.4. Escenario de estudio	103
3.5. Caracterización de sujetos	104
3.6. Procedimientos Metodológicos de Investigación	106
3.7. Técnicas e Instrumentos de Recolección de Datos	107
3.8. Mapeamiento	109
3.9. Rigor Científico	109
IV. Resultados	111
V. Discusión	128
VI. Conclusiones	139
VII. Recomendaciones	143
VIII. Propuesta	147
IX. Referencias	149
X. Anexos	155
Anexos 2. Gráfico de acceso de información a la red	158
Anexos 3. Gráfico de acceso de los hogares a las Tecnologías de la información y comunicación	159
Anexos 4. FODA del Ministerio Publico	160
Anexos 5. Delitos más comunes cometidos por la Red-Internet publicado por la dirección de investigación criminal y apoyo a la justicia (DIRINCRI)	161
Anexos 6. Delitos más comunes cometidos por la Red-Internet publicado por la dirección de investigación criminal y apoyo a la justicia (DIRINCRI)	162
Anexos 7. Examen pericial de informática forense	163
Anexos 8. Organización interna del laboratorio de pericia informático	164
Anexos 9. Componentes del sistema informático	165

Anexo 10. Matriz de categorías y sub categorías:	166
Anexo 11. Matriz investigación	167
Anexo 12. Matriz de triangulación	168
Anexo 13. Entrevista a los peritos de informático Perú	172
Anexo 14. Entrevista a los jueces y fiscales	173
Anexo 14-A. Entrevista a los jueces y fiscales	174
Anexo 14-B. Entrevista a los jueces y fiscales	175
Anexo 14-C. Entrevista a los jueces y fiscales	176
Anexo 14-D. Entrevista al Perito Analista de Divindat-PNP	177
Anexo 14-E. Entrevista a docente universitario	178
Anexo 14-F. Entrevista a Fiscal Provincia de Ventanilla	179
Anexo 14-G. Entrevista a Fiscal Provincia de Ventanilla	180
Anexo 14-H. Entrevista a Fiscal Provincia de Ventanilla	181
Anexo 14-I. Entrevista a Fiscal Provincia de Ventanilla	182
Anexo 15- Acta de Transcripción de prueba digital en la Fiscalía de Ventanilla	183
Anexo 15-A. de acta de transcripción	186
Anexo 16. Audiencia de Visualización de prueba digital	188

Resumen

La presente investigación titulada: "Tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017", tuvo como objetivo general describir el tratamiento de la prueba digital aportada por las partes en el Proceso Penal del Ministerio Publico de Ventanilla, Callao - 2017.

El método empleado fue deductivo, el tipo de investigación fue básica de nivel descriptivo de enfoque cualitativo; de diseño no experimental. La población estuvo formada por fiscales y jueces del distrito judicial de Ventanilla y perito especialista en informática forense. La técnica empleada para recolectar información fue la observación, entrevista, análisis documental y los instrumentos de recolección de datos fueron cuestionarios, guía de observación, guía de entrevista; que fueron debidamente validados a través de juicios de expertos.

Se llegaron a las siguientes conclusiones:

La prueba digital no solo es insuficiente, sino, no cuenta con un tratamiento especial en el Nuevo Código Procesal Penal del 2004, dado que el manejo se lleva a cabo bajo la observancia del Artículo 185º del Código Procesal Penal como prueba documental.

El Ministerio Publico cuenta con una insuficiente implementación tecnológica para brindar un manejo adecuado que garantice la valoración de la prueba digital.

La obtención de las pruebas digitales debe ser bajo la observación y respeto de los derechos fundamentales de las personas, y la incorporación y valoración están sujetos al debate probatorio en juicio; de lo contrario es susceptible de exclusión probatoria.

La vulneración de los Derechos Fundamentales en la obtención de la prueba digital, impide al Juez la valoración de la prueba tal como lo dispone el Artículo 159º de Código Procesal Penal.

Palabras claves: prueba digital, forense, Hash, informática y valoración.

Abstract

The present investigation entitled: "Treatment of the digital evidence offered by the parties in the criminal prosecution of the Public Prosecutor's Office of Ventanilla, Callao - 2017", had as its general objective to describe the treatment of the digital evidence provided by the parties in the criminal proceedings of the Public Ministry of Ventanilla, Callao - 2017.

The method used was deductive, the type of research was basic descriptive level qualitative approach; of non-experimental design. The population was formed by prosecutors and judges of the judicial district of Ventanilla and expert forensic computer expert. The technique used to collect information was observation, interview, documentary analysis and data collection instruments were questionnaires, observation guide, interview guide; that were duly validated through expert judgments.

The following conclusions were reached:

The digital test is not only insufficient, but also has no special treatment in the New Code of Criminal Procedure of 2004, given that the handling is carried out under the observance of article 185 of the Criminal Procedure Code as documentary evidence.

The Public Ministry has an insufficient technological implementation to provide an adequate management that guarantees the valuation of the digital test.

The digital evidence must be obtained under the observation and respect of the fundamental rights of the people, and the incorporation and evaluation are subject to the evidentiary debate in the trial; otherwise it is subject to probation exclusion.

The violation of the Fundamental Rights in obtaining the digital proof, prevents the Judge from assessing the evidence as provided in Article 159 of the Criminal Procedure Code.

Key words: digital, forensic, Hash, computer and assessment test

I. Introducción

1.1 . Trabajos Previos

En el presente trabajo de investigación respecto a la prueba digital se identificó algunos trabajos previos con la finalidad de determinar el tratamiento de las pruebas digitales ofrecida por las partes en el proceso penal, para lo cual se ha citado los siguientes trabajos:

Trabajos Previos Internacionales

León (2015), en su trabajo de investigación tesis titulada, *procedimiento de cadena de custodia sobre contenido digital y su valoración como prueba documental dentro del código orgánico integral penal*; el tipo de investigación es cuantitativa, sustentada en la Universidad Nacional de Loja de Ecuador, para obtener el Título de Abogado; en el cual presentó las siguientes conclusiones que a continuación se detalla “el manejo de custodia sobre el contenido digital no es suficientemente, lo que generara un problema en la interpretación y puede ser pasible de exclusión en la valoración. Asimismo, los profesionales de derecho no están capacitados en las técnicas digitales forenses, desconociendo los procedimientos para valoración sin que hayan sido alteradas” (p.95).

Según Bueno de Mata (2013), en su investigación de tesis doctoral titulada, *a prueba electrónica en el marco de una administración de justicia informatizada*. El tipo de investigación con enfoque cualitativa y nivel descriptivo, sustentada en la Universidad Nacional de Salamanca; escuela de posgrado con la finalidad de obtener el grado de magister en Derecho; presentó las siguientes conclusiones, “el Derecho Penal no ha tenido otra opción que volverse permeable al avance vertiginoso de la tecnología y ceder espacio a la informatización de sus contenidos. Los emails, páginas web, SMS, Whatsapp, imágenes digitales, videos conferencias, y otros son elementos que constituyen elementos digitales, denominado prueba electrónica, las mismas que necesitan una secuencia de procedimientos tecnológicos que la administración de justicia no cuenta para una valoración eficaz” (p.130).

13

Pereira (2013), en su Tesis titulada “*la exhibición de documentos probatorios y soportes informáticos*”, sustentada en la Universidad Nacional de Girona,

Cataluña de España; presentó las siguientes conclusiones que a modo de resumen se detallan “La aplicación Hash es una técnica informática de la más alta tecnología que permite el aseguramiento de la integridad de las pruebas digitales. Están basadas en la obtención de datos de los medios electrónicos denominado copia espejo el que identifica el origen de la información en los dispositivos electrónicos como una copia única. Las funciones que cumple el criptográfico hash, es mitigar las dificultades o errores de los sectores de los dispositivos de almacenamiento de la información que pudieran afectar la integridad de los datos, dando una alta fiabilidad de autenticidad e integridad de la información” (p.419).

Chavarry (2011), presentó su tesis doctoral titulada, *la prueba ilícita penal en la administración de justicia en el Perú*. Sustentada en la Universidad Nacional de Trujillo; Perú, en la escuela de posgrado en Derecho; presentó la siguiente conclusión “en el Proceso Penal uno de los elementos de mayor relevancia está constituido por la prueba, consecuentemente su obtención debe realizarse con observancia de los preceptos de legitimidad, licitud y legalidad; y, fundamentalmente, con observancia del respeto de la persona humana” (p.160).

Bravo (2010), en su Tesina titulada, *la prueba en el proceso penal*, tipo de investigación descriptiva, sustentada en la Universidad Nacional Universidad de Cuenca facultad de jurisprudencia, ciencias políticas y sociales; escuela de Derecho; Presentó las siguientes conclusiones que a modo de resumen se detallan, “La prueba dentro de cualquier proceso es fundamental, porque de ella se va a obtener la verdad procesal; y, el juzgador en base a las pruebas formará su convicción para declarar la responsabilidad penal del acusado. Puesto que, en el nuevo sistema acusatorio oral vigente en la actualidad, es donde más se ve reflejado el peso fundamental de las pruebas, y bajo los principios de oralidad e inmediación el tribunal constará la acreditación e incorporación”. (p.73).

Puig (s/f), en su tesis doctoral titulada, *la prueba electrónica y sus implicancias en la seguridad de la empresa*. Sustentada en la Universidad Nacional Ramón Llull; Barcelona de España, en la escuela de posgrado; presentó las siguientes conclusiones que a modo de resumen se detallan, “la valoración de la prueba digital por el Tribunal se fundamenta en la facultad discrecional del juzgador que consiste

en las reglas de la libre y sana crítica razonada y oralizada del informe o dictamen pericial bajo la observancia del principio de contradicción en el juicio. En esa misma línea, el juzgador realiza un ejercicio de razonamiento lógico para su respectiva valoración e exclusión probatoria para luego emitir un fallo con una debida motivación” (p.376).

Trabajos Previos Nacionales

Pareja (2017), presentó su tesis doctoral titulada, *modelo de control constitucional para la admisión de la prueba de cargo con violación a derechos fundamentales en el sistema jurídico peruano*. Sustentada en la Universidad Pontificia Católica del Perú; en la escuela de posgrado con la finalidad de optar el grado de Magister en Derecho Procesal Penal; quién en su investigación presentó la siguiente conclusión “los derechos fundamentales de las personas consagrado en la Constitución constituyen la base y piedra angular de principios y garantías sobre la cual se erige todo el ordenamiento jurídico como protección de los conflictos y mantener la armonía de la sociedad; en consecuencia es importante el reconocimiento pleno de los derechos constituciones de las personas” (p.116).

Sequeiros (2015), en su Tesis titulada, *vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano-2015*; el tipo de investigación No experimental enfoque cualitativo, sustentada en la Universidad Nacional Huánuco facultad de Derecho y Ciencias Políticas, para obtener el Título de Abogado; en el cual Presentó las siguientes conclusiones que a modo de resumen se detallan “la naturaleza virtual de los delitos informáticos, puede generar lagunas en la tipificación y subsunción entre el hecho del delito y encuadramiento de la norma penal, ya que la informática no tiene límites, que a nivel general, existen modalidades de comercio electrónico, asimismo distintas formas de delitos informáticos, por lo que se debe crear instrumentos legales eficaces que afronten este problema social.

De la misma forma los delitos informáticos no deben ser impedimento que el cibernauta se vea limitado en las actividades de comunicación remota, Interconectividad, comercio electrónico, entre otros; sino por el contrario esta problemática debe plantear un reto a los profesionales de la informática, y a los

operadores jurídicos esfuerzos para implementar los aspectos de seguridad, controles, integridad de la información” (p.44).

Cárdenas (2015), en su Tesis titulada, *la comunicación digital mediante Redes sociales de organizaciones Públicas*; el tipo de investigación enfoque cualitativo, diseño descriptivo; sustentada en la Universidad Nacional Mayor de San Marcos Facultad de Letras y Ciencias Humanas E.A.P. De Comunicación Social, para obtener el Título de Abogado; en su investigación presentó las siguientes conclusiones que a modo de resumen se detallan “la comunicación a través de redes sociales, como Facebook, instagram, WhatsApp, email, entre otros, influyen aperturas de espacios de comunicación tecnológica en la mayor parte de la población, tanto a nivel local, nacional e intercontinental. Esto hace que las personas naturales, instituciones y organizaciones accedan a este sistema de plataformas para interactuar constantemente con los trabajadores, instituciones, empleados, funcionarios y público en general. El uso de estos entornos virtuales de parte de las instituciones privadas y públicas genera un nuevo contexto por el cual las instituciones gubernamentales y la sociedad puedan comunicarse. Esta necesidad de comunicación remota ha reflejado en los diferentes países de modo que han considerado como el inicio de un Gobierno electrónico a nivel mundial, incluso la ONU ha declarado el Uso de Internet como un Derecho Humano, por el cual los países deben trazar políticas para su implementación, y también considera que el uso de redes sociales forma parte activo del tráfico comercial entre las entidades públicas y privadas en el ámbito del intercambio comercial que concierne al Gobierno electrónico entre los países”(p.103).

Duarte (2012), en su Tesis titulada, *Valoración probatoria de los documentos audiovisuales*; el tipo de investigación enfoque cualitativo nivel descriptivo; sustentada en la Universidad Nacional Mayor de San Marcos, Facultad de Derecho, para obtener el grado Magister en Derecho Procesal; en su investigación Presentó las siguientes conclusiones que a continuación se detallan “La filmación en audiovisuales que sirva de prueba para la sanción de la comisión de un hecho delictivo no vulnera el derecho fundamental a la intimidad, puesto que, de acuerdo al criterio del reconocido jurista Carlos Santiago Nino, el derecho constitucional al respecto de la intimidad, comprende específicamente aquellas acciones privadas

que no dañen a terceros, y son exentos del conocimiento de los demás. En consecuencia, el film de un delito son documentos audiovisuales probatorios útiles y pertinentes que acreditan los actos ilícitos. Concluyó que, el video no vulnera ninguna de las garantías constitucionales tales como: el Derecho a un proceso justo, el derecho al ejercicio de la libertad de expresión y derecho al acceso a la información, derecho a la no violación de la intimidad, derecho al prestigio profesional y al honor, derecho a la propia imagen y/o voz. La conclusión de la investigación también es, si uno de los intervinientes graba la conversación y luego ofrece como medio probatorio en un proceso, no configura una prueba ilícita por lo que no hubo vulneración del derecho fundamental al secreto de las comunicaciones, puesto que éste derecho sólo y exclusivamente puede ser afectado por la intervención de las terceras personas quienes representan ser ajenas a la conversación” (p.227).

Baudelio (2011), en su Tesis titulada, *la prueba ilícita penal en la administración de justicia en el Perú Petroaudios Vladivideos*; el tipo de investigación enfoque cuantitativo; sustentada en la Universidad Nacional de Trujillo, Facultad de Derecho, para obtener el grado Doctor en Derecho y Ciencias Políticas; en su investigación Presentó las siguientes conclusiones que el resumen se detallan a continuación “uno de los elementos de mayor relevancia para impartir justicia y conocer la verdad está constituido por la consistencia de la prueba, consecuentemente su obtención, incorporación y valoración probatoria debe realizarse bajo la observancia de los principios constitucionales de legitimidad, licitud y legalidad; y, principalmente; teniendo en cuenta el primer Artículo de nuestra carta magna el respeto de la persona humana y su dignidad humana. Cabe señalór que en la época actual, la actuación y valoración de la prueba está sujeto a los conocimientos técnicos y científicos de los peritos, pues su valoración y eficacia depende de la facultad discrecional de los jueces, quienes deciden a través de las reglas de la sana crítica y las máximas de experiencia; vale decir por la observancia de las pruebas sometidas a los criterios de la ciencia y la tecnología de manera que los dictámenes periciales corroboren fiabilidad y autenticidad para las decisiones judiciales”(p.172).

1.2 . Marco Teórico Referencial de la Prueba Digital

En este capítulo se abordará los conceptos más importantes que constituyen la estructura de la investigación, en virtud del cual, primero abordaremos el concepto más importante que va permitir la decisión de proceso judicial.

Antes de enfocar la evidencia digital es importante definir el concepto de sistema informático, que consiste en un conjunto de elementos que se encargan del tratamiento automático de la información, que a su vez conformado por tres componentes: el primero es el componente físico, está constituido por todos los dispositivos Hardware (disco duro, memorias, USB (Universal Serial Bus), CD (Disco Compacto), DVD (Disco Video Digital), etc.), el segundo es el componente lógico conformado por los programas denominado software (hash, recuperadores, hacker, antivirus, restauradores, servidores, IP, Internet, redes sociales, email, páginas web, etc.) y un tercero es el componente humano está conformado por las personas que interactúan con el uso de las computadoras, quiénes son las personas que sufren agravios contra su derechos o las personas que cometen algún acto ilícito a través de las red y las mismas que dejan evidencias (ver anexo 9). Es así que la informática es el estudio y tratamiento automático de la información y la información es un conjunto de datos tales como audio, videos, texto, imagen, programas, etc.

La globalización o integración mundial a través de las redes ha generado un gran avance tecnológico, de manera que ha permitido cambiar nuestro modo de comunicación de manera rápida e inmediata; esta dinámica de comunicación e interacción virtual hace que las personas dejen evidencias en la red. Lo que implica que este medio de comunicación se da a través de los medios como son: e-mails (correo electrónico), SMS (Short Message Service que significa servicio de mensajes cortos), Skype (video llamadas), YouTube, y redes sociales como Facebook, Twitter e Instagram, entre otros, como las denominadas App WhatsApp, lo que permite las comunicaciones bidireccionales o multidireccionales entre las personas de los distintos países (Pérez, 2014, p.3).

Los medios digitales cuyo contenido se registra a través de Internet, páginas web, redes sociales, mensajería instantánea entre otros, se han convertido en

auténticos y verdaderos instrumentos de registro de evidencias digitales; por lo que no podemos dejar de mencionar lo jurídico, dado que la interacción de las personas en esta red hace que dejen evidencias de los hechos delictivos, como imágenes, textos, audio, vídeos, sonidos de voz, grabaciones, etc. Lo que representa un medio de prueba digital que permite probar un hecho en la vida judicial de modo que tal permite generar certeza en el juez (Sánchez, 2016, pp.41-42).

Es importante hacer una distinción del medio de prueba, puesto que será considerado como tal, cuando haya de probarse electrónicamente un hecho en la red, es decir, cuando una persona ha cometido un hecho ilícito a través de los medios como WhatsApp, Facebook, Skype, MSN, email, entre otros. Estas evidencias, a pesar de representar hechos ciertos, pierden valor probatorio si en su obtención se ha afectado algún derecho fundamental, asimismo está sujeto a la autenticidad e integridad; es más existe un requisito que debe haber sido examinado por un profesional de pericia informática, de modo que garantice la eficacia y validez procesal. (Gines, 2011, p.26).

En nuestra legislación peruana la prueba digital está implícito en el Art. 185 del Código Procesal Penal del 2004 considerado como una prueba documento, por lo que tenemos que recurrir a la doctrina para poder tener una referencia: la prueba es aquella razón, fundamento, argumento, elemento, instrumento u otro medio con el que se pretende demostrar, corroborar, contratar y hacer patente la autenticidad e integridad de un una cosa o hecho delictivo ocurrido, vale decir la prueba representa un derecho fundamental para las partes que lo invocan y una obligación el juez valorar y motivar (Sentis, 1979, p.35).

Enseguida se abordará distintas posturas de los juristas respecto a la prueba digital o electrónica. La prueba electrónica no cuenta con una regulación especial en el Código Procesal Penal y dejan a la independencia y autonomía. Esto implica que la prueba digital es admitida e incorporada al proceso como una prueba documental jurisprudencialmente, dado que se trata de un medio de reproducción de la palabra, el sonido y la imagen, por lo que representa un instrumento que permite almacenar y reproducir palabras, datos, información relevante. En consecuencia se considera incluso como *numerus apertus* es decir la prueba digital

está comprendida como un medio de prueba independiente y autónoma que no depende de manera específica de algún Artículo del código penal, puesto que no está regulado su tratamiento procesal de manera específica (Bueno de mata, 2013, p.103).

Marco Normativo.

La normatividad que garantiza el derecho a ofrecer las pruebas digitales es la carta magna Constitución Política del Perú de 1993, del cual citaremos los siguientes: el Artículo 2º tipifica respecto a la garantía de los Derechos constitucionales de la persona, es decir toda persona tiene los siguientes derechos: en el inciso 6) del mismo Artículo de esta carta magna señaló que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. Es decir, tanto las organizaciones e instituciones públicas y privadas, que hacen uso de la tecnología de la información y comunicación-Tics están prohibidas en difundir informaciones que afecten directamente al respecto al derecho fundamental mencionado, de caso contrario estarán sujetos a una responsabilidad civil, penal y administrativa.

Del mismo modo, el numeral 7) de la Código Penal tipifica, toda persona tiene el derecho al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias.

Desde el punto de vista de la obtención de las pruebas digitales, sin su consentimiento del titular que afecte la imagen el profesionalismo y la dignidad; ya sea una grabación de voz sin que haya una autorización del secreto de las comunicaciones, o cualquier otro que atente la intimidad personal o familiar o que denigre la imagen o dañe la dignidad, será excluido del proceso como una prueba ilícita, ilegal o irregular dependiente de cada caso. También el inciso 9), señala que toda persona tiene el derecho a la inviolabilidad del domicilio. Continuando desde la perspectiva de la obtención de los medios probatorios digitales o electrónicos, ninguna persona puede ingresar a un domicilio por más que sea autoridad policial a efectuar investigaciones, registros, incautaciones, detenciones, decomisos, otros sin previa autorización de la autoridad judicial, es decir del juez, o en todo caso con autorización de la misma persona que lo habita, salvo excepción de delitos que se

cometen en flagrancia o en todo caso en grave peligro inminente de su perpetración inmediata.

Por último, el inciso 10) de la Código Penal preceptúa, toda persona tiene el derecho al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. En este acápite la constitución tipifica de manera categórica y expresa que toda persona tiene el derecho fundamental a que no se le intervenga sus comunicaciones, vale decir todas las conversaciones son inviolables, están completamente prohibidas los chuponeos o interceptaciones telefónica, no solo ello, sino también, los documentos privados gozan de esta misma protección constitucional. Para considerar como un ejemplo de ello fue el Caso de Alberto Quimper, a quién se le interceptó telefónicamente sin autorización del juez, motivo por el cual se exculpo, dado que el medio probatorio fue excluido por considerarse como ilícita y por haber atentado el derecho fundamental al secreto de las comunicaciones.

Asimismo, el contenido de la normatividad señaló que las comunicaciones, telecomunicaciones y sus instrumentos, solo y únicamente pueden intervenir, incautarse, registrar, interferir, interceptarse o intervenir, previa autorización del juez competente de la jurisdicción, además que dicha orden debe estar debidamente motivado, es decir debe contener de manera explícita todas las acciones a tomar, con sus respectivas descripciones y características con fecha, hora y plazo, bajo la observancia de las garantías constitucionales establecidas en la ley, la constitución y en los tratados.

Del mismo modo, sobre los principios y garantías constitucionales establecidas en el Artículo 200º respecto a las Acciones de Garantía Constitucional, en el numeral 3) señaló sobre la Acción de Hábeas Data, es decir todas las personas gozan de un derecho constitucional de acceso a la información para obtener de manera gratuita de cualquier institución pública o privada, este derecho le permite a los ciudadanos de estar informado de las actividades de las instituciones. De caso contrario el recurso de habeas data permite hacer respetar en los casos “contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el

Artículo 2, incisos 5, 6 y 7 de la Constitución”. Vale decir, toda persona tiene el derecho de conocer y solicitar cualquier información de las entidades, las mismas otorgan dentro del plazo de ley, bajo responsabilidad de ser denunciado por ocultamiento de información.

Prueba Digital.

Existen diferentes posturas en la doctrina respecto al concepto de prueba digital, en este contexto la definición más aceptada es, cualquier información o datos obtenida a través de cualquier medio o dispositivo electrónico cuya finalidad sea corroborar o demostrar convencimiento y certeza al juez de un acto delictivo suscitado, siempre que cumpla los requisitos en su obtención de no vulnerar los derechos fundamentales, de manera que constituya evidencias útiles, lícitas, idóneas y pertinentes.

De modo que permite acreditar y corroborar como elementos de convicción hechos relevantes, ya sean físicos impresos a través de medios electrónicos, contenido en dispositivos hardware, y un elemento lógico denominado software. También se refiere a toda información de Internet, redes sociales, pagina web, emails, etc. que tenga valor probatorio almacenada en un dispositivo electrónico, cuyo contenido permita corroborar un hecho en el proceso de investigación ya sea por una falta u infracción penal que se subsuma en los delitos informáticos (Delgado, 2013, p.01).

En ese orden de ideas el jurista reconocido en la doctrina, sostuvo que la prueba digital es “todo dispositivo electrónico, soporte magnético, medio digital o electrónico, creado para almacenar datos o transferirla, cuyo contenido represente un hecho, una actividad, expresión de voluntad de hacer o no hacer entre otros”, la información a la que hace referencia en autor esta almacenada en un soporte electrónico, el cual puede ser un USB, disco duro, memorias, pendrive, email, onedrive, cloud computer, etc. Que están guardados en un formato determinado, el cual permitirá conocer y acreditar la certeza de un hecho ilícito (Fernández, pp. 397-398).

La Prueba.

En la presente investigación abordaremos los conceptos más relevantes que forma parte de la estructura del trabajo y uno de los más importantes es la definición de la prueba. Al respecto se abordará la postura de los diferentes juristas:

Palacio (2000), conceptualiza doctrinalmente a la prueba dentro del derecho penal como “el conjunto de actos procesales que se realizan bajo el límite de un plazo establecido, establecido y autorizados por la ley; cuya finalidad es a generar la certeza y convicción en el juez acerca de la existencia o inexistencia de los hechos materia de imputación”. (p.12).

La cita textual respecto a la postura del autor refiere que la prueba es una secuencia de actos generalmente dentro del proceso, que su validez está delimitada por los principios y derechos constitucionales; vale decir que su legitimidad está condicionado a la no vulnerabilidad del derecho a la intimidad, así como también a la vulnerabilidad del secreto de las comunicaciones e inviolabilidad de domicilio y otros bajo el principio de legalidad. De lo contrario podría ser materia de exclusión probatoria. Adicionalmente todo medio probatorio cuya finalidad es probar la verdad o falsedad de un hecho está delimitado por una secuencia de plazos, incluso a pesar de tener pruebas que corroboren un hecho si no se presenta dentro del plazo que establece la Ley, sencillamente no será valorado por el Juez.

En ese orden de ideas, también el jurista Jauchen (2002), sostuvo que la prueba es “el conjunto de razones que representan un hecho aportados u ofrecidos al proceso, que le permite conocer al juez a través del principio de la inmediación la existencia o inexistencia de un hecho sobre el cual, quién con la facultad discrecional debe decidir emitiendo un fallo”. (p.19). La cita refiere que el juez conoce los hechos realizados a través de los medios de prueba que han sido introducidos, siguiendo los procedimientos y protocolos procesales, de manera que el juicio a través del principio de oralidad el juez conoce los hechos, el cual le permitirá valorar y dictar una resolución.

Asimismo, Guerrero (2004), sostuvo que la prueba “es la contrastación, corroboración o demostración concreta y legal de un hecho ocurrido” (p.13). El autor

refiere que la prueba es la demostración legal, lo que advierte con el término legal es que, toda producción y /o recojo de la prueba debe estar bajo los límites del respeto de los derechos constitucionales; solo así se garantizará la legitimidad y la legalidad para demostrar un hecho dentro de un proceso judicial, de caso contrario será materia de exclusión probatoria.

También la postura del reconocido Echandía (2002), coincidió en señaló que la prueba judicial “son las razones que permiten al juzgador tener los elementos de certeza de los hechos, mientras que los medios de prueba comprenden los elementos o instrumentos presentados por las partes para su valoración”. (p.20). El autor hace una aclaración de la diferencia entre la prueba judicial y los medios de prueba, dado que algunas veces genera confusión entre estos dos términos. La prueba permite generar convicción y certeza en el Juez, puesto la motivación de la sentencia estará fundamentado en los hechos corroborados en las pruebas; y los medios de prueba referidos por el autor son los instrumentos o elementos que han servido su incorporación, por ejemplo, a través de documentos escritos, digitales, testimonios, peritajes, etc.

Otro autor de la doctrina sostuvo, que la prueba en el Derecho Penal, “es un hecho ocurrido en el contexto del mundo de los fenómenos constitutivos que atenta los derechos como una infracción penal”; tales como puede ser el delito de homicidio, injuria, robo y cualquier otro; en tanto el medio de prueba son los instrumentos o documentos a través del cual el juez incorpora en el proceso, la misma que será acreditado y corroborado como un hecho constitutivo de infracción penal; cabe resaltar que tanto los medios de prueba como la prueba en si misma deben haber sido obtenidos sin la afectación de los principios y derechos constitucionales; de ser así permitirá la valoración del juez en el proceso, quién a su vez motivara fu fallo correspondiente al hecho factico. A manera de conclusión respecto a la diferencia entre prueba y medio de prueba es que, el primero son los hechos facticos ocurridos y el segundo es que dichos hechos se encuentra almacenados en algún medio o dispositivo, ya sea electrónico o físico; para su mejor comprensión se considera el ejemplo de un homicidio ocurrido en un hotel que fue registrado en la cámara de seguridad, en este caso la prueba seria el homicidio, y el medio de prueba es el Disco Compacto (CD), Computadora o Disco

duro que contiene los hechos. Asimismo, es importante precisar que las pruebas en algún dispositivo electrónico deben haber sido sometido a una pericia informática para su valoración. (Zavala, J. s/f. p.21).

Bustamante (2001), señaló que “el derecho constitucional al ofrecimiento de la prueba se articula con otro derecho que es el debido proceso a lograr la justicia; que goza de todos los principios y garantías constitucionales del cual derivan la relevancia de su carácter protector; su mayor valor, su progresividad, y la especial protección de su contenido” (pp. 8-9). El autor refiere que el derecho a la prueba integra implícitamente el derecho al debido proceso, lo que implica la tutela jurisdiccional efectiva del cual goza las partes del proceso como un derecho fundamental.

Naturaleza de la Prueba.

A lo largo del tiempo, según los estudios jurisprudenciales y doctrinales la prueba digital o electrónica se ha caracterizado como una prueba eminentemente documental, tal es así en la actualidad nuestra legislación ha sido considerado como una prueba documental, tipificado en el Artículo 185º del Nuevo Código Procesal Penal. Existe varias teorías, la doctrina sostiene, que la teoría analógica defiende la existencia de ciertas semejanzas entre la prueba digital o electrónica y la prueba documental, razón por la cual se encuentra tipificado en el Artículo 185º del Código Procesal Penal. Sin embargo, la teoría autónoma considerada como una segunda tesis de mayor aceptación, quién sostuvo que la prueba digital es completamente independiente a la prueba documental, por lo que para hacer valer en un proceso se necesita dos requisitos, primero que su obtención sea lícita sin vulneración de los derechos fundamentales y la segunda, para su valoración necesita de su posterior verificación y autenticidad de la autoría (Pereira, pp.257-259).

En ese mismo orden de ideas, la tercera teoría de la equivalencia funcional, sostuvo que “el contenido de un medio, dispositivo o documento electrónico representan el mismo valor o efecto que el contenido plasmado en un documento físico en soporte de papel”, lo que implica que no debe haber una discriminación entre los mensajes de datos y las declaraciones de voluntad, quiere decir que las

consecuencias o efectos jurídicos pretendidos por el emisor de la declaración deben ser independientes al del soporte en papel y el de digital. Sin embargo, para su valoración en el proceso debe ser un documento autentico y original con un autor identificado (Jurado, 2011, p.56).

Uno de los elementos más relevantes de la prueba electrónica es la investigación del hecho electrónico, vale decir, la integridad y sobre todo el origen no haya sufrido ninguna modificación, alteración, edición, etc. De manera que se pueda ofrecer e incorporar al proceso para que el juez pueda valorar. Uno de los reconocidos en el ámbito de la doctrina es Muñoz (2009), quién sostuvo que “investigar una prueba digital es como abrir una puerta para descubrir lo que hay dentro” (p.23). El autor hace una distinción entre probar y investigar, el primero consiste en acreditar la existencia del hecho con los medios digitales para incorporar al proceso; mientras que, investigar significa la búsqueda de conocimientos e circunstancias acerca de los hechos ocurridos. También afirma que el hecho electrónico de la prueba recaerá sobre su misma naturaleza elementos y efectos.

Medios de Prueba.

Los medios de prueba en nuestra legislación peruana son tres, uno de ellos el medio testimonial, los cuales a través de los dictámenes de los peritos con conocimientos científicos, artísticos, técnicos o prácticos de experiencia de personas especializadas se incorpora al proceso. El segundo es el medio de prueba documental, precisamente las evidencias digitales se encuentran en éste, los cuales se aportan a través de medios electrónicos como el USB, correo electrónico, disco duro, pendrive, Cloud Computing entre otros y finalmente el medio de prueba técnica, la se incorpora a través de la cadena de custodia. Respecto a los medios de prueba tipifica el Artículo 157º del Código Procesal Penal, que tipifica, de manera expresa, los hechos ocurridos materia de investigación u objetos de prueba, pueden ser corroborados, contrastados o acreditados por cualquier medio, siempre en cuando esté permitido por la ley; previniendo a que no se vulneren los derechos fundamentales reconocidos por la Constitución Política del Perú.

Fuente de Prueba.

Es de vital importancia distinguir de donde proviene la prueba, es decir cuál es la fuente; para dilucidar el concepto real se considerará al tratadista reconocido en el mundo jurídico: Carnelutti (2000), quién sostuvo, que las fuentes de prueba “son hechos que permiten la deducción del hecho a probar y que están constituidos por la representación de éste”. El tratadista refiere que es una realidad que ocurre en el ámbito extraprocesal, lo que implica, que se da fuera del ámbito del Proceso Penal o judicial; sin embargo, su incorporación al proceso es indispensable para la determinación de los procesos. Un ejemplo de fuente de prueba se da con el dictamen pericial, que definitivamente se da fuera de un contexto de todo Proceso Penal o judicial, dicha prueba científica cuenta con una alta probabilidad de convertirse en argumento eficaz de valor probatorio para el juez, dado que el juzgador conocerá en el juicio oral los hechos a través de la oralización del perito.

Es importante distinguir los delitos cometidos que permitan acreditar con la evidencia digital, este tipo de procesos es completamente distinto a los procesos comunes, puesto que valoración está sujeto al tratamiento adecuado que se da al momento de obtener e incorporar al proceso. Para lo cual abordaremos las fuentes de la evidencia digital.

Las Fuentes de Evidencia Digital.

Continuando con las fuentes encontraremos la clasificación en tres grupos importantes, los cuales son: primero sistemas de Computación (Hardware). - estos sistemas están conformados por un conjunto de equipos electrónicos como las computadoras personales incluidos sus componentes como teclados, mouse, monitor, cámara web. Adicionalmente los periféricos como USB (Universal Serial Bus), CD (Disco Compacto), DVD (Disco Video Digital), pendrive, disco duro, memoria flash tienen la gran capacidad de almacenamiento de información, los que los convierte en una importante fuente de evidencia digital. Segundo sistema de comunicación electrónica, dentro de este tipo de comunicación se encuentran la gran red de telecomunicaciones, ya sea de fibra óptica o inalámbrica y la banda ancha de Internet. Es decir, la comunicación a través de Facebook, WhatsApp, Instagram, correo electrónico, páginas web, Cloud Computing entre otros, los

mismos que representan la fuente de información como evidencia de la prueba digital.

Tercero sistemas Convergentes, es una conjunto de equipos que están conformados aparatos móviles como teléfono celulares, asistentes personales digitales PDAs, las tarjetas inteligentes con Internet Protocol (IP), pendrive que son lápices con memoria de almacenamiento entre otros que pueden servir de evidencia digital y cuarto la comunicación virtual y acceso remoto en las que interactuamos en la sociedad actual, los delitos que se cometen dejan evidencia en algún sistema ya sea de computación, de comunicación electrónica u otro. Dicha evidencia puede ser un mensaje de texto, una foto, un audio, un video u otro que queda almacenado como datos, los cuales permitirán identificar y descubrir la conducta ilícita de sus víctimas. Por último el Cibercrimen; que consiste en la conducta ilícita que afectan los sistemas de datos informáticos, así como también afectan otros bienes jurídicos tutelados de relevancia penal, que se comenten a través del uso de la red Internet, páginas web, emails, redes sociales y programas como el Phishing y Pharming entre otros (Congreso de la República, 2013).

Objeto de la Prueba.

Existen distintas posturas de la doctrina respecto al objeto de la prueba electrónica en el proceso judicial, el portal una publicación oficial señaló, que “la prueba electrónica son hechos electrónicos, vale decir, que la información obtenida a través de los dispositivos electrónicos, magnéticos o medio digital. El objetivo que persigue la prueba electrónica es corroborar y probar o en su defecto acreditar los hechos ocurridos los cuales deben tutelar los petitorios de las partes que invocan Asimismo, el Código Procesal Penal en su Artículo 156º tipifica respecto al objeto de prueba, considerándolos como a los hechos que se refieran a la imputación, es decir la acreditación o indicio de permitirá la imputación del autor; que posteriormente su acreditación de la misma permitirá la determinación de la sanción penal del responsable de los hechos; así como el respectivo resarcimiento de los daños y perjuicios derivada del delito (Art. 156, NCPP).

Regulación de la Prueba.

La norma suprema de nuestra legislación peruana tipifica en el Art. 2º 4 derechos fundamentales el cual señaló “toda persona tiene derecho al honor, es decir ningún medio probatorio puede ser obtenido con vulneración de este derechos, asimismo el otro derecho es la buena reputación, que es algo inherente al ser humano, y a gozar de las tranquilidad de entorno familiar o la intimidad personal y familiar, ninguna persona puede gravar su voz o utilizar de ella sin su consentimiento y menos utilizar su imagen, y menos pueden vulnerar, interferir o interceptar el secreto de las comunicaciones, salvo casos excepcionales bajo la autorización judicial del juez competente.

Inherente a este Artículo también hace mención del principio de presunción de inocencia; “toda persona es considerada inocente mientras no se haya declarado judicialmente su responsabilidad”, es decir cualquier persona, por más imputado o denunciado que esté, es inocente, solo se quiebra su inocencia con una sentencia judicial, de caso contrario goza de esta protección constitucional. Asimismo, la constricción tipifica de manera expresa que ninguna persona debe ser víctima de violencia, se entiende por violencia tanto a las agresiones verbales, psicológicas y físicas que generan lesiones, asimismo ninguna persona puede ser sometido a tortura que le generen menoscabo y tampoco no pueden estar sometidos a tratos inhumanos, discriminatorios o humillantes. Es decir, existe una protección constitucional de estos derechos reconocidos en la Constitución, dando una ponderación a ciertos derechos como fundamentales y todos tienen el deber de respetarla.

Asimismo, el Título Preliminar del Nuevo Código Procesal Penal en su Artículo II, tipifica: “la presunción de inocencia es una protección constitucional que persiste pese a que un sujeto este procesado, investigado o imputado, sin embargo, se preserva su inocencia mientras no se demuestre lo contrario y que su culpabilidad de haya declarado a través de un fallo debidamente motivado por el Juez competente”.

Es decir que toda persona goza de una protección constitucional, de manera que a pesar de estar imputado o procesado por cualquier delito o falta, mientras el

juez no se haya pronunciado su culpabilidad a través de una sentencia firme goza de la presunción de inocencia.

Del mismo modo, el Art. IV del mismo código señaló que “el persecutor del delito y el titular de la acción penal es el Ministerio Público, quién a través de los fiscales competentes asumen el proceso de investigación y quiénes a su vez tiene el deber de la carga de la prueba desde el inicio del proceso penal, es decir desde las investigaciones preliminares hasta el juicio oral. En ese mismo orden de ideas el Artículo VI del Título Preliminar señala respecto a la legalidad de las medidas limitativas de derechos, es decir, las decisiones que tome el juzgador sobre las medidas que impidan, restrinjan los derechos fundamentales, es por única y exclusivamente por autorización del juez, a pedido especial del propio Ministerio Público, solo en esos casos se pueden restringir los derechos y sobre todo cuando sustenten suficientes elementos de convicción.

Adicionalmente el Artículo VIII del Título Preliminar tipifica sobre la legitimidad que debe cumplir la prueba. Es decir, en toda obtención de la prueba se debe haber tomado en cuenta el respecto de los principios y garantías constitucionales; de ser así cumplirá con el requisito de la legitimidad, asimismo su obtención e incorporación al proceso debe cumplir con el procedimiento establecido en la normatividad. De caso contrario carecen de efecto legal y es materia de exclusión probatoria considerado como prueba ilícita por afectar y vulnerar derechos constitucionales. De la misma forma la inobservancia de cualquier regla de garantía constitucional favorece al imputado o procesado y que no podrá hacerse valer en su perjuicio.

La legislación peruana señaló tres tipos de prueba en el Código Procesal Penal: el primero es la prueba personal, segundo la prueba documental y por último la prueba técnica, de los cuales la prueba digital se encuentra regulado de manera implícita en la prueba documental tipificado en el Artículo 185º, respecto a las clases de documentos, lo que señala expresamente “son documentos los manuscritos, impresos, fotocopias, fax; luego hace mención a los dispositivos magnéticos como son los disquetes, los dispositivos electrónicos, ópticos como CD, DVD, USB, Pendrive, etc. los cuales pueden almacenar películas, fotografías, y

otros medios con las cuales se pueda registrar o almacenar pruebas radiografías, representaciones gráficas, dibujos, grabaciones magnetofónicas, asimismo hace referente a otros medios que contienen registro de sucesos, imágenes, voces; y, otros similares”. En el caso de las evidencias digitales o pruebas digitales precisamente está considerado como prueba documental, y su tratamiento es bajo la observancia de este Artículo y en cuanto a las pruebas obtenidos por correos, paginas, Twitter, WhatsApp, Facebook, Instagram, Cloud Computing, y otros también están considerados dentro de las pruebas documentales.

Este acápite precisamente refiere a las pruebas digitales, vale decir que la prueba digital o prueba electrónica está tipificado expresamente en nuestro Código Procesal Penal, y su tratamiento está implícita dentro del Artículo 185º específicamente como pruebas documentales y tiene el mismo tratamiento que las pruebas tradicionales.

Documento Electrónico.

También es importante tener en cuenta la definición de documento electrónico, ya que nuestra sociedad actual hace uso continuo de las TICs, dicha tecnología que forma parte de nuestras vidas, en tanto nuestra comunicación es dinámica, es decir nuestra comunicación se ha virtualizado con el uso masivo de las páginas web, correo electrónico, mensajes, WhatsApp, redes sociales, entre otros.

Respecto a la definición de documento electrónico, Peñaranda (2008), sostuvo que “es un instrumento cuyo contenido es un mensaje escrito, cuyo destino es permanecer en el tiempo, en lenguaje convencional, plasmado o guardado sobre un soporte magnético, que puede ser un dispositivo USB, Cloud Computing, u otros” (p. 24). El autor refiere que el documento electrónico es un instrumento escrito, pero a diferencia de otros, esto está en formato electrónico o digital, que puede ser un mensaje, video, fotografías u otros.

Asimismo, en connotado jurista, Rivera (2012), sostuvo que un documento electrónico “contienen mensajes, datos, información, etc., o ser simplemente instrumentos, sin embargo, cabe aclarar que no todo medio electrónico transmite o traslada información, por lo que es recomendable hablar de medios informáticos o

tecnologías de la información” (p.657). El jurista también refiere en el mismo sentido respecto al documento electrónico, al señalar que no todo medio electrónico transfiere información, en tanto recomienda que se debe denominar medio informático, al que engloba de manera general el concepto.

Medios Digitales.

En el medio virtualizado en que vivimos, donde la información se masifica a través de medios electrónicos como WhatsApp, redes sociales, Internet, Messenger, páginas web, Cloud Computing, entre otros, existen un conjunto de medios digitales, los cuales son información ya sea como fotos, imágenes, textos, audio, video, conversación, que se registran en los dispositivos informáticos que tienen la capacidad de almacenamiento en los distintos tipos de periféricos o dispositivos, tales como: computadoras, teléfono celular, Tablet, memorias USB, DVD, CD, cámaras fotográficas, GPS, cámaras de seguridad, drones, etc. Lo cuales pueden ser aportados al proceso judicial a través de estos medios digitales. El Código Procesal Penal, tipifica los medios de prueba en el Artículo 157º el cual señala, los hechos cuyo contenido es objeto de prueba para determinar la responsabilidad, pueden ser contrastados o acreditadas a través de cualquier medio de prueba, siempre en cuando estén establecidos y permitidos por la Ley.

Evidencia Digital.

Para definir el concepto de evidencia digital, trataremos de abordar las diferentes posturas de los tratadistas, uno de los más connotados es Casey (2004), quién sostuvo que la evidencia electrónica o digital es “cualquier información o dato que puede acreditar el suceso de un delito ejecutado (commit), asimismo puede hacer referencia a una dirección, enlace (link) entre el delito cometido y el autor de su víctima” (p.11). (Anexo 1-D), el autor refiere que la evidencia digital es toda información producto de la conducta humana plasmado o extraído en un medio o dispositivo electrónico y/o informático. Es decir, son dispositivos magnéticos constituidos por USB, Disco duro, CD, DVD, memorias, Cloud Computer, OneDrive, e-mails, etc. Los cuales tienen almacenados como contenido datos o información de los hechos, como textos, fotos, imágenes, audio, video, etc. a los cuales también se les denomina evidencia digital. Cabe aclarar la postura del autor refiere que la

evidencia digital es la información que se encuentran registrados o almacenados en algún medio o dispositivo, ya sea electrónico, magnético, óptico magnético o digital.

De singular postura fue la doctrina al sostener, que la evidencia digital “es la materia prima de los investigadores para descubrir la verdad o falsedad donde la tecnología informática forma parte fundamental para obtener resultados científicos de las pruebas”. (Cano, p.67), no obstante, teniendo la visión clara de lo que es cambiante y dinámico la informática, la evidencia digital exige que su tratamiento sea de un manejo de profesionalismo, dado que son volátiles, es decir, duplicable, modificable, alterables, eliminable. Estas características especiales nos advierten que las evidencias digitales necesitan de especialistas con cierto grado de experiencia en la materia, en este caso se necesita de especialistas den informática forense, de manera que emitan un informe de prueba de carácter científico manteniendo su integridad.

Respecto a las pruebas digitales la doctrina considera un conjunto de conceptos, uno de los tratadistas es Casey, quién sostuvo que las pruebas digitales, “es un tipo de evidencia cuyo contenido se encuentra en algún dispositivo construida de campos electrónicos, magnéticos y pulsos electrónicos, los cuales pueden ser extraídos, recolectados y analizados por un conjunto de especialistas llamados peritos, quiénes con instrumentos tecnológicos especiales pueden convertirlo en prueba científica”.

El autor refiere que las pruebas digitales son evidencias (información) recolectados o almacenados en diferentes dispositivos, ya sea en USB (Universal Serial Buss), CD (Disco Compacto), DVD (Disco Video Digital), Celulares, Cámaras de Seguridad y otros aparatos, que para su validez necesariamente tiene que ser analizados por especialistas denominados peritos en informática; quiénes se encargaran de garantizar su fiabilidad e inalterabilidad sometiendo a través de un conjunto de técnicas científicas.

De la misma forma un concepto conocido en la doctrina señaló, que “la evidencia digital es una información o datos almacenados en algún dispositivo en formato binario entre 0 y uno (1) que en términos informáticos se denomina archivos

o ficheros, los cuales se encuentren almacenados en soportes físicos o lógicos de un sistema informático” (López, 2012. p).

El autor refiere que la evidencia digital está constituida por un formato binario, es decir la computadora registra información en ceros y unos, el cual necesita una interpretación de un especialista para poder dar fe de su integridad. Es decir, el almacenamiento se realiza en un medio físico como puede ser un USB, disco duro, etc., sin embargo, la información es lo tangible almacenando en la parte lógica.

También, otro doctrinario sostuvo que la evidencia digital “son objetos de datos de información contenido en dispositivos de almacenamiento, que no son más que una cadena de ceros y unos, es decir, información binaria o digital grabada en un dispositivo magnético” (Reyes, 2010). El autor refiere que la evidencia digital es la información conformada por una cadena de ceros y unos, es decir el código binario almacenada en un dispositivo magnético como: discos duros, memorias, USB, CD, DVD y otros.

Sin ir tan lejos, el jurista sudamericano Del Pino (2012), sostuvo que “la evidencia digital constituye todos aquellos datos e información histórica almacenada en archivos para que se pueda procesar mediante algoritmos abiertos y auditables, con la finalidad de ser expuestos de manera muy sencilla ante los tribunales de justicia”. El autor refiere que la evidencia digital debe ser procesada y auditable es que toda información almacenada en un medio electrónico como los USB, correo electrónico, disco duro entre otros; necesariamente deben ser sometida una pericia informática para su valoración en el proceso judicial.

La Aplicación Hash.

Actualmente el mundo digitalizado viven la sensibilidad o volatilidad de la información, razón por la cual es importante la autenticidad de los archivos digitales, un archivo está constituido por (foto, vídeo, imagen, documento, programa, texto, audio, etc.), dicha información está sometida a una constante manipulación u alteración de datos. En la modificación u alteración de un documento o archivo, se aplica un control denominado filtro, por el cual, las imágenes y archivos son

editados, ya sea comprimiendo, recortando, alterando la autenticidad, según el interés o la necesidad de las partes. He aquí interviene la aplicación del Hash es un algoritmo matemático que permite identificar la autenticidad a través de un valor de codificación el contenido de la información.

Correo Electrónico.

La mensajería electrónica está considerada como correo electrónico, en inglés e-mail, que representa una herramienta de Internet, que permite enviar y recibir mensajes a través de una PC, teléfono móvil, u otro aparato que tenga acceso a la red, que consisten en la transferencia de información de tipo texto, imágenes, sonido, audio, videos, entre otros. Cabe señalar, que los correos electrónicos se encuentran almacenadas en un servidor de emails, es decir no se encuentran en el equipo de quién envía (emisor), tampoco el que recibe (destinatario), salvo que el destinatario descargue y lo guarde en el equipo.

El funcionamiento de los correos electrónicos, es que al momento de enviar primero se transmiten al servidor de correo electrónico para luego ser enviados al destinatario. Al recepcionar el proveedor de correo electrónico hace una solicitud al Servidor de correo, para que los mensajes enviados sean transmitidos al destinatario, de modo que el operador tenga la posibilidad de almacenarla en un dispositivo electrónico. Lo que significa que cualquier evidencia que demuestre una conducta delictiva a través de este medio no quedara impune, dado que con un peritaje se puede acceder al servidor de correo afín de corroborar si fue enviado el mensaje.

Marco Constitucional de la Prueba.

Desde la base constitucional de la legitimidad de la prueba, consideraremos el derecho que tiene todo ciudadano a presentar la prueba en todo proceso; lo que representa un derecho de protección constitucional que goza toda persona, pues se trata del eje transversal por el cual gira la presunción de inocencia; su contenido se encuentra implícito dentro del derecho al debido proceso, tipificado y reconocido en el inciso 3, del Artículo 139 de nuestra carta magna y también en el Art. IX.1 del Código Procesal Penal reconoce el Derecho a utilizar los medios de prueba

pertinentes, asimismo debe la normatividad exigir a que debe cumplir ciertos requisitos para que la obtención de la prueba digital sea lícita y valorada por el juez dentro de un proceso:

El primer requisito de la evidencia digital, es que, en su incorporación al proceso debe cumplir con ser: idónea, pertinente (es decir debe guardar una estrecha relación con el objeto del proceso), útil (sea útil para esclarecer los hechos) y lícita (que haya sido obtenido con respecto de a los principios y garantías constitucionales). Segundo la evidencia debe tener relevancia jurídica de manera que permite corroborar hechos de trascendencia jurídica; Tercero que la prueba haya sido obtenido bajo la observancia de las reglas de la buena fe, cabe señalar que no serán valorados las pruebas obtenidas con la vulneración de los derechos fundamentales, tales como derecho a la intimidad personal y derecho fundamental al secreto de las comunicaciones, al derecho y protección a la inviolabilidad de domicilio, al derecho a la reserva financiera, etc., de caso contrario estaríamos ante un caso de exclusión probatoria.

Cuarto la seguridad y control de prever la cadena de custodia de la prueba, es decir, los medios digitales que conservan los hechos de los actos ilícitos por tratarse de ser públicos, una vez obtenida y ofrecida debe cautelar su autenticidad, para lo cual debe preservarse a través de la cadena de custodia, que representan un elemento indispensable para la validez procesal y la admisibilidad correcta de los medios digitales. Este tratamiento permite garantizar el control, la seguridad y la no contaminación de medio probatorio contenido en cualquier dispositivo electrónico.

Quinto, que las pruebas digitales sean sometidas o practicadas a un examen de pericia informática forense de manera que se garantice la autenticidad y valoración en la eficacia probatoria.

Derecho a la Prueba.

Toda persona que invoca tutela jurisdiccional tiene derecho a la actuación probatoria, ya sea para acreditar o negar, teniendo en cuenta el siguiente orden:

i) *El derecho a ofrecer pruebas*, este derecho básicamente está orientado a contrastar, corroborar y acreditar los hechos ocurridos o no, que representa objeto de la prueba en concreto. Se sostiene sobre la base del principio de aportación de parte, tipificado en Artículo 155º.2 Código Procesal Penal, el mismo que se da en dos instancias: el primero respecto al derecho de ofrecer los medios de prueba para el juicio, oportunidad que se da en la etapa intermedia el Art. 350º.1, posteriormente de la conformidad Art. 373º.1, el segundo, el respecto a la nueva prueba (Art. 385º.2).

ii) *El derecho a que se admitan las pruebas*, la admisión de la prueba está fundada en los siguientes principios de: licitud (Art. VIII Título Preliminar, 155º.2. 167.3 y 159), utilidad (Art. 155º.2. y 352.5.b, necesidad Art. IIº.1. Título Preliminar, y de principio de investigación material tipificado en los Artículo s 385º y 155º.3.

iii) *El derecho a actuación de prueba Art. 375º Código Procesal Penal*, en esta fase se dará inicio a un debate probatorio, en el cual el Juez Penal en la oralización escucha a las partes para luego decidir el orden en la que deben intervenir las declaraciones de los imputados y la actuación de los medios de prueba admitidos. Dando lugar el siguiente orden: Primero el examen del acusado, luego como segundo punto se programará la actuación de los medios probatorios admitidos; en tercer lugar, el interrogatorio directo de los órganos de prueba tanto del Ministerio Público (fiscal) y a los abogados defensores de las partes, en cuarto lugar, la oralización de los medios probatorios. Esta fase de recepción de la prueba se lleva a cabo, bajo los principios de inmediación Art. 393º.1, Publicidad Art. 356, 7,8º, oralidad Art. 356º.1. 361, contradicción Art. IX, 375, 398.8, 386, Legalidad Art. 155º.1. Quinto la valoración probatoria. Para este caso se aplica tres tipos de reglas, tales, que implica la valoración de la legitimidad, exposición oral de resultados obtenidos y adoptados, exposición de hechos convenidos, exposición del examen individual. Lo que permite la aplicación de los criterios del Juez, la lógica, máximas de la experiencia y ciencia, implica que se debe valorar los arrepentidos, coimputados, colaboradores, confesión, testigos de referencia, prueba indiciaria.

iv) Actúen en juicio los medios probatorios válidamente admitidos y también las pruebas de oficio que han sido incorporados a solicitud del Juez; de la misma

manera toda persona tiene derecho a la conservación, seguridad y que se *asegure* la producción probatoria anticipada en casos especiales de riesgo de desaparecer o destrucción de la prueba;

v) Finalmente toda persona tiene el derecho constitucional a que se *valoren* las pruebas ofrecidos y admitidas dentro del proceso, en consecuencia a una debida motivación los medios de prueba actuadas.

La base constitucional de las partes que interviene en el proceso judicial para obtener una tutela de derecho, es el derecho a la prueba, que consiste, en el uso de los medios probatorios más relevantes para formar certeza y convicción en el juzgador; lo que implica, que está íntimamente relacionado con el Principio de la Presunción de Inocencia, que nadie puede ser condenado tampoco sancionado, sin que se haya demostrado su culpabilidad, de la misma forma, este principio está intimidante ligado con el principio de legalidad.

En el caso específico de la prueba digital no tiene una regulación específica con la misma denominación, lo que implica, se encuentra regulado como prueba documental en el Artículo 185º del Código Procesal Penal, vale decir, la prueba digital tiene el mismo tratamiento que la prueba tradicional. Es decir, el derecho a la prueba permite garantizar que los medios probatorios ofrecidos sean válidamente admitidos, actuados y valorados en el proceso judicial, observando los principios que delimitan su contenido, he aquí salta a la vista una diferencia con la pruebas digitales, dado que éstas necesitan de una tratamiento especial, por lo que su aportación generalmente se da a través de medios como electrónicos, USB, correo, disco duro, CD, teléfono celular, Cloud Computing entre otros, y estas pruebas necesitan pasar por una pericia de informática forense para su validez procesal, de manera que garantice la integridad.

Tal como sostuvo el reconocido y catedrático Mg. Raúl Rubén Soto Aranda, en su publicación sostiene, “el derecho a la prueba forma parte del principio de presunción de inocencia y éste a su vez guarda relación con el principio de legalidad constitucional”, del cual toda tutela de derecho exige el derecho a un debido proceso legal. De manera que el derecho a exponer los medios probatorios, es el ejercicio del derecho fundamental de toda persona, a que se recepciones, se

admitan y fundamentalmente se actúen, los medios probatorios ofrecidos por las partes, éstos a su vez, sean valorados debidamente por un juez competente; tomando en cuenta el siguiente orden de prelación: primero el derecho a ofrecer determinados medios probatorios, luego a que se admitan los medios probatorios pertinentes, idóneos, útiles y lícitos, el derecho a que se actúen, y finalmente a que se valoren los medios probatorios incorporados (Talavera, 2009. p. 105).

Convenciones Probatorias.

Es posible llegar a una negociación entre las partes en el proceso que determina la constitución de una convención probatoria, aquel que tiene legitimidad procesal; vale decir, tener un interés concreto en el devenir del proceso amparado por el Derecho en el Art.350º.2 Código Procesal Penal, tipifica de manera expresa “las partes o sujetos procesales podrán exponer y proponer los hechos, sin embargo, quedara a criterio del Juez para su valoración. Lo que implica, que las partes, tienen la posibilidad de llegar a un acuerdo respecto a que medios probatorios determinantes para acreditar los hechos”.

La Presunción de Inocencia.

El derecho a la presunción de inocencia, es una garantía constitucional reconocido en el literal e), del numeral 24 del Artículo 2º de la norma suprema, que expresamente tipifica “toda persona ya sea imputada, procesado o investigado es considerada inocente mientras su responsabilidad no se haya declarado judicialmente a través de una sentencia firme”. Asimismo, el constituyente ha reconocido el principio de presunción de inocencia como un derecho fundamental, si bien es cierto no se encuentra expresamente; sin embargo, según el reconocimiento de este órgano actualmente representa un derecho fundamental.

Según la posición del Tribunal Constitucional , el derecho a la presunción de inocencia parte de un principio, incluso teniendo una relación directa con el derecho de dignidad humana tipificado en el Artículo 1º de la norma fundamental, así como en el principio pro hómine que es una categoría de los Derechos Humanos [STC 10107-2005-PHC/TC]. En esta misma perspectiva la prueba digital tiene las mismas prerrogativas que la prueba tradicional, es decir, representa la garantía

constitucional de la presunción de inocencia, que deben ser valorados por el juzgador dentro de la etapa de juicio de un proceso judicial.

En esa misma línea existe otra sentencia recaída en el Exp. N° 0618-2005-HC/TC, sostuvo que la “presunción de inocencia, iuris tantum, es una protección constitucional de los derechos de procesado, considerándole inocente mientras no se ha demostrado su responsabilidad en el marco de un proceso justo” (08/05/05, FJ.21).

También existe otro fallo del Tribunal Supremo recaída en el Exp. N°1230-2002-HC/TC, que señaló expresamente lo siguiente “el problema generado a consecuencia de lo que no se hayan actuado algunos medios o se llevó la actuación de manera incompleta, o se haya sentenciado al procesado con parte de esta prueba; no representa una violación al derecho a la debida motivación de las resoluciones judiciales, sino, representa una vulneración al derecho a la presunción de inocencia (FJ.13). La sentencia refiere, el juez, en caso no acreditar un medio probatorio convincente para imputar un delito, debe optar por absolver al imputado, puesto que, de por medio esta la ponderación de derecho a la presunción de inocencia, como un derecho constitucional.

Tratamiento de la Prueba Digital.

El marco de aseguramiento de la prueba, necesita un conjunto de procedimientos de seguridad para mantener su integridad, los cuales son: La prueba anticipada, Regulado en el título IV de la sección segunda del libro segundo, específicamente en los Artículos 242° a 246°. Que señaló que la prueba anticipada es aquella prueba practicada antes del juicio, en el caso de las pruebas digitales conforme al amparo de este Artículo, también es posible solicitar al juez, una orden para que se practique una prueba anticipada o en todo caso el juego pueda practicar de oficio, siempre que la prueba esté en riesgo de desaparecer o de ser destruido. Prueba preconstituida, este tipo de prueba se da fuera del ámbito del proceso de investigación, o cabe la posibilidad también de que se practique dentro de la fase de la investigación, se realiza previa autorización del juez competente, bajo la observancia de los límites y garantías constitucionales. Su finalidad es conservar o asegurar el contenido integral de las fuentes de prueba (Base Legal. 325, Art. 383

1. C.).

Cadena de custodia, es una técnica que permite custodiar, a su vez es un procedimiento de seguridad y conservación principalmente se da en el marco del proceso de investigación, con la finalidad de generar un valor probatorio, de manera que las evidencias entren en un proceso de control y vigilancia.

Según el especialista en criminalística sostuvo, que la Cadena de custodia es un conjunto de procedimientos orientados a brindar una seguridad, preservación y custodia para garantizar la integridad de las evidencias de manera que sean incorporadas en el proceso, bajo la observancia del principio de mismidad o autenticidad destinados a garantizar la validez procesal dentro del proceso, afín de no contaminar o adulterar los elementos probatorios (Aguirre, 2012, p.9). El autor refiere que, en caso de cadenas de custodia es la obtención conjunta de elementos de conservación y protección de las evidencias de prueba, que posteriormente permitirá la admisibilidad, luego su incorporación, y validez procesal.

En ese mismo orden de ideas, tanto la protección y vigilancia debe sobre los documentos objeto de los hechos ilícitos. La persona responsable encargado de recabar evidencias dentro de la investigación, al recolectar debe dejar constancia y el acta de lacrado y deslacrado para evitar que sea removido o adulterado, consignando anotaciones detalladas de la descripción de la evidencia. En la actualidad la sociedad está completamente virtualizado en la era digital, la misma deja evidencias de las infracciones, faltas y delitos en el ciberespacio, es decir, la interacción en la red mundial denominado Internet, redes sociales, acceso remoto, mensajes electrónicos, mensajería electrónica instantánea, entre otros; aún más extremo las acciones delictivas de ciberdelincuencia se ejecuta a través de los programas como el phishing, pharming, cybersquatting, Keylogger, email spoofing, revenge porn, dating violence, stalking, sexting, grooming, etc, precisamente por esta interacción virtual, nuestra legislación peruana ha realizado modificaciones legislativos y ha penalizado los delitos cibernético.

Las evidencias electrónicas que circulan en el ciberespacio exactamente no son auténticas o íntegras y su confiabilidad no garantiza la acreditación de un hecho, por lo que existe una vulnerabilidad en la seguridad, sobre todo por la

masificación de los hackers cuya función es acceder, destruir, modificar, alterar y robar datos de los sistemas informáticos, incluso existen ataques constantes sobre la información, quienes pueden extraer información mediante emails, PenDrive, otros., por la volatilidad de la información digital, se acude a que la prueba electrónica o digital, que deba ser corroborado con otras pruebas como la documental, testimonial de las partes y sobre todo a la prueba científica denominada pericia de informática forense.

Actuación de los Medios de Prueba.

La actuación de los medios probatorios en el Proceso Penal peruano está garantizado por la carta magna, los tratados internacionales, a su vez ratificados por el Código Penal Peruano; donde se admiten a solicitud del Ministerio Público o de los demás sujetos procesales, el juez de la investigación preparatoria decidirá la admisión o exclusión, tomando en cuenta la afectación a los derechos fundamentales (Código Procesal Penal 2004, Art. 155°).

Se entiende por actuación de la prueba, a los actos procesales urgentes y necesarios, cuyo propósito obliga el cumplimiento de los requisitos y procedimientos para su incorporación de la prueba. Asimismo, una vez admitida, los actos procesales permiten la formalidad, plazo oportuno respecto a la vía competente, en virtud del cual, el juez valorará la prueba incorporada en juicio para emitir su fallo final (Talavera, 2009, p.13). Esta fase, es el momento preciso y adecuado para que las evidencias sean incorporadas en el proceso judicial; a su vez también deben cumplir con los requisitos de no vulnerar los derechos fundamentales y bajo la observancia de los principios de publicidad, así como también principio de contradicción, de oralidad e intermediación, a través del cual el juez conoce de manera directa los hechos.

Existen tres estadios donde se deben hacer valer las reglas de exclusión probatoria, ya sea de prueba ilícita, ilegal o prueba irregular: El primer momento para invocar nulidad, oposición u otro acto que permita la exclusión de los medios de prueba, es precisamente en la audiencia de tutela de derechos, frente a un acto u omisión de los derechos a la prueba, cabe aclarar que ésta oportunidad se da en la etapa de investigación preparatoria, tal como lo consagra el Código Procesal

Penal 2004, Art. 71,4. La segunda oportunidad para invocar la exclusión probatoria es por distintas causales, y uno de ellos es la audiencia de control de acusación, donde se cuestiona la admisibilidad de las pruebas, su pertinencia, idoneidad, conducencia, utilidad y licitud; estos actos corresponden a la segunda etapa, es decir, la etapa intermedia (Código Procesal Penal 2004, Art. 352,5).

Como tercer y último actuación es la valoración de la prueba ofrecida, pero previamente debe ser admitida, luego incorporada al juicio oral en la etapa de juzgamiento, la esencia en esta oportunidad es la actuación probatoria, a través de un debate del principio contradictorio y oralización de los informes periciales, al finalizar el juez valorará las evidencias y las mismas que serán convertidas en prueba producto del debate contradictorio. Es decir, la actuación de los medios de prueba se da en esta fase, bajo la observancia del respecto de los derechos fundamentales y principios procesales los cuales permiten valorar y producir la prueba (NCP 2004, Art. 393°.1). De esta forma la actuación probatoria se lleva a cabo en orden de prelación dentro de la fase del juicio oral, en el siguiente orden; primero se inicia con el examen del acusado, es decir, con el interrogatorio del o de los imputados, enseguida se da la actuación de las evidencias de las pruebas admitidas, que consiste en la incorporación a juicio, pero bajo los requisitos de idoneidad, pertinencia y utilidad, y por último la valoración de las pruebas por el juez competente. Lo que implica que el juez al valorar comprueba los hechos, lo que da lugar a la conversión de evidencia en prueba (NCP. Art. 375).

Examen del acusado, luego de haber culminado la intervención oral de las partes a través de los alegatos preliminares, seguidamente el juzgador dará la oportunidad al interrogatorio del acusado; previamente se le informará el respecto de sus derechos, asimismo, se le dará indicaciones de los derechos a guardar silencio, y no estar obligada a declarar, el cual no será usado en su contra.

Examen o interrogatorio directo de testigos, un testigo es la persona que ha presenciado y percibido de manera directa a través de sus sentidos un acto u hecho ilícito con relevancia penal. Vale decir, que se percibe las circunstancias de un suceso el cual es revelado y descrito por el testigo. Cabe señalar, que es el primer examen que se le practica al declarante propuesto por la parte.

Este tipo de interrogatorio también es conocido como el interrogatorio directo tipificado en el Art. 375^o.3; en el caso de las evidencias digitales, puede ser testigo cualquier persona quién haya presenciado de manera directa o indirecta hechos delictivos, pero en este caso se trata del contexto virtual, de manera que se corrobore los hechos delictivos cometidos por el agresor. Contraexamen o conainterrogatorio de testigos, en esta fase se interroga al testigo propuesto por la parte adversaria, es interrogar con preguntas cerradas al testigo por la parte adversa. Lo que implica interrogar con preguntas cerradas a quién ofreció el testimonio. Asimismo, el Código Procesal Penal, otorga potestad a las partes para solicitar al juez la autorización, respecto a la fecha y hora a practicarse un nuevo interrogatorio, ya sea de testigos, o peritos especializados, tal como lo tipifica el Art. 378^o,10.

Examen especial de testigos, el Nuevo Sistema Garantista Adversarial reconoce de manera excepcional las formas de actuación probatoria; como en circunstancias ajenas a los hechos, ya sea de carácter temporal, por factor de distancia de la residencia, temor de algún riesgo inminente que da por hecho. El examen se inicia corriendo traslado al testigo de lo actuado para que conteste, siempre anteponiendo el respeto a las leyes, la Constitución y los Tratados Internacionales. En este caso tratándose de prueba testimonial, también participan los peritos informáticos, quienes están obligados a conferenciar ante el juez, para exponer los procedimientos tecnológicos confiables que garantizan la autenticidad y la integridad de las evidencias digitales; obtenidas de las redes sociales, de la web, de email, o de cualquier dispositivo electrónico.

Cabe resaltar que es indispensable que pase por un examen de pericia de informática forense, de modo que pueda ser valorado por el Juez. De caso contrario será una ventaja de impugnación para el abogado de la defensa; es decir, todo medio de prueba, está sujeto al principio contradictorio para evitar la vulneración de los derechos fundamentales, vale decir, que toda evidencia digital para su incorporación en el proceso debe haber sido obtenido de manera lícita bajo el respeto de los principios constitucionales, de caso contrario será sensible de la exclusión probatoria, tal como lo establece el Art. 378^o, 4.

Examen de peritos, consiste en conferenciar en juicio de parte de los expertos, con el fin de exponer las características y detalles de autenticidad de las pruebas para su valoración, cabe advertir, en esta fase de exposición de los informes periciales, sólo se valorarán cuando haya sido sometido al principio contradictorio, el cual consiste en un debate de las pericias, de modo que el juez pueda conocer, corroborar, contrastar y valorar para convertirlos en prueba. En el caso de la prueba digital los expertos como los peritos informáticos deben conferenciar en el juicio el contenido de sus informes y estar sujeto a los interrogatorios de manera que el juez pueda valorar la evidencia; de caso contrario la prueba carecerá de eficacia probatoria puesto que se pondría en duda la autenticidad e integridad de la información. Además, es indispensable el examen de informática forense de la evidencia, dado que la información en los medios electrónicos o virtuales son volátiles a ser modificados o transformados y la única forma de garantizar su autenticidad es a través de un estudio de los expertos (Art. 382º.2. NCPP).

La actuación de otros medios de prueba. - Si después de las diligencias de la investigación preparatoria resultase que nos hay suficientes elementos de convicción para continuar con la investigación, el juez penal competente de oficio o en todo caso a petición de las partes, previo debate del principio contradictorio puede ordenar nuevas diligencias tantas inspecciones, reconstrucción de los hechos u otros actos procesales para generar convicción y certeza. En este caso las partes al momento de ofrecer las pruebas digitales deben aportar el dispositivo original que contiene la información, ya sea el celular, teléfono móvil, disco duro, USB, etc. De modo que se garantice su integridad y se debe obtener un Backup para el peritaje de autenticidad. (N CPP. Art. 385º.1)

En cuanto a la lectura y presentación de la prueba documental el código señaló, que solo se podrán utilizar en juicio para efectos de deliberación única y exclusivamente las pruebas que no sean ilícitas, o irregulares que cumplan con los requisitos y legítimamente incorporadas en el proceso. Vale decir, que el juez no tomará en cuenta las pruebas que se ofrece posterior a la etapa de ofrecimiento de la denuncia o contestación de aquella, salvo excepciones, finalmente, la prueba sobre la prueba, consiste en la actuación de nuevos medios probatorios autorizados

por el juzgador luego de haber culminado la recepción de las evidencias; solo de manera excepcional el juez en casos de que en el debate sobre la incorporación de las pruebas resultasen indispensables, útiles, pertinentes, e idóneo para impartir justicia y resolver el conflicto de intereses (NCPP. Art. 385.2 y 393)

Legitimidad de la Prueba

La doctrina extranjera aborda el tema de legitimidad de la prueba en sus diferentes concepciones, tal es así, que el especialista Echandia (2002), sostuvo que “la legitimidad de la prueba tiene una vinculación directa con el derecho constitucional a la presunción de inocencia, que además exige que las pruebas hayan sido obtenidas bajo la observancia de los requisitos de validez, licitud y respeto de los derechos fundamentales” (pp. 117-118). La postura del autor refiere, que la prueba es legítima, siempre en cuando su obtención haya sido de manera legítima y lícita, sin la afectación de los Derechos Constitucionales de las personas.

Del mismo modo Silva (1963), sostuvo que “la legalidad, licitud o legitimidad de la evidencia para su validez y eficacia procesal, exige que su obtención no haya afectado los principios y garantías constitucionales, asimismo su ofrecimiento e incorporación este bajo el estricto respeto a los procedimientos y plazos; de lo contrario será susceptible de exclusión probatoria, calificados como evidencias provenientes de fuentes impuras o ilícitas” (pp. 29-30). También el autor comparte la misma postura en el sentido de que las pruebas deben obtenerse por las vías lícitas, se entiende, sin afectar los Derechos Fundamentales consagrados el ordenamiento jurídico.

Asimismo, en nuestra legislación nacional, el Tribunal Constitucional peruano se pronunció en su fundamentación “la actuación probatoria representa un derecho constitucional que consiste en el respeto de los derechos fundamentales y al ordenamiento jurídico, de modo que, en la obtención, recepción, incorporación, y valoración se debe tomar en cuenta no transgredir este precepto constitucional”. Este colegiado refiere, para que la prueba sea legítima debe cumplir dos aspectos esenciales, primero la obtención de la prueba debe adquirirse bajo el respecto de los presupuestos constitucionales, vale decir, con el respeto estricto de los derechos fundamentales, y como segundo aspecto que su obtención no

transgredan el ordenamiento jurídico, es decir, con respeto a las normas y leyes establecidas; sólo cumpliendo estos dos requisitos la prueba será legítima (STC. N° 1014-2007-PHC/TC, f.15).

La Academia Nacional de la Magistratura en su publicación respecto a la prueba consignada en el Nuevo Código Procesal Penal, tipifica, “las prohibiciones probatorias están referida estrictamente a la legitimidad probatoria, asimismo advierte que la prueba irregular o defectuosa no es más que la prueba ilícita”. En la misma postura también se pronuncia la doctrina, al señalar que los inconvenientes de validez de la evidencia digital radican en la volatilidad, lo que implica, que es sensible a la manipulación y/o alteración, es decir, las evidencias digitales no gozaran de valoración en los procesos judiciales, si han sido obtenidos de manera ilícita, así como también, por falta de autenticidad e integridad. Las partes que lo invocan deberán probar su autenticidad con un informe de un peritaje de informática forense; en los casos de alteración o fotomontaje digital, las partes del proceso pueden presentar una oposición, así como el Ministerio Público y el Juez puede solicitar un examen por un especialista en pericia informática.

Implementación Tecnológica.

En la sociedad moderna y la era digital en la que nos encontramos, la comunicación virtual, y remota se ha convertido en un instrumento crucial para interactuar con las personas y cada vez más las personas interactúan a través de Internet, redes sociales, páginas web, etc., lo que implica, que las personas dejen evidencia digital en las redes de sus actos o conductas. Dichas evidencias están representados por fotos, mensajes de texto, mensajes de voz, vídeos, audios, email. Los cuales pueden representar la comisión de un delito tales como: mensajes de amenazas, chantajes, robo de cuentas, estafas, injurias, calumnias, entre otros. Cada vez más hay personas agraviadas por un delito en la red y a la vez cada año va en aumento personas que acuden al Ministerio Público para interponer una denuncia, portando como medio de prueba en algún dispositivo electrónico cuyo contenido es una evidencia digital como prueba del delito. He aquí surge distintas interrogantes, tales como; ¿El Ministerio Público cuenta con la implementación suficiente para dar

tratamiento a las evidencias digitales? ¿Qué procedimientos sigue el Ministerio Público para garantizar la autenticidad de la prueba?

En la visita realizada al Ministerio Público de Ventanilla, se observó que falta una implementación tecnológica para brindar un tratamiento apropiado a las pruebas digitales, de modo que el Ministerio Público como ente persecutor del delito cuente con los instrumentos tecnológicos para brindar seguridad y garantizar la autenticidad e integridad de las pruebas digitales, que garantice una eficacia procesal y valoración probatoria, en la visita se observó ambientes reducidos, casi no hay espacio donde sentarse para los visitantes, cada fiscal cuenta con un escritorio, una computadora, una impresora y dos sillas, además hay ambientes de 3x3 metros cuadrados (9m²) donde atienden 4 fiscales. En cuanto a la sala de visualización de pruebas digitales no existe, no cuentan con equipos tecnológicos adecuados; por la insuficiencia de la implementación se ven obligados a dar el tratamiento de la prueba digital (transcripción en soporte de papel) en la computadora de su oficina que muchas veces carecen de audio o parlante (Anexo N°15 acta de transcripción de video). En los últimos 5 años el índice de cibercriminalidad ha aumentado de manera alarmante tal como muestra el informe estadístico de la División de Investigaciones de Delitos de Alta Tecnología (DIVINDAT) quiénes son los nuevos policías del ciberespacio cuya función es patrullar el ciberespacio (ver anexo 6).

Sala de Visualización.

Una sala de visualización es un ambiente adecuado dotada de una implementación tecnológica con equipos de tecnología de punta, ya sea, como monitor TV, con entrada para USB, con Lectora de CD, DVD, Blu Ray, además con grabador de sonido y parlantes, con impresora láser, con un sistema apropiado (aplicación Hash) que permita dar un tratamiento a las evidencias digitales.

Cuando las partes agraviadas ofrecen evidencias digitales al Ministerio Público, debe garantizar el derecho a ofrecer prueba, para lo cual el persecutor del delito necesita una implementación adecuada para garantizar la autenticidad y posterior valoración probatoria. Vale decir, las partes ofrecerán como prueba del delito, información cuyo contenido se encuentran en dispositivos

electromagnéticos, representados en fotos, videos, sonidos de voz, audio, emails, etc. El objetivo es determinar cuáles son los protocolos e instrumentos que permitirá que las pruebas digitales no sufran ninguna volatilidad. Para lo cual, el Ministerio Público debe contar con periféricos Hardware y una sala de visualización de evidencias digitales, tales como: Computadora, pantalla monitor, Parlantes, y Software autorizado para obtener un backup de la información para derivarlo a la División de Investigaciones de Delitos de Alta Tecnología (DIVINDAT) quienes dentro de su estructura orgánica de la DIRINCRI – PNP son los agentes encargados vigilar el ciberespacio (cloud computing). Tal como señalaba el reconocido Juez Quiroz (2018), el Ministerio Público debe estar en la capacidad de la guarda, custodia e incluso de tener con un laboratorio implementado para practicar las pericias informáticas en las mismas sedes y no estar sujeto una centralización de la División de Alta tecnología, además agrego y si no lo implementan, será responsabilidad de las autoridades.

Pericia Informática.

La doctrina define a la Informática Forense como una disciplina criminalística que sigue una secuencia de procedimientos, con el objeto de investigar los sistemas informáticos de datos de hechos delictivos con relevancia jurídica, cuya finalidad es determinar la autenticidad o veracidad de un hecho. La secuencia de procedimiento para identificar la autenticidad de las pruebas digitales, son identificar, preservar, analizar y presentar un informe, de modo que brinde la fiabilidad de la autenticidad de la prueba digital; cabe señalar en este procedimiento la aplicación de los valores Hash, se lleva a cabo en un laboratorio especial denominado Workflow, tiene una relevancia jurídica, dado que permite generar un código de valor de autenticidad. (Sebastián, 2009, p.3) (Ver anexo 7 y 8).

El reconocido perito informático y director de Aldama Informática Legal, sostuvo que las pericias informáticas consisten en la búsqueda y extracción de los datos almacenados en dispositivos informáticos, los cuales pueden ser computadoras, tablets, laptops, teléfonos móviles, discos duros, USB, Cámaras digitales, Pendrive, entre otros. Los procedimientos se practicarán con herramientas de análisis forense, para asegurar la completa extracción de datos y

garantizar la cadena de custodia. La aplicación de esta pericia tiene como objetivo determinar el autor de un documento, analizar la actividad en un dispositivo, recuperar datos eliminados, y certificar los emails, conversaciones a través de WhatsApp, Facebook, y toda información publicada en Internet. Asimismo, los dispositivos que contienen la información digital que son materia de análisis son: Discos externos, pendrive, Tablet, USB, cámaras digitales, teléfono móvil, pagina web, redes sociales (whatsApp, Facebook, instagram, etc.) y los servidores de correo y otras (Aldama, 2017. Pub).

Regulación de Delitos Informáticos.

Existe un conjunto de normas que regulan los delitos informáticos, los cuales permiten sancionar los actos delictivos que se cometen a través de Internet y redes sociales, lo cuales son: la reciente Ley 27309 que ha permitido flexibilizar el Código penal incorporando modificatorias respecto a los delitos informáticos (Promulgada el 15 de Julio del año 2000), también la realidad tecnológica ha permitido promulgar la Ley N° 27269 Ley de Firmas y Certificados Digitales, mediante el cual se le da valor a los todos los documentos electrónicos, de modo que los Notarios encargados de dar fe pública, así como las Instituciones Estatales están facultadas en dar fe, y certificar los documentos electrónicos.

En ese mismo orden de ideas, existe actualmente la Ley N° 27459 Ley Contra la Pornografía Infantil, para sancionar los delitos que comenten las personas contra los menores de edad a través de las redes. De la misma forma también se ha publicado la Ley N° 28119 Ley de protección al menor que regula las prohibiciones de los menores de edad que Prohíbe el Acceso a Páginas Web, a través de Internet de Contenido Pornográfico. También la regulación del envío y recepción de los mensajes de correo electrónico, la Ley N° 28493 permite sancionar a los envíos de mensajes desconocidos sin autorización, del quién recibe, este envío con el uso del correo electrónico no solicitado (SPAM), y por último la Ley N° 26612 que permite regular el uso adecuado de las tecnologías avanzadas concerniente a los archivos de documentos e información, y las responsabilidad que pueda generar los Procedimientos Legales - Los Delitos contra el honor (difamación, calumnia e injuria), Ley N° 29733, Ley de protección de datos

personales y DS. N° 003-2013-JUS, Reglamentó de la Ley de protección de datos. Los delitos más comunes cometidos por los usuarios en la red son: amenaza por email, hurto por tarjeta, chantaje sexual, acceso de datos no autorizados, etc. (como se muestra en el anexo 5)

Incorporación de la Prueba en Juicio.

La obtención de las pruebas digitales se regula bajo la observancia de los principios constitucionales y con el estricto respeto de los Derechos fundamentales, como el Derecho a la inviolabilidad de domicilio, a la intimidad personal, secreto de las comunicaciones y secreto financiero. Salvo las excepciones previstas en la norma penal; asimismo existen prohibiciones sobre la obtención de la prueba en el Código Procesal Penal (Art. 155°, 165°).

La norma penal actual refiere, que las evidencias se admiten a solicitud del Fiscal titular de la acción penal o de los otros sujetos procesales, es decir, las evidencias se ofrecen cumpliendo los requisitos de Ley, lo que implica, sin afectar los derechos y principios tutelados, de modo que el Juez admita las pruebas a través de un auto debidamente motivado; él tendrá la facultad de excluir las pruebas ilícitas o prohibidas que afecten los derechos constitucionales (Art. 155,2 NCPP).

Asimismo, dentro del proceso de investigación intraproceso y extraproceso existe la prohibición de determinadas evidencias, las que están impedidas de la actuación probatoria, en los siguientes casos: primero, el código advierte que no procede un debate o enfrentamiento entre el careo de la persona imputado y la agraviada víctima menor de catorce años de edad, quién haya sufrido los agravios del sujeto activo (Art. 182°).

En ese sentido el mismo código también advierte de manera categórica, que no pueden ser usados las pruebas obtenidas, aun con el consentimiento de la parte interesada, quién haya usado de manera directa métodos, estrategias, o técnicas idóneas para cambiar e influir respecto a su derecho fundamental a la libertad de autodeterminación, o también haya alterado, modificado, cambiado la capacidad de recordar o valorar los hechos sucedidos, serán excluidos y exentos de valoración (Art. 157,3). En el caso de prueba digital o electrónica, los contratos suscritos con

firma electrónica conservados en un dispositivo magnético, disco compacto (CD), disco video digital (DVD), dispositivo portátil de almacenamiento (Pen Drive), disco duro (Hard Disk), correo electrónico (mail), mensajes (SMS), etc., deben obtenidos bajo los requisitos que exige la Ley, sin afectar los Derechos Fundamentales, su omisión será materia de exclusión como prueba ilícita.

En consecuencia, debido a la naturaleza virtual de la prueba digital es indispensable su documentación y se haga a través de dispositivos de almacenamiento de la información que acreditan su existencia y su origen de los hechos. Sin embargo, para que la evidencia digital pueda ser admitida en el proceso judicial debe cumplir con tres requisitos indispensables:

La Licitud. - En el caso de la obtención de la evidencia digital, tiene que estar bajo el marco del respeto de los límites de los principios constitucionales y derecho fundamentales, es decir el derecho al secreto de las comunicaciones, a la intimidad personal, a la inviolabilidad de domicilio, a los secretos financiero entre otros. En caso de vulneración de uno de los derechos, será considerada como una prueba ilícita, es decir inconstitucional, por lo tanto, su exclusión será inmediata de todo proceso judicial.

Integridad. - Debido a la volatilidad de la evidencia digital garantizar la inmutabilidad del soporte digital, es importante que la evidencia electrónica sea sometida a la una pericia de informática forense, de manera que un profesional especializado emita un informe respecto a la integridad de la evidencia digital para su valoración en el proceso judicial.

Autenticidad. - Consiste en garantizar que la muestra o evidencia sobre la que se hace la investigación sea idéntica a la muestra original, lo cual se conserva y se custodia a través de la Cadena de Custodia, garantizando que la evidencia digital no haya sufrido ninguna modificación, manipulada o alteración en su obtención, transferencia y/o almacenamiento. Este es el primer estadio de acceso a las fuentes de la evidencia electrónica o digital; vale decir, la obtención de la evidencia digital por las partes del proceso o por parte de la autoridad judicial en el proceso penal, refiere al momento previo a la aportación de la evidencia digital al proceso; es decir al acceso a la información de hechos almacenados en un

dispositivo electrónico, o en todo caso transmitidos a través de mensajería electrónica, ya sea por redes, vía Internet, pagina web, redes sociales, WhatsApp, CludComputing, disco duro, USB (Universal serial Bus), CD (Disco Compacto), DVD (Disco Video Digital), pendrive, u otro. Es decir, es la corroboración de las evidencias que existieron en las fuentes de prueba.

Acceso a Datos Digitales.

En esta fase para el acceso al contenido del sistema o equipo hardware, se debe contar con la posesión física del material, es decir que el persecutor del delito o el Ministerio Publico debe recibir el dispositivo electrónico que contiene la información producto del delito. Teniendo el dispositivo y el contenido de la información se puede garantizar la integridad de la evidencia digital.

Los datos obtenidos por una de las partes o del accionante esta enmarcados en dos posibilidades: primero, los datos o la evidencia digital se encuentren contenidos en el mismo dispositivo electrónico de la parte interesada (imputada). En este caso, la dificultad radica en la forma de incorporación de la evidencia al proceso judicial, sobre todo la acreditación de la autenticidad y la integridad de la prueba son las dificultades más resaltantes, dado que la agraviada no cuenta con este medio de prueba. Como segundo punto, la evidencia digital que se encuentran contenidos en un dispositivo electrónico de un tercero, en este caso la información o evidencia pueden ser aportados a través de una orden del mismo juez, y en un tercer caso el acceso a la información puede haber sido obtenido con infracción de derechos constitucionales, de ser así sería inconstitucional, por vulnerar los límites y principios constitucionales, que da origen a una exclusión de una prueba ilícita.

Según Velasco (2014), sostuvo que en el Proceso Penal existe un conjunto de formas de acceder u obtener la información de evidencia digital que se encuentran contenidos en dispositivos, en sistema electrónicos, y los procedimientos más recomendables son: primero, la aprehensión o posesión del propio objeto material fuera del lugar cerrado; como segundo procedimiento se encuentra la diligencia de acceso al registro de información del propio dispositivo electrónico; como tercer posibilidad, también existe la posibilidad de procedimiento y técnica de acceder al contenido original de un sistema informático vía virtual o

remoto, sin que exista la necesidad de contar con el mismo material en físico; asimismo existe posibilidad de acceder a los datos contenida en un servidor de red; finalmente existe la posibilidad de acceso a la información exfronterizo, es decir, suele ocurrir cuando la información o evidencia se encuentran almacenados en un dispositivo o servidor de red internacional, intercontinental o mundial. Aquí podemos poner como ejemplo el caso de la captura del Caso Orellana, que fue capturado con un hackeo de la cámara de seguridad de la habitación en que vivía en Colombia, gracias a este acceso de información extrafronterizo se logró ubicar. Sin embargo esta prueba digital (film-video) fue autorizado por el Juez, en consecuencia no se configura la ilicitud al margen que se allano su domicilio con esta diligencia.

Los Derechos fundamentales constitucionalmente reconocidos son vulnerados en la obtención de la prueba digital, en este caso normalmente son afectados los derechos a la no vulneración de la intimidad personal o familiar, derecho a la no vulneración del secreto de comunicaciones, derecho la no inviolabilidad de domicilio, derecho al secreto financiera, etc. Normalmente las obtenciones ilícitas de la evidencia digital son a través de videos, audios, mensajes, fotos, etc.

Fase de Ofrecimiento Probatorio.

La oportunidad de ofrecimiento de las evidencias de prueba se da al momento de invocar la tutela jurisdiccional, es decir, al interponer la denuncia, ya sea a la policía o fiscalía y también al momento de contestar o contradecir la denuncia.

Cabe señalar, que los medios probatorios que no se ofreció al momento de presentar la denuncia fiscal no se puede discutir y menos valor en el juicio. Sin embargo, es posible ofrecer medios probatorios en la etapa intermedia, siempre que se trate de una prueba nueva. Una vez culminada la etapa de investigación preparatoria y en el inicio de la etapa intermedia, el Ministerio Publico a través del fiscal podrá realizar su acusación del delito adjuntando los elementos de convicción que haya aportado las partes y las obtenidas en la investigación.

Fase de Admisión Probatoria.

Como se ha abordado el tema de la prueba, existen distintas formas de incorporar la evidencia digital tipificado en el Código Procesal Penal, uno como prueba documental, precisamente en su incorporación se discute en la etapa intermedia, de manera que el juez conozca controle y admita las pruebas ofrecidas teniendo en cuenta los criterios de pertinencia, conducencia y utilidad; asimismo que las evidencias hayan sido obtenidas con el estricto respecto de los derechos fundamentales. El código señaló que es posible incorporar en el proceso cualquier documento que permita acreditar como medio de prueba los hechos producto del delito, asimismo el Ministerio Público en la fase de investigación preparatoria está en la posibilidad de ordenar diligencias directamente a las partes quienes cuentan con el documento, afín de que se presente, exhiba voluntariamente, de ser negativa la voluntad de exhibir los documentos solicitará al Juez penal de investigación preparatoria la autorización para la incautación correspondiente. (Art. 184º NCPP).

Fase de Actuación Probatoria.

La actuación probatoria de las evidencias digitales admitidas, se practica en la fase del juicio oral, el cual tiene una secuencia lógica, de modo que el Juez pueda conocer de manera directa el caudal de información recopilada en la etapa de investigación preparatoria. Además, en esta fase cabe la posibilidad de presentar excepcionalmente nuevos medios probatorios ocurridos con posterioridad a la acusación fiscal, del mismo modo se puede solicitar una nueva evaluación o reexamen de las evidencias no admitidas en la etapa intermedia, fundamentando la necesidad, pertinencia y utilidad de los elementos.

Fase de Valoración Probatoria.

La valoración de las evidencias para convertirlo en prueba, se lleva a cabo en la etapa del juicio oral, en el cual las partes oralizan las pruebas, de manera que el juez conoce directamente a través de ellas; que finalmente a través del principio discrecional y el criterio de las reglas de la sana crítica, y de las máximas de la experiencia, el juez convierte en prueba las evidencias incorporadas. Asimismo, la actuación de las pruebas se lleva a cabo a través del principio de inmediación de

manera que el juez conoce y percibe los hechos de manera directa, el cual le permitirá generar convicción respecto de la realización de los hechos; dichas pruebas obligatoriamente para ser valorados y tener fundamentos de sentencia deben ser sometidos al debate a través del principio contradictorio. En los párrafos anteriores se había advertido que el Código Procesal Penal ha establecido una serie de secuencias u orden en las que se debe llevar a cabo la actuación probatoria: en primer lugar, se iniciara con el interrogatorio o examen al acusado, en seguida se actuaran las pruebas debidamente admitidas, luego será oralizados en juicio frente al juez. En caso de existir una pluralidad de acusados el orden en que se le examinará es determinado a criterio del juez. Es más, si en caso existiese vacíos o por practicar otros órganos de prueba lo determina el juzgador (Art. 375º NCPP).

Admisión de Prueba.

La admisión de la prueba está íntimamente ligado al principio de aportación de parte, no solamente de quién lo ofrece, sino también, la prueba de oficio que dispone el juez; es decir, se admiten a petición de los sujetos procesales o del fiscal quién representa al Ministerio Público. Cabe advertir, también existe una excepcionalidad, luego de la admisibilidad es posible que se admitan nuevos medios probatorios practicados de oficio autorizados por el Juez (Art. 385º, 2. NPP).

Siguiendo la línea de tiempo, en el caso de las pruebas digitales es importante la práctica de examen de interrogatorio al acusado; decir que se comenzará interrogando, con la finalidad, si acepta ser autor de la publicación ya sea a través de WhatsApp, Facebook, Chat, email, mensajes, etc. Evidencia ofrecida del envío o recepción de grabaciones, audios, sonido de voz, fotos, imágenes constitutivas de la comisión de un delito, el cual otorgará valor probatorio de acuerdo a los principios constitucionales, de modo que no se haya afectado el derecho fundamental de las personas y tampoco debe subsumir ningunas de las prohibiciones, para la valoración y eficacia procesal.

La Oportunidad para Presentar Pruebas.

La oportunidad para ofrecer pruebas testimoniales, ya sea de parte del Ministerio

Publico representado por el fiscal, por la defensa técnica y demás partes procesales es precisamente en la fase intermedia, en esta fase de ofrecimiento se presentarán las pruebas testimoniales tales como: testigos y peritos, luego se ofrecerá las pruebas documentales, que consiste de un conjunto de documentos, informes, videos, audios, etc. La incorporación de la prueba digital debe cumplir los mismos requisitos, ser conducente, pertinente y útil, de modo que pueda incorporarse, enseguida ampliaremos los conceptos de los requisitos:

Conducencia.- Se refiere a la idoneidad legal que representa la prueba, de manera que permita demostrar un determinado hecho factico. Por ejemplo, es posible acreditar la compra venta de un inmueble con un contrato de compra venta privado; asimismo es posible cuestionar que tal documento no representa la idoneidad, puesto que el código civil tipifica que la transferencia debe ser a través de una escritura pública. Se caracteriza por ser un medio probatorio idóneo para demostrar un hecho, y que su obtención haya sido legítimamente con respeto de los derechos fundamentales. De manera que permita un eficaz resultado generando convencimiento en el juez más allá de toda duda razonable. **Pertinencia.-** permite demostrar o corroborar el hecho con la prueba de manera que la prueba este en estrecha relación con el hecho investigado. **Utilidad.-** Consiste que es posible establecer de manera concreta un hecho materia de conflicto, y que aún está pendiente de demostrar. Es decir, una prueba es útil siempre en cuando sea idónea, que sea útil, y que permita demostrar el hecho ocurrido; no todas las pruebas son útiles, por ello es importante seleccionar solo lo que es útil, que permita corroborar el hecho. Las partes del proceso, así como el representante del Ministerio Público están en la facultad de solicitar autorización al juez penal competente sobre la exclusión, ilicitud, rechazo, impugnación o inadmisibilidad de los medios probatorio ofrecidos, que, según el procedimiento, límites y reglas legales, resulten ilícitos, ilegales, inadmisibles, inidóneo, impertinentes, inútiles.

La Teoría del Riesgo.

Puede valorarse la prueba prohibida, cuando es el propio imputado quién no cuida sus propias garantías constitucionales (verbigracia se expone a ser filmado en público). Las pruebas obtenidas de manera directa o indirecta con vulneración a las

garantías y derechos fundamentales de la persona carecen de efecto legal; vale decir que existe requisitos de validez para la obtención de los medios de prueba, establecido como principios de rango constitucional, los cuales permiten garantizar el derecho a presentar medios de prueba sin vulneración de derechos; de darse tal afectación, se considera prueba ilícita, el cual, no podrá ser usado ni directa o indirectamente en la valoración de un proceso (Art. 159 NCPP).

En todo proceso judicial existe un conjunto de formas de incorporar al proceso la prueba digital, Delgado Martín sostuvo que existe una diversidad de medios y elementos tecnológicos determinan la forma de acceder al contenido de los dispositivos o medios; lo que implica, que la naturaleza jurídica de la prueba digital es incorporar al proceso. Ésta puede ser, a través de la prueba documental, prueba personal o prueba técnica y precisamente la prueba digital se enmarca dentro de la prueba documental que refiere a documentos manuscritos, impresiones, fotocopias, fax, disquetes, películas, fotografías, radiografías, representaciones gráficas, dibujos, grabaciones magnetofónicas y medios que contienen registro de sucesos, imágenes, voces, y otros similares. En cuanto a las otras pruebas electrónicas tales como mensajes de correo electrónico, páginas web, mensajes de Facebook, cloud computing, entre otros, el código no especifica de manera clara el manejo y tratamiento; por lo que debemos entender, que se encuentra en otros similares del mismo Artículo Art. 185º, Código Procesal Penal.

Es así que se puede incorporar una gama de medios electrónicos, siempre en cuando en su obtención se haya respetado los principios y derechos fundamentales, además que después de su admisión cumpla con el respeto de los principios de unidad, comunidad, contradicción, ineficacia, intermediación, oportunidad y oralidad de la prueba en el juicio.

Es usual encontrar prácticas profesionales con transcripciones de mensajes enviados fotos, audio, video, otros ya sea por email, Facebook, messenger, youtube, whatsapp, cloudComputer, onedrive, entre otros. Sin embargo, este tipo de aportes no tienen eficacia, dado que se omiten datos relevantes, tales como la autoría, el origen y la autenticidad e integridad de los datos obtenidos, ya sea de un teléfono móvil, Tablet, etc, el cual pase por una pericia de informática forense. Existen un

conjunto de medios utilizados en la práctica profesional, para el caso específico de las pruebas digitales se deben analizar:

Impresión privada del mensaje en un documento.- este caso consiste en la impresión en físico en un soporte de papel la información almacenada en un dispositivo electrónico (teléfono móvil, Tablet, USB (Universal serial Bus), CD (Disco Compacto), DVD (Disco Video Digital), whatsapp, otros); sin embargo, su eficacia jurídica se ve disminuida en caso de ser impugnada, porque muchas veces se obvia la autoría de la información y además por la volatilidad de la información.

Aportación de capturas de pantalla. - consisten en aportar mensajes de las conversaciones como prueba del proceso penal. Sin embargo, existe un principio de presunción de inocencia que protege los derechos del procesado, el cual desvirtúa y destruyen las auténticas pruebas digitales, por falta de un tratamiento adecuado, sobre todo cuando no ha sido examinado por un perito informático.

Acta del letrado de la administración de justicia. - consisten en la intervención de un letrado de la administración pública que otorga fe pública, quién levanta un acta de la transcripción de los mensajes recibidos o da fe pública que la prueba digital existe en los dispositivos electrónicos; sin embargo, tampoco esta técnica garantiza la eficacia de la validez de la prueba digital, dado que la fe pública no certifica la autoría de las pruebas y menos la autenticidad.

Acta de protocolización notarial.- similar al caso anterior este tipo de técnica tampoco ofrece una eficacia para una valoración en el proceso, pues el notario en su calidad de fedatario verifica y corrobora que los datos digitales adquiridos a través de un backup o transcritos se asemejan al original de los dispositivos electrónicos. Tampoco garantiza la autenticidad de la volatilidad.

Prueba testifical.- este tipo de prueba consiste en acreditar la autenticidad de la prueba digital a través del reconocimiento del imputado o agraviado expreso del envío o recepción de los mensajes o datos digitales aportados en el proceso. En este caso, la dificultad para demostrar la autenticidad se presenta cuando el imputado se acoge al derecho a la guardar silencio o a la abstención a la declarar. Pero si el autor reconoce en envío o recepción de los datos digitales o mensajes

electrónicos, se corrobora con la información e identifica al autor, por lo que en este caso si la prueba digital seria autentico.

Pericia de informática forense.- es una técnica que consiste en obtener un backup del dispositivo o medio electrónico con la finalidad de practicar un examen y determinar su autenticidad y conocer si se produjo alguna manipulación o alteración de los datos o medios digitales. En este caso el perito que es un profesional experto que emite un informe que acredite la autenticidad e integridad de los datos almacenados en los dispositivos.

Reconocimiento judicial.- Esta técnica consiste en que el Juez practicara un examen directo del dispositivo electrónico, en el cual se encuentra la información, ya sea en dispositivo móvil, Tablet, USB (Universal serial Buss), CD (Disco Compacto), DVD (Disco Video Digital), otros. Asimismo, también es necesaria e indispensable la práctica de un examen de pericia informática para corroborar la autenticidad e integridad de la prueba digital aportado en el proceso.

Aportación de medio audiovisual (*fotos, imágenes, audio, video, u otro*). - la prueba electrónica o digital es un instrumento que está constituido por dos componentes de imagen con movimiento y sonido, se puede incorporar al proceso mediante dispositivos electromagnéticos almacenados, presentando copia de la prueba de los hechos ilícitos en un DVD, CD, USB, disco externo, teléfono móvil, u otro, acompañado de una transcripción o impresión en soporte de papel. En este caso la eficacia también está sujeto a una pericia de informática forense para demostrar y corroborar su autenticidad e integridad de las pruebas aportadas al proceso.

Huella digital.- En el mercado tecnológico existen diversos medios para certificar la autenticidad e integridad de los medios digitales. Uno de los más conocidos y estudiados es la criptográficas *hash*, la función más importante de este dispositivo es hacer una copia espejo de los dispositivos electrónicos, tales como Disco duro, USB, CD, DVD, memoria del teléfono móvil, memoria del Tablet, etc. No obstante, es insuficiente para una eficacia, por lo que es recomendable recurrir al notario para protocolizarlo del original, previo verificación y corroboración de la copia espejo y el dispositivo en el que se encuentra almacenado.

Valoración de la Prueba Digital.

Los requisitos para la valoración procesal de las evidencias digitales son los siguientes: en la admisibilidad debe emplearse una metodología adecuada, que la autenticidad debe ser copia espejo del original bit a bit y firmas de seguridad, la diligencia debe realizarse en el ámbito del escenario del delito. La actuación fiable de un profesional experto en el uso de procedimientos, técnicas y herramientas legales para una pericia en informática, debe ser clara y precisa, en los procedimientos de extracción, clonación, grabación, y aseguramiento con cadena de custodia, y finalmente el análisis y conclusiones periciales debe ser entendible para el destinatario y para el juez, auténtica, íntegra, credibilidad y experiencia comprobada.

En el proceso judicial, para ser más específico en la etapa del juicio el juez valorar las evidencias digitales en base a las reglas de la sana crítica, el estado de inocencia, y el *In dubio pro reo*. Primero considera las reglas de la sana crítica, el cual se subdivide en tres aspectos que son: la lógica, las máximas de experiencia y la ciencia, el primero denominado la lógica está conformada por los principios de: Identidad (autenticidad de sí misma), principio de contradicción (imposibilidad de tener dos posiciones contrarias), principio de razón suficiente (justificación de su existencia), y un tercero excluido (explicación dentro de dos posiciones, siendo excluida de un tercero).

El segundo las reglas de las máximas de la experiencia consisten en criterios de la vida a las que el juzgador recurre. Estos criterios normativos o reglas no jurídicas, producto de que generalmente ocurre en numerosos hechos productos de la vida social concreta, sirven al juez, en una actitud prudente y objetiva, para emitir juicios de valor acerca de una realidad, con funciones heurística, epistémica y justificativa.

La Jurisprudencia suprema vinculantes recaída en la sentencia de exp. N°010-2002-AI/TC el derecho fundamental a probar, es uno de los elementos esenciales del derecho al debido proceso y a la tutela procesal efectiva. El Acuerdo Plenario Extraordinario N°1-2011/CIJ-116, sostuvo que “el Juzgador es el soberano en la valoración de la validez de la prueba, quien debe analizar todas las fases

desde el ofrecimiento, sin limitaciones ni control alguno; ningún imputado puede ser acreedor de responsabilidad penal sin elementos de prueba, y además se debe realizar bajo la observancia de las garantías constitucionales. El tercero es la ciencia, que consiste en los conocimientos científicamente aceptados socialmente, tal como exigen los cánones de la comunidad científica mundial.

Prueba científica.

Respecto a la prueba científica recientemente se ha dictado el Acuerdo Plenario N° 2-2007/CJ-116 como precedente vinculante, de fecha, dieciséis de noviembre de dos mil siete, el cual establece:

[...] la prueba pericial es de carácter compleja que va más allá de los actos previos [cuando la Dirección de Criminalística de la Policía Nacional, el Instituto de Medicina Legal, la Contraloría General de la República, emite los denominados Informes Especiales, que gozan de una presunción iuris tantum de imparcialidad, objetividad y solvencia], las pericias constan de tres elementos esenciales: a) el reconocimiento pericial, b) el dictamen o informe pericial que es la (f.8).

De la misma forma el mismo acuerdo plenario en el siguiente fundamento señaló respecto a la obligatoriedad del examen pericial:

[...] Un dictamen de prueba pericial para su valoración debe ser sometido al principio contradictorio, de modo que debe ser oralizado por el mismo perito, el cual no requiere de contrastación, corroboración o de fiabilidad; cabe señalar con ello el derecho al debido proceso y para ser más específico el derecho a la defensa no se desnaturaliza y tampoco infringe los principios de inmediación, contradicción y oralidad (f.9).

Es decir, en este acuerdo plenario establece que todo dictamen pericial es sometido a un debate en el juicio, donde el perito quién practico el informe está en la obligatoriedad de acudir al juicio para efectos de oralizar, ante el juez, quien conoce los hechos, que le permitirá emitir un criterio de valoración de la prueba.

Valoración de la Prueba.

Respecto a la valoración de las pruebas en un proceso, Esquivel (2005), sostuvo

que la valoración de la prueba es “la actuación probatoria que tiene una vinculación directa con realización de la actividad procesal, por el cual las partes influyen en el criterio o fallo del juzgador, quién va a resolver el juicio, creando y produciendo prueba que acredite la realización de los hechos”. (p.5). El Autor refiere que las pruebas incorporadas deben ser idóneas, pertinentes, conducentes, útiles y no esté en ninguna de las causales de ilicitud; es decir, que su obtención haya sido con el respecto de los derechos fundamentales de manera que el juez pueda tener la convicción y que su decisión sea en base al principio más allá de la duda razonable.

Siguiendo el mismo orden de ideas de las pruebas que deben ser valoradas por el juzgador, es importante citar a Téllez (2007), quién sostuvo “las evidencias de prueba están interrelacionados con el sistema informático, las pruebas digitales guardan una estrecha vinculación con las computadoras y con los soportes magnéticos y otros (p.243).

A lo que refiere el autor, es por el modo de vivir una comunicación electrónica, ya sea por redes sociales, Internet, web, correo electrónico entre otros, las personas por el uso diario de las TIC dejan evidencias en el mundo virtual, y éstas pruebas se encuentran en los dispositivos electrónicos, ya sea en el disco duro de la computadora, USB (Universal Serial Bus), CD (disco compacto), DVD (Disco Video Digital), Pendrive, email, cloud computing entre otros; de modo que estas mismas pruebas se encuentran enmarcadas dentro de la prueba documental tipificadas en el Art. 185 del Nuevo Código Procesal Penal.

El momento para la valoración de las evidencias digitales será en la etapa del juicio oral, lo que implica, que con el debate y respecto de los principios de inmediación, igualdad de condiciones, contradicción y publicidad; el Juez está en la capacidad de otorgar validez procesal, cabe precisar en esta fase probatoria se incorporarán las pruebas ofrecidas en los escritos de calificación penal, pero la condición es que fueran admitidas para ser practicadas; lo que da la oportunidad que se planteen objeciones, contradicciones, impugnaciones, entre otros, ya sea de parte de los acusados o de la defensa técnica.

Prueba Ilícita.

Se llama prueba ilícita o prohibida cuando en el momento de recabar fue obtenida a través de la infracción de los derechos constitucionales tutelados en su real dimensión. Según la concepción restrictiva, la prueba será prohibida cuando la prueba se obtiene o se practica dentro o fuera del proceso, siempre en cuando incurra en violación de derechos fundamentales, vale decir, cuando se afecte en la producción o recojo de la prueba a un derecho fundamental. En este caso específico estamos ante una prueba ilícita, el cual es excluido de la valoración, dado que nuestro ordenamiento jurídico prohíbe la actuación o valoración por afectar las garantías constitucionales. La doctrina en el derecho comparado lo denomina prueba prohibida, cuando en la obtención de la prueba se ha vulnerado la Ley, las garantías establecidas en la Constitución o de manera genérica cuando se afecta el derecho al debido proceso (Conso, López, Echandia).

Tomando en cuenta el segundo supuesto de concepción amplia, según Paz *Rubio*, sostuvo que la interpretación extensiva de la prueba prohibida consiste “en una desmesurada ampliación del ámbito de la prueba prohibida”. Lo que refiere el autor es que, la prueba prohibida o llamada prueba ilícita en nuestro país, según el autor debe ser interpretada de manera amplia, lo que implica que no debe dejar de sancionar al responsable del hecho, para ello incluso propone excepciones que se debe tomar en cuenta al momento de valorar, tales como el grado de afectación, la magnitud del hecho, ponderación de intereses, grado de complejidad del problema, entre otros.

Exclusión probatoria, respecto a esta teoría de la prueba ilícita el Máximo Tribunal se ha pronunciado “es un derecho fundamental la no utilización de la prueba prohibida”, es decir, la constitución en su Artículo 1º proscrib taxativamente la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del estado. Lo que implica que en la obtención o producción de la prueba no debe afectar los derechos fundamentales, de lo contrario se incurrirá en prueba ilícita o prueba irregular cuando no incurra en irregularidades o afectación de la actividad procesal (STC N° 655-2010 – PHC/TC).

Con similar postura la Corte Suprema se ha pronunciado señalando “prueba ilícita es aquella prueba cuya, obtención o actuaciones lesionan derechos fundamentales”. La postura de la corte es concreta al señalar que debe existir un respeto único en la producción, obtención y actuación de las pruebas, lo que implica que la obtención, ya sea, fuera o dentro del proceso debe respetar los Derechos Fundamentales; además aclara si en la actuación dentro del proceso, al momento de admitir, incorporar, excluir la valoración existió alguna afectación a los derechos fundamentales, inmediatamente la prueba debe ser excluida del proceso como ilícita (Corte Suprema R.N. N° 05-02-2008).

Nuestro país ha sido testigo, de múltiples casos de los Vladivideos, interceptación telefónica de Alberto Quimper, Kenjivideos, el caso del Congresista Mamani, recientemente el caso de Walter Ríos, Hinostroza, entre otros. La prensa mediática nos ha mostrado un conjunto de indicios que muestran de los hechos ilícitos; sin embargo, no fueron valorados por el juez, dado que existe una serie de afectación a los derechos fundamentales y algunos han sido observados en cuanto a su autenticidad de pericia de informática forense, por lo cual fue excluido del proceso.

Asimismo, la Corte Suprema R.N N° 342-2001-Lima sostuvo que “la inadmisibilidad e ineficacia de la prueba ilícita impide su valoración acuerdo del pleno jurisdiccional superior nacional penal”, impide su valoración (de la prueba directamente e indirectamente obtenida de la violación de los Derechos Fundamentales) teoría del fruto del árbol prohibido.

Existen dos manera o formas de vulnerar los derechos fundamentales reconocidos por la constitución de nuestro país; los cuales son: Extraprocesal, que consiste, en el hecho que ocurre, antes del inicio del proceso, se da específicamente la afectación de los derechos en el momento del recojo, producción y obtención de la fuente de la prueba digital (Independiente del proceso). Intraprocesal, en este segundo caso la afectación de los derechos se realiza en la ejecución de los actos procesales, es decir, la proposición, admisión y práctica de la prueba durante el proceso. Lo que implica, que se presente un conjunto de irregularidades, ya sea en plazo de presentación, falta de debate, plazo

extemporáneo, falta de pericia, etc., en este caso se denomina prueba irregular que como consecuencia trae su exclusión probatoria, por causales de irregularidad procesal.

En cuanto al ámbito de la exclusión, la doctrina es explícita en reconocer la exclusión de la valoración probatoria, cuando la prueba ha sido obtenida producto de una vulneración directa o indirecta de derechos y garantías constitucionales sustantivos (derecho a la libertad personal, derecho a la libertad domiciliaria, derecho a la intimidad, etc.). Sin embargo, viene cuando se trata de la vulneración de derechos constitucionales “procesales”: tales como el derecho al debido proceso, derecho a la tutela jurisdiccional efectiva, derecho a la presunción de inocencia y derecho de igualdad procesal, en conexión con normas de rango ordinario. Es decir, toda prueba digital, electrónica que se va ofrecer al momento de interponer la denuncia de un hecho, no solo debe licita, sino también cumplir con los procedimientos que establece el Código Procesal Penal. Cabe mencionar en este punto, si en la comisión de un delito ya sea por una llamada, vía redes sociales, email, y otros medios electrónico o digital, las partes son afectados, cualquiera de los agraviados puede presentar las pruebas como medios de evidencia del delito, en ese caso no se configura la afectación del derecho fundamental y tampoco es excluido como prueba ilícita. Pero cuando una tercera persona ajena a los hechos que no forma parte, obtiene la evidencia, en este caso específico si se configura la afectación de los derechos y por ende sería prueba ilícita.

El reconocido Jurista, sostiene, que la obtención de pruebas con violación a los derechos fundamentales de la persona, no puede tener eficacia alguna en el proceso. No puede ser objeto de valoración en el proceso, por lo que no constituye en sentido estricto prueba judicial válida, por lo que, debe reputarse inexistente, como tal, establece tres criterios: a) es insubsanables, esto es, una prueba obtenida con vulneración de derechos fundamentales, no puede ser convalidada por ningún otro medio, dado que ya incurrió a la ilicitud; en este caso opera la “regla de exclusión” es imperativa. b) la ineficacia de la prueba no trasciende al plano fáctico, lo que significa que, si bien los hechos descubiertos inconstitucionalmente no sirven para sustentar una prueba válida, ello no significa que no existieron en la realidad o que son otros distintos, de suerte que eventualmente es posible tanto a

su acreditación por otros medios de prueba (v. gr.: confesión). c) excepcionando la prueba independiente, por lo general la exclusión se extiende a todas aquellas evidencias conseguidas o practicadas de forma ilícita que se basan, derivan o tienen su origen en informaciones o datos conseguidos en la práctica de una diligencia inconstitucional (Muñoz, s/f).

Invalidez de la prueba, no genera efectos las evidencias digitales obtenidas directa o indirectamente con evidente vulneración de los derechos protegidos, los que concretamente este órgano constitucional protege los derechos tales como, el derecho al secreto de las comunicaciones, secreto financiero, a la intimidad de las personas, estos son los derechos que se deben ponderar al momento de valorar los medios probatorios”. El tribunal refiere que los derechos constitucionales merecen una ponderación de máxima protección frente a los demás derechos, en tanto los operadores jurídicos deben garantizar el respeto de los derechos consagrados y además son los encargados de aplicar la teoría de la exclusión probatoria (STC. N.º 1915-2005-PHC/TC, f.j9).

Ineficacia procesal. - El hecho de que se haya admitida una prueba ilícita no significa que ya está garantizado la eficacia procesal; incluso el juez tiene el criterio discrecional de poder no autorizar su incorporación, de ser así, por más que haya sido admitida será ineficaz; tampoco se oralizaría en juicio y menos se permitiría el debate probatorio, sado que el juez está impedido de valorar.

La postura de nuestra legislación peruana ha optado por la teoría de la prueba ilícita, lo que implica que no solo, el acto procesal o extraprocesal sea ilícito, sino también es absolutamente nulo de pleno derecho; asimismo genera a su vez una ilicitud en los actos procesales a carrea irregularidades de ineficacia procesal e inutilizable que no poder ser convalidad con ningún acto posterior (STC N° 2053-2003-HC/TC, fj.3).

A diferencia de otras constituciones internacionales del Derecho Comparado, incluso del mismísimo Constitución Norteamericana de los Estados Unidos, la Constitución peruana tipifica la denominada regla de exclusión de la valoración probatoria a las pruebas ilícita obtenidas con violencia moral, agresión física o psíquica y a los que obtienen pruebas con infracción o violación de los

derechos fundamentales consagrados en la constitución y en la Ley. (Const. Art. 2º. 10,24).

La normatividad citada refiere que nuestra carta magna, ha adopta la teoría del criterio de la prueba ilícita de exclusión de la valoración probatoria y también la ineficacia probatoria en caso de que las pruebas no cumplan con la validez y legitimidad que exige la ley. Según el Tribunal Constitucional peruano respecto a la legitimidad de la prueba, sostuvo: “la prueba legítima es un derecho fundamental complejo, cuyo contenido deben ser admitidos, incorporados, actuados, y valorados, de manera que se asegure la atención, producción o conservación de la prueba para su incorporación con los requisitos y procedimientos procesales, con el fin de que en la fase probatoria sea valorados por el juez, dando mérito a una sentencia debidamente motivada”. El máximo intérprete refiere que una prueba debe gozar de la legitimidad y no haber vulnerado ningún derecho fundamental al momento de su obtención, para ser admitidos, actuados y valorados, de lo contrario debe ser excluido (STC 6712-2005- HC/TC y STC 1014-2007-PHC/TC).

En el caso específico de la ilicitud en la obtención prueba digital con vulneración de derechos fundamentales, que hemos conocido por la prensa mediática, fue la absolución del caso de Alberto Quimper, la Corte Suprema de Justicia en la sentencia absolvió, señalando que la prueba digital (audio) materia de acusación, había sido obtenido con vulneración a sus derechos fundamentales, por lo tanto, era prueba ilícita o prohibida. Lo que implica de ninguna manera se puede valorar las pruebas obtenidas con vulneración a los derechos constitucionales, el audio que se utilizó en el proceso fue una grabación de una interceptación telefónica, es decir, fue una evidencia digital, lo cual no fue valorado por el juez, por lo que en su obtención se vulnero el derecho al secreto de las comunicaciones, en consecuencia, se excluyó porque se consideró como una prueba ilícita (San Martín, p.871).

A pesar de que existe una regulación constitucional respecto a las pruebas ilícitas, también, existe una postura distinta de los juristas, que sostuvieron que, “las pruebas ilícitas deben ser válidas y consideradas dentro de la eficacia probatoria en el proceso; sin perjuicio de la sanción que se debe imponer a los responsables

de dicha obtención, puesto que de por medio debe primar la búsqueda de la verdad y la justicia. Asimismo, debemos aclarar que los derechos fundamentales no son derechos absolutos y no existe ningún derecho absoluto y en esa medida los operadores del derecho, en este caso de manera directa el juez debería valorar la prueba ilícita tomando en consideración los principios de razonabilidad y proporcionalidad de los hechos.

Bajo la postura de la doctrina respecto a que las pruebas ilícitas deben ser valoradas, comparto con esta teoría; puesto que, en nuestro país se han visto en los últimos tiempos casos en los que las autoridades, como Alex Curi, Vladimiro Montesinos, el Congresista Kenji Fujimori, Mamani, Cesar Hinostroza, Walter Ríos, entre otros se han visto involucrados en hechos de corrupción, sin embargo, bajo el pretexto de la prueba ilícita se han escudado en la impunidad. Desde esta óptica se debe flexibilizar los derechos constitucionales, para cierto sector de corrupción de funcionarios, porque los derechos no son absolutos y que debe ponderar, como lo sostiene el autor, los principios de razonabilidad de la gravedad de los hechos, la complejidad, el daño causado, entre otros y debe ser validado la prueba ilícita bajo la excepcionalidad de ponderación de intereses en conflicto.

El pronunciamiento refiere, a que tanto la prueba tradicional como las pruebas electrónicas o digitales en su obtención no deben vulnerar los principios y derechos fundamentales, asimismo deben haber sido obtenidos bajo el conducto regular del respeto a los procedimientos y protocolos de ley, de caso contrario sería una prueba irregular. Sin embargo existe un conjunto de excepciones a la regla de exclusión de valoración probatoria, los cuales son cinco: primero es la fuente independiente, el descubrimiento inevitable, segundo es la buena fe, tercero es la infracción constitucional beneficiosa para el imputado, cuarto el principio de proporcionalidad o de ponderación de intereses en conflicto, asimismo el nexo causal atenuada del hecho, quinto la destrucción de la mentira de la persona imputada y sexto es la teoría del riesgo y la doctrina de la eficacia de la prueba ilícita para terceros o la infracción constitucional ajena.

Excepción a la regla de exclusión de la prueba prohibida.

La fuente independiente, sólo se excluye la prueba obtenida originalmente

de la violación de los Derechos Fundamentales, más no las pruebas derivadas de esta; el descubrimiento inevitable, consiste en valorar aquellas pruebas que igualmente se hubieran obtenido lícitamente, de no ocurrir la violación a los Derechos Fundamentales; la buena fe, consiste en valorar la prueba prohibida obtenida con violación sin intención (por error o ignorancia) de los Derechos Fundamentales; el principio de proporcionalidad o ponderación, lo que permite la valoración de prueba prohibida, cuando están en juego intereses de mayor intensidad que los lesionados para su obtención (verbigracia casos de criminalidad organizada), el nexo causal atenuado, sostiene que la ilicitud de la prueba se disipa o atenúa por efecto del tiempo.

También la infracción constitucional beneficiosa para el imputado, que admite la prueba prohibida cuando ésta puede ser utilizada a favor del imputado, asimismo la destrucción de la mentira del imputado, consisten en que puede aceptar la prueba prohibida a fin de atacar la credibilidad del imputado, finalmente la Infracción constitucional ajena, considera que pueden ser valoradas para condenar a imputadas no víctimas de la violación del Derechos Fundamentales.

Historia de Informática Forense.

Es así tomando en cuenta los antecedentes de la informática forense nos remontaremos a comienzo de los años 90, en el cual el FBI (Federal Bureau of Investigation) quienes determinaron que las pruebas electrónicas o también denominadas evidencias digitales gozaban de potencial imprescindible, que permitiría como prueba de alta probabilidad para combatir la lucha contra la delincuencia o criminalidad, es así que aprecio la prueba científica del ADN. Con estos antecedentes casi al finalizar los años 90, se creó por primera vez la IOCE (International Organization of Computer Evidence) con el propósito de compartir este paradigma de pericia de informática forense a nivel global, es decir, a nivel de todos los países, llegando a universalizarse como una prueba científica, confiable con valor de eficacia procesal.

Uno de las pruebas más importantes para determinar la integridad de las pruebas digitales es la informática forense, el cual es, practicada por un perito

especialista, quién emite un informe pericial para su debate en el juicio; de manera que el juez pueda valorar para motivar una sentencia.

Remitiéndonos a los antecedentes, uno de los reconocidos McKemish (1999), sostuvo que la informática forense es “la identificación, conservación, análisis y presentación de pruebas electrónicas o digitales” (p.19). El autor refiere que la informática forense, es practicada por un especialista, quién emite el informe pericial el cual contiene, la identificación de las pruebas, conservación y su origen que permitirá en juicio a través del principio de mediación conocer los hechos a través de la prueba científica para valorarla.

La Ciencia de la pericia en informática forense desde una óptica probatorio comprende identificar, recuperar, reconstruir, eliminar, además de analizar objetivamente un hecho electrónico. Se trata de la aplicación de los instrumentos para obtener un resultado científico de relevancia y pertinente para el proceso; no obstante, se presenta otros problemas, tales como la valoración, a través de las reglas de la sana crítica y las máximas de experiencia de parte de los jueces de los tribunales; es así que la prueba de informática forense va permitir demostrar de los medios digitales como prueba; siempre y cuando haya cumplido ciertos requisitos al momento de su obtención como en su incorporación al proceso, de manera que la prueba digital sea un elemento que cause certeza en el juez que vaya más allá de la duda razonable.

Los informes o dictámenes del profesional experto en la materia denominados peritos que examinen los dispositivos electrónicos (cuyo contenido es evidencia digital) deben identificar la marca y modelo de los dispositivos electrónicos o magnéticos para ubicar el origen o procedencia de las evidencias. Lo relevante para obtención y tratamiento de la evidencia digital está en su preservación y seguridad, de modo que los medios magnetos, ópticos (CD o DVD, BluRay), medios electrónicos (email) son los más adecuados, puesto que evitan la modificación, la alteración accidental o borrado voluntario y que en la pericia sea practicada por la investigación pública.

Asimismo es conveniente estudiar la estructura de la investigación informático forense, los cuales están determinados en tres aspectos: el primero es

análisis preliminar, para identificar las características y protocolos para someter la pericia de informática, segundo es la obtención de los datos informáticos, a cuyo efecto es de relevancia de manera que se identifiquen de las fuentes del origen, el estado de conservación, la constatación de la aplicación de las técnicas empleadas para garantizar la integridad y la legitimidad de la información.

Siguiendo la línea del tiempo la pericia en informática forense cada más aumenta su relevancia jurídica, debido al aumento de la comunicación virtual, vale decir que las tecnologías juegan un rol protagónico para las víctimas de esta sociedad riesgosa. En la cual los documentos electrónicos circulan a gran escala virtual, de modo que las evidencias de los delitos quedan registradas en la red. Es precisamente dichas evidencias se puede obtener y ofrecer. Pero para que sea valorado por el juez tiene que evaluarse, si al momento de obtener, fue de manera lícita sin vulnerar los derechos constitucionales. Además de ser lícita, hay otro requisitos para su valoración, que debe ser examinado por un perito especialista en informática forense, como sostuvo los especialistas, es la aplicación de un conjunto de técnicas científicas, analizadas por profesionales especializados en infraestructura tecnológica que permite garantizar identificar, preservar, analizar y presentar información o datos que sean válidos y confiables dentro de un proceso.

La importancia de los peritajes de informática forense, nace de la necesidad de las personas agraviadas por el alto grado de criminalidad y que en su mayoría han sido impugnadas por falta de autenticidad.

Cabe precisar que, el momento oportuno para que el representante del Ministerio Público, en este caso el Fiscal, la defensa y las demás partes puedan ofrecer los medios de prueba, es precisamente es en la fase intermedia, es decir una vez concluida la investigación preparatoria, con el auto de conclusión, pasa a la siguiente fase, en la que tendrá oportunidad de presentar; tal como lo establece el Nuevo Código Procesal Penal del 2004. Esta fase permite ofrecer la lista de testigos y peritos precisando sus datos personales y los hechos controvertidos que serán materia del examen en el desarrollo del debate (Art. 349º.1 h y 350º.1. f).

Asimismo, el persecutor del delito representado por el fiscal es el encargado de ofrecer los medios de prueba en la fase de la acusación, adjuntado la lista de la

cantidad de testigos y peritos especializados debidamente identificados, los hechos controvertidos para ser sometidos al examen dentro del proceso de juicio. De la misma forma, de manera excepcional, las partes intervinientes tendrá la oportunidad de reiterar nuevamente el ofrecimiento de medios de prueba que no fueron admitidos dentro de la audiencia de control de pruebas, sin embargo, para argumentar esta segunda oportunidad se requiere una especial fundamentación del peticionante, para que el mismo juez valore de inmediato en la misma audiencia, previo traslado a las partes (NCP. Art. 373º literal 2).

Contradicción de las Pruebas.

Las comunicaciones electrónicas están expuestas a un conjunto de riesgos, los cuales pueden ser pasible de ser impugnadas o excluidas del proceso, porque existe una gran dificultad para asegurar y garantizar la autenticidad e integridad de las pruebas, además por su volatilidad, vale decir que se puede manipular con facilidad, simular, modificar o borrar.

Asimismo existe una dificultad para determinar su origen y contenido, también la dificultad en los procedimientos para asegurar y vigilar la cadena de custodia hasta su incorporación a juicio oral y la dificultad en el manejo de los medios o dispositivos electrónicos de almacenamiento.

Todo medio de prueba necesariamente para su valoración en un proceso debe haber sido sometido a la contradicción, tal como lo señaló el Art. I del Título Preliminar del Código Procesal Penal establece el principio o criterio rector de la justicia penal, señaló que todo medio probatorio que presentan las partes en la etapa intermedia en el sistema acusatorio adversarial garantista, deben interiorizar al principio contradictorio como un requisito de validez de la valoración probatoria, dado que no solamente deviene como un derecho a la defensa, también como un instrumento de eficacia procesal y de llegar a la verdad de los hechos ocurridos .

Tal como señaló Taboada, docente universitario de la Universidad UPAO y Juez; el principio contradictorio o debate de las pruebas es la posibilidad que tienen las partes del proceso, de cuestionar todo medio o evidencia de prueba que pueda ser crucial en la decisión final de la resolución, en esta fase las partes tienen

igualdad de armas y puede ser eficaz, siempre en cuando las partes tengan la misma fuerza o igualdad de armas. También en esta fase de la investigación se da la posibilidad de refutación de la contraprueba.

En ese orden de ideas, la valoración de la evidencia digital, respecto a fotos tomadas de whatsApp llamadas pantallazos, grabación o transcripción de conversaciones de las partes implicadas suelen ocurrir con frecuencia; para que la evidencia se convierta en prueba las partes agraviadas debe conservar el equipo y mensaje, audio, video, etc. en sus respectivas direcciones electrónicas, dispositivo digital o imprimir en soporte de papel, luego ofrecerle como medio de prueba ante el Ministerio Público, Policía Nacional, es decir ofrecer el mismo equipo en que registra la evidencia, afín de que la fiscalía derive a un peritaje con el objeto de determinar la autenticidad e integridad de las evidencias, de tal manera que en el juicio no sea cuestionada su integridad y autenticidad y sea valorada por el juez para determinar un hecho.

Para garantizar la valoración y evitar la oposición e impugnación de la parte contradictoria contra las evidencias digitales es de vital importancia mantener la autenticidad e inalterabilidad de las pruebas sin hacer cambios a las imágenes originales, asimismo, los mismos deben contar con fecha y hora, codificación y contar con duplicados digitales originales de las imágenes reproducidas para preservar la autenticidad como una garantía de certeza de la fidelidad de la evidencia ubicada en el escena del suceso. A través, de software especiales es posible llegar a establecer las características, la marca y modelo de los equipos cuyo contenido son las evidencias digitales, de manera que las partes tengan la posibilidad de solicitar un peritaje, inspección o constatación pericial del origen y/o procedencia de la evidencia digital.

Cadena de Custodia.

La cadena de custodia se rige a través de un procedimiento sujeto al reglamento de la cadena de custodia, que está conformado de una serie de protocolos cuyo contenido son los elementos materiales, evidencias digitales y administración de bienes decomisadas o incautados como prueba de un hecho. Sin embargo, para garantizar el procedimiento de la cadena de custodia es importante tomar en cuenta

la importancia de la conservación de la prueba, tal como sostuvo el especialista Bradford, que “la cadena de custodia consiste en un procedimiento de alta confiabilidad cuyo contenido es un acta que describe los datos que documenta la manipulación y el acceso a las pruebas objeto de la investigación, que debe ser conservada y mostrar los datos específicos, con fecha y hora determinada”. (Resolución N°729-2006-MP-fn del 15. junio.2006)

El autor sostiene que, la cadena de custodia es la conservación y la seguridad de la inalterabilidad que debe seguir el procedimiento y los protocolos de ley, de manera que la prueba mantenga su autenticidad para su posterior valoración. Siguiendo la línea del tiempo, Colquitt. (1990) sostuvo “la cadena de custodia es para convencer al Tribunal de Justicia que la prueba sea autentica e inalterable”. La postura del autor es en la misma línea, dado que la finalidad de la cadena de custodia es para demostrar la autenticidad de la prueba, de tal manera que se garantice la validez y eficacia procesal.

Asimismo, el Instituto Nacional de Justicia de los Estados Unidos (2011) también se ha pronunciado respecto a la cadena de custodia, señalando que “es un proceso que permite mantener y documentar la historia cronológica de las pruebas”. Lo advertido por el Instituto de Justicia Norteamericana es que la cadena de custodia de las pruebas, conceptualiza como un conjunto de procedimientos que se debe seguir para garantizar la seguridad de las pruebas, de manera que mantengan una cronología en el tiempo y en el espacio para asegurar la valoración en los procesos judiciales.

La prueba Digital en la Etapa de Investigación Preliminar.

En primer lugar, la parte agraviada interpone una denuncia ya sea en la policía o en el Ministerio Público, es precisamente en este acto postulatorio de tutela las partes ofrecen los medios probatorios de los hechos delictivos, por el cual el Fiscal como representante del Ministerio Público designa a la policía de investigaciones para que dé inicio con las pesquisas. En cuanto a las pruebas digitales ofrecida por las partes el Fiscal debe solicitar a la parte que ofrece la evidencia digital que presente el dispositivo o componente electrónico el cual contiene la prueba. Es decir, si presenta fotos tomados con el celular, se debe presentar el teléfono móvil

con el cual se tomó las fotos, de esta forma el fiscal tendrá la seguridad de que la evidencia no hay sufrido modificaciones o alteraciones; luego inmediatamente se debe proceder al lacrado y cadena de custodia, asimismo se debe solicitar una pericia informática, a fin de garantizar la autenticidad y la valoración en el proceso.

Investigación Preparatoria.

El fiscal es el titular de la acción penal encargado de investigar y recabar los medios probatorios para su posterior acusación penal de los hechos a quién se le atribuye la responsabilidad penal, en el caso específico de las evidencias digitales, los agraviados deben ofrecer los medios ya sea celulares, USB, disco duro, pendrive, u otro medio en las cuales se encuentran almacenados los elementos de la prueba, de modo que la fiscalía, pueda derivar a través de una cadena de custodia al Centro de Peritaje del Ministerio Público, de modo que se pueda obtener el código valor de Hash de autenticidad e integridad, acto que al finalizar la investigación preparatoria el fiscal pueda realizar su acusación ofreciendo los medios probatorios, para causar certeza en el juez. En la etapa intermedia, una vez culminada la etapa de investigación preparatoria, teniendo como requisito la sospecha grave, se pasa la fase intermedia, en el cual se debatirán la incorporación de las pruebas.

En el juicio oral, el juicio oral es la última fase en la que las partes, los peritos, los testigos y otros oralizan las pruebas, es en esta etapa, que se da el principio contradictorio a través de un debate de las partes, uno defiende la autenticidad y el abogado de la defensa su objeción o exclusión, para convencer al juez de acuerdo a los intereses que persiguen.

Derecho Comparado

Sentencias Precedentes sobre la Prueba Digital.

En el mes de agosto del año 1986, un Caso relevante de Irán Contreras, donde un militar de los Estados Unidos con el cargo de Teniente Coronel Sr. Oliver North escribió y envió mensajes a través de correo electrónico, pero luego borró los correos, sin embargo, terminaron involucrándolo, por lo que la computadora guardaba una copia de respaldo y los mensajes fueron recuperados del servidor de respaldo de correo, por lo que los Jueces lo declararon culpable.

En caso indica que todos los mensajes enviados por correo electrónicos, por más

que se elimine de la bandeja de entrada queda en el servidor de correo, significa que con un peritaje es posible recuperar los mensajes eliminados.

Otro del caso sobre la prueba digital sucedió en el año 1991 denominado Caso Guttman, donde su esposa apareció muerta sorpresivamente con un mensaje o nota de suicidio, sin que la nota consigne su firma, la nota fue escrita desde su propio computador e impresa con una impresora matricial en blanco y negro. En la investigación se determinó que Gudman tenía una amante, quién fue investigada y en su casa se le incauto un dispositivo magnético Disquete de 5^{1/4} cortado en pedazos, dicho material se reconstruyó físicamente y luego se recuperó la información con el uso de un software denominado Anadisk y se encontró culpable del asesinato de su esposa y fue condenado culpable.

En tercer caso fue de Mitnick en el año de 1995, donde Kevin Mitnick tras una persecución de la FBI por tres largos años, quién había sido procesado en los años 1981, 1983 y 1987 por cometer diversos delitos electrónicos contra la sociedad, “se le acusó de haber ingresado sin autorización a la información de las computadoras más seguras de los Estados Unidos, es decir era un hacker experto”, por el cual se le condeno a no hacer llamadas telefónicas durante la permanencia de su encarcelamiento”, luego de su libertad fue considerado por la comunidad hacker como un ¿Héroe?.

Un caso peruano el Tribunal Constitucional recientemente se pronuncia respecto a una grabación de una conversación telefónica, sostuvo “el registro de la conversación telefónica del acusado por parte de la Fiscalía se produjo a raíz de una denuncia verbal previa de un particular, ante la alta probabilidad de que se consume un delito de cohecho pasivo en su agravio. La intervención, por ende, se produjo con la expresa autorización de uno de los interlocutores, quién permitió la grabación de las llamadas con el fin de descubrir un delito “(...) en tanto el Tribunal considera que la grabación es constitucionalmente legítima y el contenido de la comunicación telefónica, la que no supuso una violación del derecho al secreto de las comunicaciones del actor, ni una vulneración de su intimidad, pues en las grabaciones no existe causa que pueda entenderse como parte de su vida íntima.

1.3 . Marco Espacial

La presente investigación tuvo la finalidad de determinar el tratamiento legal de la prueba digital, el cual se desarrolló en el Ministerio Público de Ventanilla, ubicada en la panamericana norte, en el contexto interdistrital conformado por dos los distritos de Lima Norte y la Provincia Constitucional del Callao provincia de Lima; situada aproximadamente a 34km al noroeste de Lima, a la altura del Km 28.5 de la Panamericana Norte camino a Ancón y a 18km al norte del Callao. Se optó este lugar por lo que existe un alto grado de criminalidad y también por lo que a nivel de la Provincia Constitucional del Callao se ha implementado el Nuevo Código Procesal Penal.

1.4 Marco Temporal

El desarrollo del presente estudio se llevó a cabo durante los meses de octubre del 2017 a julio del año 2018; y específicamente en el Ministerio Público de Ventanilla, provincia Constitucional del Callao, Lima Metropolitana, Perú.

1.5 Contextualización: Histórica, Política, Cultural, Social.

Como contexto histórico es importante resaltar la Ley de Enjuiciamiento Civil del año 2000, que fue la primera vez que se pretendió aportar soluciones para el tratamiento de los medios de prueba. Con el transcurrir de los años se incorporaron como medios de reproducción de la palabra, el sonido y la imagen; y paralelamente aparecieron los dispositivos magnéticos que permitía almacenar, o reproducir palabras denominados audios, datos, textos, imágenes, videos, etc. Que en la actualidad con el avance tecnológico se han convertido en archivos digitales, que juegan un papel crucial como medio de prueba digital en los procesos judiciales, su relevancia radica, en que el tráfico jurídico ya sea contratos, firmas electrónicas son enviados o remitidos por correo electrónico; así como las transacciones a través de redes sociales, web, whatsapp, etc. Son parte importante de la integración, por lo que el gobierno actualmente está implementando el aparato judicial con tecnología de punta, sin embargo, no es suficiente, dados que el Ministerio Público no cuenta con sala de visualización de medios digitales.

Contexto político

El contexto político en nuestra legislación aún no se han regulado en el Código Procesal Penal del 2004 específicamente respecto a la prueba digital, porque solo se subsume dentro de las pruebas documentales tipificado en el Artículo 185º, actualmente nuestros políticos están haciendo uso de los medios digitales como prueba de las actividades ilícitas, sin embargo a falta de autenticidad y/o vulneración de los derechos no fueron valorados, los peritos en informática forense especializados en la criminalística de la Policía nacional del Perú, son los encargados de emitir los informes de la veracidad e integridad de los medios digitales.

Contexto cultural

Según el informe del INEI del año 2017 aproximadamente de cada 100 personas 93 hace uso de la tecnología, es un indicador que la sociedad peruana está haciendo uso de las tecnologías, no solo computadoras, sino los distintos medios de acceso a Internet. Estos informes demuestran la cultura integracionista y tecnológica con la red mundial. Lo que significa que el uso de medios digitales como correo electrónico, páginas web, redes sociales, entre otros hace que dejen las evidencias de los actos delictivos, de manera que con un peritaje de informático se puede identificar la autenticidad de la información, no solo ello sino también los mensajes su ubicación, tiempo y modo de envió.

Contexto social

En el contexto social existe una criminalidad en aumento, sobre todo con el uso de las tecnologías de la comunicación, es decir los medios electrónicos se han convertido como un medio de comunicación para cometer delitos, los cuales dejan mensajes, fotos, videos, audios, y otros medios electrónicos que son evidencias digitales para identificar y sancionar a los responsables; sin embargo, muchos de estas pruebas son impugnados por falta de un tratamiento adecuado, tanto en su conservación y seguridad o por no haber sido examinado por un perito en informática forense. Motivo por el cual los sujetos que delinquen quedan libres e impune.

1.6 Supuestos teóricos

Supuesto general

Es insuficiente el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017.

Supuesto específico 1

Es insuficiente la implementación tecnológica para el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao- 2017.

Supuesto específico 2

El incumplimiento de los procedimientos, tales como el respeto de los Derechos Fundamentales, la cadena de custodia, peritaje de informática forense impide la incorporación de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.

Supuesto específico 3

La vulneración de los derechos fundamentales impide la valoración de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017

II. Problema de Investigación

2.1. Aproximación temática

Actualmente nos encontramos en la era de la generación virtual, y en la era de la inteligencia artificial, es decir en el tiempo de la desmaterialización del documento, incrementándose vertiginosamente la comunicación a través de medios electrónicos y la amenaza de la desaparición del papel en físico. Los individuos interactúan, creando, intercambiando información a través de la red. Incluso se han atrevido a catalogar que nos encontramos entre la generación denominada nativos digitales; y la generación cibernética o internautas a través de estos medios nos encontramos conectado con el mundo global. Incluso en la legislación peruana se ha legitimado el uso de la tecnología en todos los procesos judiciales, tales como la resolución administrativa N° 872-2017-P-CSJCL/PJ publicado el 29 de diciembre de 2017 por la Corte Superior de Justicia del Callao, que autoriza a los abogados litigantes que podrán tomar fotografía a los expedientes de tal distrito judicial del Callao. Así como también la publicación de la Resolución Administrativa N° 342-2016-CE-PJ con fecha, 26 de diciembre de 2016, que autoriza la disposición para que el diligenciamiento de las notificaciones y citaciones judiciales puedan realizarse vía telefónica, incluidas las tramitadas vías exhorto.

Por lo referido el Derecho Procesal ha tenido que ceder la presión del avance tecnológico dando lugar a espacios de la informatización. Las TICs han permitido un importante cambio dentro del poder judicial permitiendo una celeridad importante en la emisión de actos procesales y menguando las cargas procesales. Asimismo la comunicación masiva a través de la red y el uso de las tecnología permite acceder y obtener pruebas digitales de los delitos, lo más preocupante es que los agraviados no conocen el tratamiento adecuado de tal medio probatorio para aportar al Ministerio Público y éste a su vez, carece de instrumentos tecnológicos para su tratamiento y valoración eficaz, lo que deja a múltiples personas en la indefensión y falta de justicia. Por lo expuesto surgió la necesidad de investigar respecto a la regulación del tratamiento de las pruebas digitales en el nuevo Código Procesal Penal.

2.2. Formulación del Problema de Investigación

La Tecnología de Información y Comunicación ya forma parte de nuestras vidas

cotidiana que ha cambiado nuestro modo de comunicarnos a través de ellas compartimos información inmediata y lo más sorprendente en tiempo real ya sea fotografías, textos, información, datos, audios, videos, mensajes etc. asimismo usamos chats, correos electrónicos, plataformas virtuales, webs, redes sociales, Facebook, Twitter o Dropbox, Whatsapp, Skype, Cloud computing, entre otros. Incluso podemos observar en las audiencias cuando los jueces algunas veces están comunicándose por whatsapp, redes sociales, entre otros; este modo de interactuar también deja evidencias digitales de las personas que delinquen, y cada vez más los agraviados usan estos medios digitales para ofrecer como medio probatorio.

Cabe señalar que en el Callao se concentra un buen porcentaje de índice delictual, producto de ellos existen una gran cantidad de denuncias penales, sobre todo la mayoría de los denunciados presentan como evidencia un conjunto de medios electrónico o digitales, tales como fotos, videos, audios, correos electrónicos, entre otros. Precisamente aquí surge una serie de interrogantes, ¿son admitidas estas evidencias electrónicas? ¿El Ministerio Público cuenta con la implementación tecnológica como para garantizar la autenticidad? ¿Son legítimas para que el juez pueda valorarlas? ¿Cuál es el tratamiento que brinda el Ministerio Público para que estas pruebas electrónicas ofrecidas tengan eficacia procesal? ¿Cuáles son los requisitos para obtener una prueba electrónica?, ¿cuáles son los procedimientos para incorporar la prueba electrónica? ¿Cuándo una prueba digital es considerada ilícita o irregular? ¿Cuáles son las reglas o criterios de valoración de parte del juez?, este y otras interrogantes han sido desarrolladas y resueltas en el presente trabajo de investigación, gracias al aporte de los expertos en actividad en el campo jurídico, tanto jueces y fiscales de reconocida trayectoria.

2.3. Planteamiento del Problema

Problema General

¿Cuál es el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao- 2017?

Problema específico 1

¿Cuál es la implementación tecnológica para el tratamiento de la prueba de digital

ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017?

Problema específico 2

¿Cuáles son los procedimientos para la incorporación de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017?

Problema específico 3

¿Cuáles son los derechos fundamentales afectados que impiden la valoración de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017?

2.4. Justificación

El reconocido jurista Uriarte sostuvo que la investigación encuentra su justificación en “la pregunta y respuesta del porque se ha seleccionado específicamente este problema de investigación, así como las razones que puedan explicar el carácter social, económicas, culturales, técnicas, científicas, teóricas, prácticas, personales, del fenómeno de estudio” (Uriarte, s.f., p. 3).

Las razones por las que se emprende el presente estudio es debido a que en la realidad se aprecia una falta de regulación para un tratamiento especial en el nuevo Código Procesal Penal sobre el manejo de prueba digital, de manera que se pueda atenuar la criminalidad, y los medios digitales cumplen una función importante para el recojo de información con relevancia jurídica; los agraviados obtienen evidencias digitales o electrónicos con facilidad, sin embargo la mayoría no son valorados por falta de un tratamiento adecuado, precisamente cuando las partes hace uso del derecho de contradicción, se invierte la carga de la prueba para quién lo ofrece, si no ha sido examinado por un perito se excluye la prueba, más aun el Ministerio Publico no cuenta con la implementación tecnológica suficiente y los peritos para dar respuesta inmediata y seguridad de la prueba.

En este orden de ideas, las razones por las que se emprende este estudio es debido a que en la realidad se aprecia problemas con el avance de la tecnología, dado que toda la información electrónica, tanto mensajes, fotos, conversaciones, videos y otras evidencias electrónicos pueden presentarse como medio probatorio, sin embargo el Ministerio Publico, las notarías no están implementadas como para dar un tratamiento de manera que puedan ser valorados en el proceso judicial, por lo que pueden ser impugnadas; vale decir, la criminalidad puede seguir campeando, por falta de un tratamiento legal de las pruebas digitales. ¿Este problema me impulso a investigar para conocer con mayor certeza las causas si el Ministerio Publico cuenta con la implementación suficiente para dar un tratamiento y seguridad de los medios electrónicos? Asimismo, para conocer cuál es el tratamiento que brinda el Ministerio Publico del distrito judicial de Ventanilla a los medios digitales ofrecidas por las partes, para asegurar su valoración y eficacia procesal; como también en ¿qué medida ha afectado a los derechos de las víctimas que forman parte del proceso?.

Justificación teórica.

La presente investigación está referida a determinar si existe un tratamiento especial de la prueba digital en el nuevo código penal, desde este punto de vista, el contenido de investigación investiga adquiere su justificación teórica, toda vez que tiene por objeto analizar la regulación vigente y en cuanto corresponda fortalecer o reformular, dichas normatividad con respecto al tratamiento de la prueba digital en el nuevo Código Procesal Penal, así como la naturaleza y filosofía de la autenticidad de la prueba digital; todo ello debido a su gran importancia como parte del derecho a la prueba, en la medida que importa la salud colectiva y combate de la criminalidad.

Justificación legal.

El presente trabajo de investigación encuentra su relevancia jurídica al sistematizar distintas normas, jurisprudencias, doctrinas y posturas de los expertos de jueces, fiscales, peritos y abogados litigantes, todos relacionados al tratamiento jurídico de la prueba digital, incorporación y valoración de la prueba digital, y el derecho a presentar una prueba. Dicha investigación incluye análisis de la normatividad:

Constitución Política del Perú, Ley del peritaje, Código Penal, Código Procesal Penal del 2004 y Sistema de cómputo

Justificación metodológica.

La metodología que se ha empleado en la presente investigación está orientado a generar nuevas estrategias que permitirán analizar de manera concienzudo los conocimientos nuevos del fenómeno de estudio, dado que se busca otras formas de investigar a través de la aplicación de métodos científicos. La investigación tiene un sistema de categorización de la información de manera que el análisis se realiza de forma conglomerada y desde una perspectiva filosófica del fenómeno objeto de estudio. En esta orden de ideas, el tratamiento de las pruebas digitales ofrecida por las partes fue sometido al análisis riguroso y metódico, a fin de dar respuestas a los objetivos propuestos con la confiabilidad sustentada en la experiencia de los expertos y de la normatividad vigente.

2.5. Relevancia

La presente investigación encuentra sustento y relevancia teórica, práctica, metodológica, jurídica y social, toda vez que pretende ahondar en un estudio profundo del objeto de investigación respecto al tratamiento de la prueba digital ofrecidas por las partes en el proceso penal. Por un lado, porque en la actualidad no existe una regulación especial en el nuevo Código Procesal Penal para dar un tratamiento específico sobre las pruebas digitales, por lo que se trata como si fuera una prueba tradicional, tal como lo estipula el Artículo 185º como pruebas documentales.

Del mismo modo la importancia se sustenta en el análisis de la constitucionalización del derecho a las pruebas, discusión sobre las teorías de obtención de la prueba, límites y exclusión de la prueba digital, la vulneración de los derechos fundamentales, las fases de obtención, incorporación y valoración de las pruebas digitales. El cual integra a la comunidad jurídica nacional y extranjera, en un medio de integración global como es el siglo XXI, donde las evidencias digitales que puedan probar un hecho delictivo corra el riesgo eminente, que por falta de un tratamiento adecuado de autenticidad e seguridad no sea valorado y que

los verdaderos responsables del delito sigan operando generando más daños a la sociedad.

2.6. Contribución

La presente investigación pretende encontrar respuestas y ampliar regulaciones del tratamiento especial de la prueba digital, con la finalidad de que exista una protección y garantía al derecho de ofrecer, a que se admitan, actúen y valoren los medios probatorios; lo que implica, encontrar una regulación especial para las pruebas digitales, a fin de que el derecho a la prueba al ser una base fundamental sea garantía en sus diversos aspectos, en este sentido la constitucionalización del derecho a la prueba no es suficiente ni mucho menos eficaz para dotar a los justiciables un tratamiento especial de la prueba digital, sino desarrollar mecanismos jurídicos que permitan garantizar la autenticidad e integridad para su valoración probatoria.

Por ende, la presente investigación tiene por finalidad analizar, cuestionar, desarrollar, interpretar, ponderar y descomponer diferentes teorías y figuras jurídicas relacionado al derecho a la prueba como un derecho constitucional, eminentemente de connotación penal, con el propósito de obtener una incorporación el tratamiento de las pruebas digitales como base del derecho al ofrecer las pruebas.

2.7. Objetivos

La presente investigadora tiene la finalidad de demostrar, contrastar, determinar o establecer una relación de tipificación entre la evidencia digital de connotación penal con el marco jurídico del derecho penal "(...) Los objetivos de la investigación es la ruta, vía o directriz hacia donde se orienta la investigación. Se redactan en verbo infinitivo y guarda estrecha relación con el problema de investigación. El aclamado Hernández, Fernández y Baptista (2014, p. 358) recomiendan en el planteamiento de los objetivos se debe utilizar verbos activos e infinitivos que permitan guiar la intención básica del estudio de la investigación, sobre todo define de manera concreta sobre las acciones que se llevarán a cabo para describir y comprender el fenómeno de estudio.

2.7.1. Objetivos específicos

Objetivo general

Describir el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017

Objetivo específico 1

Describir la implementación tecnológica en el tratamiento de la prueba de digital en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.

Objetivo específico 2

Describir los procedimientos para la incorporación de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.

.Objetivo específico 3

Determinar los derechos fundamentales afectados que impiden la valoración de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao- 2017.

III. Marco Metodológico

3.1. Categorías y categorización

Para el reconocido Gomes el término categoría, se refiere principalmente a la clasificación de conceptos de manera que tenga una estructura jerarquizada, por lo que trabajar con ellas implica agrupar elementos, ideas y expresiones en torno a un concepto que responde a una estructura jerarquizada. Los agentes o sujetos que conforman el contexto u escenario de estudio de la presente investigación son los operadores en Derecho Penal, tanto Jueces como fiscales del Distrito judicial de Ventanilla de la provincia Constitucional del Callao y Peritos en informática forense de la División de Investigaciones de Delitos de Alta Tecnología (DIVINTAD) de la DIRINCRI – PNP, quiénes son los encargados de patrullar, vigilar y custodiar el ciberespacio a nivel del Perú, quiénes son los concedores y expertos en el contenido de la investigación, asimismo tienen la mayor potencialidad de emitir un juicio de valor, con un criterio pertinente sobre el tema, respaldado por su larga trayectoria y experiencia.

Straus y Corbin sostuvo que la categorización consiste en asignar conceptos a un nivel más abstracto, lo que refiere el autor, es que las categorías tienen un poder conceptual jerarquizado, puesto que estar organizada en grupos de conceptos denominados subcategorías, las cuales están relacionadas entre sí, los cuales emergen del fenómeno de estudio. Las categorías utilizadas en una investigación responden al marco teórico y conceptual de la investigación, esto a su vez los supuestos que orientan las categorías o instrumentos de investigación empleados en la presente investigación. Enseguida se considerará la clasificación de conceptos y grupos de conceptos que responden a la investigación que tiene por título: tratamiento de las pruebas digitales ofrecida por las Partes en los procesos penales del Ministerio Público de Ventanilla.

Tabla1: Categorías y sub categorías

CATEGORÍAS	SUBCATEGORÍAS	FRASES CODIFICADAS
A. TRATAMIENTO DE LA PRUEBA DIGITAL	A1. La prueba digital Art. 155 a 252	El Tribunal Constitucional se ha pronunciado respecto a la forma de obtener y brindar seguridad a la producción o preservar la prueba, considerándolo como un derecho constitucionalmente protegido. Los aspectos esenciales de asegurar los medios y conservación de fuentes de prueba; una de ellas es la cadenas de custodia que permite la conservación, seguridad, custodia de la integridad de la prueba.
	A2. Actuación de la prueba digital. Art. 356, 350	La etapa para la actuación de la prueba es en el juicio oral, tales como incorporación de la prueba, debate contradictorio y sobre todo la valoración de la prueba, bajo la observancia obligatoria de los principios de oralidad, publicidad, intermediación y de contradicción, así como lo tipifica el Artículo 356°.1 del NCPP. Las oralización de los principios permiten a las partes controlar a los sujetos procesales sobre la legitimidad de la prueba y al juez valorar (Talavera, 2009, p.40).
	A3. Legitimidad de la prueba digital	La Jurisprudencia del tribunal constitucional STC N° 1014-2007-PHC/TC, considera que “la actividad probatoria como un derecho constitucional, la infracción de actos que violen el contenido esencial de los derechos fundamentales, trae como consecuencia la exclusión de la prueba por considerar como ilícita, por lo que el juez está impedido de valorarla.
B. IMPLEMENTACIÓN	B1. Nuevas tecnologías	La era digital en la que nos encontramos, la comunicación virtual se ha convertido en un instrumento crucial para la comunicación y según informe de INEI de cada 100 personas 93 tiene acceso a Internet, redes sociales, páginas web, etc. Lo cual hace que las personas dejen evidencia digital en las redes de las conductas ilícitas, de modo que el Ministerio Público debe contar con la implementación adecuada para afrontar los nuevos retos. (INEI, ver anexo 2)
	B2. Sala de visualización	El Ministerio Público a nivel nacional carece de una implementación tecnológica para dar un tratamiento adecuado a las pruebas digitales, además carecen de software, equipos y salas especializadas de visualización para una adecuada transcripción de los medios digitales (Entrevista: Quiroz, 2018).
	B3. Pericia informática	Pericia Informática es una disciplina criminalística de una secuencia de procedimientos con el objeto de investigar los sistemas informáticos de datos de hechos delictivos con relevancia jurídica para determinar través de los valores Hash la autenticidad o veracidad de un hecho. Este

		<p>procedimiento se lleva a cabo en un laboratorio especial denominado Workflow. (Sebastián, 2009, p.3)</p>
C. INCORPORACIÓN	C1. Admisión de la prueba digital Art. 155° N CPP	<p>El Jurista Taruffo sostuvo ciertas reglas para su admisión, se tiene: a) para la admisión se requiere un auto debidamente motivado (Art. 155°.2); b) se pueden excluir los que no sean pertinentes y los prohibidos por la ley (Art. 155°.2); c) es posible limitar a las pruebas abundantes; d) el juez examinará la prueba en juicio (Art. 155°.4); e) no es posible usar una prueba con alteración a su autenticidad (Art. 157°.3); f) no se pueden utilizar, directa o indirectamente, las obtenidas mediante la vulneración de los derechos fundamentales de la persona (Art. 159°).</p>
	C2. Principio de contradicción	<p>El Jurista Taboada, sostuvo que el principio contradictorio es la posibilidad de refutación y cuestionamiento de todo medio o evidencia de prueba que pueda ser crucial en la decisión final de la resolución, en esta fase las partes tienen igualdad de armas y puede ser eficaz, siempre en cuando las partes tengan la misma fuerza o igualdad de armas.</p>
	C3. Cadena de custodia	<p>“según es jurista Aguirre sostuvo que la Cadena de Custodia es una herramienta que permite garantizar integridad de los elementos de prueba recopilados en la investigación, de manera que permita acreditar los hechos con los autores del delito. (Aguirre, 2012, p.9).</p>
D. VALORACIÓN ART. 158° N CPP	D1. Ilícitud Art. 395	<p>“la ilicitud es la vulneración a la legitimidad de la prueba relacionada a las prohibiciones en la obtención de la prueba, su vulneración les convierte en prueba ilícita, por el cual el juez está prohibido en valorarla por ser atentatorio a los derechos fundamentales (Talavera, 2009, p.18). También el Tribunal supremo STC N° 2053-2003-HC/TC, define la prueba ilícita como la vulneración de la legalidad procesal y de los derechos fundamentales que deviene en la ineficacia de la valoración.</p>
	D2. Impugnación Art. 159° N CPP	<p>Caso de Alberto Quimper, la Corte Suprema de Justicia en la sentencia se absolvió, señalando que la prueba digital (audio) había sido obtenida con vulneración a los derechos fundamentales, por lo tanto, era prueba ilícita. Para lo cual cita el Art. VIII del Código Procesal Penal, carecen de efecto legal las pruebas obtenidas, directa e indirectamente, con violación del contenido esencial de los derechos fundamentales de la persona. (San Martín, p.871). En tanto fue excluido y absuelto.</p>
	D3. Informática Forense	<p>Es una técnica que consiste en el análisis del dispositivo o medio del electrónico, con el objetivo de conocer la autenticidad o alteración y manipulación de las pruebas digitales. Así emitir un dictamen pericial sobre los hechos para adquirir certeza.</p>

Matriz de construcción de categorías y subcategorías apriorística

ÁMBITO TEMÁTICO	PROBLEMA DE INVESTIGACIÓN	PREGUNTAS DE INVESTIGACIÓN	OBJETIVO GENERAL	OBJETIVOS ESPECÍFICOS	CATEGORÍAS	SUBCATEGORÍA
Tratamiento de la prueba digital ofrecida por las partes	La Tecnología de Información y Comunicación ha cambiado nuestro modo de comunicarnos a través de ellas compartimos datos sea fotografías, textos, información, datos, audios, videos, mensajes etc., con el interactuar las personas dejan evidencias digitales que delinquen, por ello los agraviados usan estos medios digitales para ofrecer como medio probatorio, ahí surge el problema que si el Ministerio Publico da un tratamiento adecuado para su valoración.	¿Cuál es el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017?	Describir el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.	Determinar cuál el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Publico de Ventanilla, Callao -2017	Prueba digital	<ul style="list-style-type: none"> ▪ Naturaleza ▪ Medio, fuente y Objeto ▪ Modalidades, procedimientos y límites. ▪ Tratamiento, actuación y legitimidad.
		¿Cuál es la implementación tecnológica para el tratamiento de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017?		Describir la implementación tecnológica en el tratamiento de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.	Implementación	<ul style="list-style-type: none"> ▪ Nuevas tecnologías ▪ Sala de visualización ▪ Pericia informática
		¿Cuáles son los procedimientos para la incorporación de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017?		Precisa los procedimientos para la incorporación de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.	Incorporación	<ul style="list-style-type: none"> ▪ Obtención, Pertinencia, necesidad y utilidad ▪ Admisión, y oportunidad de incorporación. ▪ Principio de contradicción. ▪ Cadena de custodia.
		¿Cuáles son los derechos fundamentales afectados que impiden la valoración de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017?		Establece los derechos fundamentales afectados que impiden la valoración de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao- 2017.	Valoración	<ul style="list-style-type: none"> ▪ Conservación ▪ Contradicción ▪ Ilícitud, y ilegalidad ▪ Excepciones ▪ Forense informática ▪ Autenticidad ▪ Integridad. ▪ Impugnación

Preguntas de acuerdo a las categorías y sub categorías establecidas:

Subcategoría	Preguntas a sujetos perteneciente al cargo de Jueces	Preguntas a sujetos perteneciente al cargo de Fiscales	Preguntas a sujetos perteneciente al cargo de peritos en informática	Preguntas a sujetos pertenecientes al cargo de Abogado litigante.
Tratamiento de la prueba digital	¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad?	¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria?	¿Cuáles son los procedimientos que debe tener en cuenta el Ministerio Público para derivar la evidencia digital a la División de Investigación de Delitos de Alta Tecnología (DIVINDAT)?	¿Cuál es el procedimiento que debe seguir un abogado, respecto a las evidencias digitales de su patrocinado antes de ofrecer al Ministerio Público?
Implementación tecnológica	¿Los Juzgados Penales cuentan con la implementación tecnológica suficiente para brindar seguridad y custodia a las pruebas digitales ofrecida por las partes?	¿El Ministerio Público cuenta con salas de visualización de video, audio, foto y otros que permita su transcripción confiable de la prueba digital?	¿La DIVINDAT cuenta con la implementación tecnológica para dar respuestas inmediatas a las pericias de informática forense?	¿El Ministerio Público cuenta con salas de visualización de video, audio, foto y otros que permita su transcripción confiable de la prueba digital?
Incorporación de la prueba digital	Según su experiencia y análisis probatorio ¿Cuáles son los problemas más comunes que impiden la valoración de la prueba digital?	¿Cuáles son los requisitos que debe cumplir una prueba digital para su admisión e incorporación al proceso?	¿Cuáles son los procedimientos técnicos que garantizan la autenticidad e integridad de la prueba digital?	¿Cuáles son las causas de exclusión probatoria de las evidencias digitales?
Valoración de la prueba digital	¿Cuáles son las causales para la exclusión de la prueba digital?	¿Cuáles son las causales para la exclusión de la prueba digital?	¿Cuál es la eficacia de las pericias de informática forense practicadas por DIVINDAT?	¿Cuáles son los procedimientos que recomienda usted, para que las evidencias digitales sean eficazmente valoradas por el Juez?

3.2. Metodología

3.2.1. Respuestas de los estamentos, triangulación de datos, y conclusiones por cada pregunta:

Categorías	Sub categorías	Entrevistado 1 Juez superior Reos en Cárcel- Lima Norte	Entrevistado 2 Juez Superior del JIP-Callao	Entrevistado 3 Perito de Informática de la DIVINDAT	Conclusión
Prueba digital	<ul style="list-style-type: none"> Tratamiento especial de la prueba digital en el Código Procesal Penal. 	<p>Tratamiento especial de la prueba digital en el Código Procesal Penal del 2004 de manera puntual y específica. No existe, no hay regulación actual como prueba digital, sin embargo el Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documental, si entre las fuentes de prueba de un hecho ilícito se encontrara un audio, o un video grabacion u otro soporte digital o electrónico, simplemente el desahogo probatorio o actuación probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004.</p>	<p>El Código Procesal Penal del 2004 señaló en el Art. 185 de pruebas documentales, dentro de ello se considera los documentos, audios, videos y todo medio electrónico, es decir el todo tratamiento digital ingresa a por ese tratamiento, pero exclusivamente un tratamiento especial en Código Procesal Penal no está establecido.</p>	<p>El Ministerio Público al recibir las pruebas digitales como prueba del delito debe solicitar a la Juez la autorización para un examen de pericia informática y luego deriva a la División De Investigaciones De Delitos De Alta Tecnología (Divindat) de la Av. España. Para lo cual debe tener en cuenta los siguientes procedimientos técnicos: -La prueba debe estar debidamente rotulado y lacrado para evitar su adulteración. -Debe contar con la cadena de custodia -Debe contar con la autorización del Juez a través de una resolución judicial.</p>	<p>La Prueba digital no tiene un tratamiento especial en Código Procesal Penal sin embargo su regulación está en el Art. 185º considerada como pruebas documentales, es decir todo las evidencias electrónicas, tanto como mensajes a través de email, cludComputing, imágenes, audio, video, u otro soporte digital son considerados como prueba documental. Si entre las fuentes de prueba de un hecho ilícito se encontrara evidencias digitales, la actuación probatoria se efectuara bajo la observancia del Art. 382 del Código Procesal Penal.</p>
		<p>Las evidencias digitales deben entrar obligatoriamente en cadena de custodia, dado que se tiene que observar, preservar, conservar, custodia, para que se altere</p>	<p>Exigir al MP que derive para un peritaje para efectos de que se perenne y armen la cadenas de custodia para su conservación y se pueda presentar a la audiencia contradictorio de juzgamiento</p>	<p>Contamos con los instrumentos tecnológicos para recuperar información de las cuentas de Twitter, Facebook, correos electrónicos, páginas web, llamadas telefónicas y entre otros dispositivos hardware como: disco</p>	<p>Las evidencias digitales obligatoriamente debe entrar en cadena de custodia, para conservar, conservar y custodiar para mantener la originalidad logrando el principio de mismidad y</p>

	<ul style="list-style-type: none"> Legitimidad de la prueba digital. 	<p>y sea original para lograr el principio de mismidad. Cumpliendo los requisitos de exhibición, autenticación, actuación, reproducción, y principio contradictorio para su valoración.</p>	<p>para evitar la manipulación, y contaminación; de modo que se evite el cuestionamiento y exclusión. En la practica judicial no estamos capacitados en el sistema de acceso a las pericias de estas naturaleza, dado que puedan quedar impunes por falta de conocimientos y/o capacitacion de los operadores de derecho.</p>	<p>duro, USB, memoria flas, teléfono móvil, cámaras digitales, etc.</p>	<p>evitar la manipulación; luego el MP debe enviar a la DIVINDAT para una pericia de informática forense a fin de obtener un código valor HASH de autenticidad e integridad, de manera que se pueda presentar a la audiencia contradictorio de juzgamiento.</p>
Implementación	<ul style="list-style-type: none"> Nuevas tecnologías 	<p>El Ministerio Publico no cuenta con herramientas para la guarda, quiero hacer una claracion, las grabaciones en audio y en video, necesariamente en observancia del Art. 382, requiere que entre en cadena de custodia, que tenga procedimientos tecnicos y el MP puede custodiarlos y conservarlos. Que bien podian estar en el laboratorio y iniciado la etapa intermedia deberia estar en manos del ministerior publico o tambien deberia estar en deposito que el ministerio debe implementar.</p>	<p>Existe una una insuficiencia de implementacion de laboratorios a nivel nacional y existe un centralismo en todo el Peru para las perfcias de pruebas digitales y de las tradicionales, para los delitos mas comunes se sigue haciendo en Lima. Incluso para los delitos informáticos es mas complejo se tiene que remitir a DIVINDAT-PNP de la Av. España y dicha división no existe en el Callao.</p>	<p>El DIVINDAT si cuenta con instrumentos técnicos y un laboratorio equipado para determinar: Donde se almaceno o publico la información, cuando, es decir la fecha en la que se borró o publico la información, como se almaceno y publico la información.</p> <p>Incluso detecta los sectores dañados del dispositivo en caso de pérdida de datos, etc. Los resultados de los informes deben estar con los formularios A6 y A7 debidamente rotulados y debe estar en cadena de custodia.</p>	<p>El Ministerio Publico no cuenta con la implementación tecnológica suficiente en la sede de Ventanilla, existiendo un centralismo a nivel nacional sobre las pericias de informática forense de las evidencias digitales; siendo los delitos informáticos los mas complejos por el cual se tiene que remitir a DIVINDAT –PNP de la Av. España lo cual dificulta el plazo y aumenta la carga procesal.</p>
		<p>Las evidencias digitales como grabaciones, de</p>	<p>Las pruebas digitales deben ser emitida a una institucion</p>	<p>A los discos duros se extrae un imagen forense al cual se le aplica</p>	<p>Las evidencias digitales para tener una validez en la sede</p>

Incorporación	<ul style="list-style-type: none"> ▪ Requisitos de obtención. ▪ Principio de contradicción 	<p>audio y video necesariamente requieren que entre en cadena de custodia y el ministerio público puede custodiarlos. Se incorpora al debate y valoración, la estación procesal para su actuación e incorporar al proceso es durante la oralización de documentos.</p>	<p>competente, reconocida y debidamente registrada para que los peritos demuestren su competencia en la materia que realizan sus pericias pueda tener la validez en la sede judicial, ratificadas en la audiencia pública, si es posible con el derecho contradictorio con peritos de parte; recién en este caso tendría validez la prueba digital, pero normalmente no es muy común que presenten este tipo de pericias, por lo general el Ministerio Público no lo utiliza por lo que no tiene recursos, lo que trata de presentar son las partes particulares por lo que los estudios son costosos.</p>	<p>el HASH que consiste en un algoritmo matemático que asigna un Código Valor que Autentica el contenido de la información. El resultado depende del caso, si es sencillo o complejo, incluso desde 24 horas se puede entregar los informes periciales.</p> <p>Sugerencia a todos los agraviados que cuenten con evidencias digitales, cuyo contenido estén en algún dispositivo electrónico, tales como: USB (Universal Serial Bus), CD (Disco Compacto), DVD (Disco Video Digital), Tablet, Pc, Teléfono móvil, cámara digital u otro. no eliminar las evidencias de los dispositivos conservarlos, hasta interponer la denuncia, asimismo ofrecer como medio de prueba el mismo aparato original como prueba del delito</p>	<p>judicial debe ser examinada por un perito informático, luego debe ser incorporada a la estación procesal a través de un debate en audiencia pública en el cual el perito ratifica, sometidos al derecho contradictorio de los peritos de parte, cumplido esta fase la valoración y producción de la prueba queda a discrecionalidad del juez.</p>
Valoración	<ul style="list-style-type: none"> ▪ Licitud ▪ Informática forense 	<p>Se excluye la evidencia digital no prueba, en caso de infracciones de los derechos fundamentales, existe el Art.159 del Código Procesal Penal sobre las prohibiciones probatorias, tanto las fuentes y medios de prueba que se actúen en juicio oral. Las pruebas cuando sean obtenidas, los datos deben ser descargados en un</p>	<p>La exclusión tiene diferentes motivos, en la audiencia de control en la etapa intermedia las partes solicitan la exclusión de las pruebas por la mala producción, como prueba ilícita, prueba irregular, por lo que no se ha respetado los procedimientos procesales en la producción, pero no es muy frecuente no se ha dado. A nivel de proceso inmediato no se ha dado, lo que si se</p>	<p>Al menos los informes periciales que se practicaron en esta institución el 100% han sido valorados por el Juez, incluso después del debate de contra peritaje de parte, contamos con laboratorios acorde con la tecnología; dado que los delitos informáticos han evolucionado, nosotros somos policías que custodiamos el ciberespacio. . En el caso de que la evidencia se encuentre en algún medio</p>	<p>Las evidencias digitales son excluidas del proceso como prueba ilícita cuando en su obtención haya afectado uno de los derechos fundamentales, el Art. 159 del Código Procesal Penal señaló el Juez no podrá utilizar, directa o indirectamente, las fuentes o medios de prueba obtenidos con vulneración de los derechos fundamentales, asimismo la prueba irregular</p>

		<p>dispositivo electrónico a través de un programa informático para ser sometidos para una dictamen pericial informático.</p>	<p>presenta es con las filmaciones.</p>	<p>electrónico como email, página web, twitter, facebook, whatsapp, u otros. Transcribir el contenido en un soporte de papel, porque ahí se encuentran todos los detalles de los datos como fecha y hora de envío, destinatario, emisor, etc. El cual será corroborado con un peritaje para identificar la autenticidad.</p>	<p>puede ser excluido si en su actuación no se respecta los procedimientos procesales.</p>
--	--	---	---	--	--

Categorías	Sub categorías	Entrevistado 4 Fiscal Provincial de la segunda Fiscalía Penal Corporativa de Ventanilla	Entrevistado 5 Fiscal Adjunto Provincial de la segunda Fiscalía Penal Corporativa de Ventanilla	Entrevistado 6 Fiscal Adjunto Provincial de la Primera Fiscalía penal corporativa de Ventanilla	Conclusión
Prueba digital	<ul style="list-style-type: none"> ▪ Tratamiento de la prueba digital en el Código Procesal Penal. 	El Código Procesal Penal del 2004 lo regula como prueba documental, pero no prueba digital y su tratamiento es como una prueba tradicional con lo mismo que estipula el artículo 185º.	No se encuentra específicamente en el Código Procesal Penal del 2004 como tal, pero toda prueba digital se trata con las mismas características de una prueba documental, conforme lo establece el artículo 185º del Código Procesal Penal.	Conforme el Código Procesal Penal explícitamente no hay un Artículo que lo desarrolle como prueba digital, ya que solo comprende como prueba tradicional o documental.	Todos los entrevistados fiscales y sus respectivos adjuntos en actividad manifiestan que no existe una regulación del tratamiento especial de la prueba digital en el nuevo Código Procesal Penal.
	<ul style="list-style-type: none"> ▪ Legitimidad de la prueba digital 	Todas las pruebas digitales deben haber sido obtenidas conforme a Ley, es decir no tiene que haber incurrido en causales de nulidad o fraude, falsificación u otro similar. En caso de las evidencias digitales tienen que presentarlo con el mismo equipo que fue grabado.	Muy pocas personas en sus denuncias ofrecen medios digitales como prueba, por lo que normalmente lo borran, ya sea de su celular, computadoras, o correo electrónico, porque se sienten afectados y atemorizados por la represalia pero luego quieren invocar el cual ya es imposible, entonces los delitos quedan impunes.	Las denunciantes cuando interponen denuncias si hacen referente de los agravios que sufrido a través de la red, sin embargo no presentan las pruebas, porque en esta zona del Callao existe las venganzas por esta razón callan o las borran, pese a existir aumento de delito hay pocos que denuncian.	La delincuencia en el distrito de Ventanilla va en aumento, sin embargo los agraviados no denuncian en su totalidad por temor a las represalias, incluso en cuanto a las pruebas digitales, acuden a la policía o fiscalía cuando tan solo con la manifestación sin pruebas, la mayoría lo borran, caso sea hace imposible de poder identificar al delincuente.
Implementación	<ul style="list-style-type: none"> ▪ Nuevas tecnologías 	Aquí en la Fiscalía de Ventanilla no contamos con recursos suficientes para la implementación tecnológica, así como también necesitamos una	El Ministerio Público no cuenta con los recursos suficientes para implementar con tecnología de punta el tratamiento de la prueba digital, sin embargo hace 15	No contamos con sala de visualización de evidencias digitales, porque lo hacemos cada uno de los fiscales en la computadora de la oficina, aquí mismo transcribimos en	Los Jueces y Fiscales de Ventanilla afirman en las entrevistas que el Ministerio Público de esta sede no cuenta con la implementación

		implementación en cuanto al manejo de las pruebas digitales, porque muchos desconocemos.	días se ha implementado una sala de visualización para las audiencias de visualización y transcripción en soporte de papel (acta de transcripción) en presencia de las partes. Cabe señalar que esta sala de visualización no se encuentra en este local, sino en la otra sede. Porque antes de ello toda la visualización lo realizábamos en la computadora de mi oficina.	presencia de las partes, por el cual se levanta un acta.	tecnológica para dar un manejo apropiado de las pruebas digitales y menos están capacitados en este sistema digital.
Incorporación	<ul style="list-style-type: none"> ▪ Requisitos de obtención. ▪ Principio de contradicción 	<p>Cuando se trate de evidencias digitales, se debe actuar según lo dispuesto en el Art. 187º todo documento de video se visualizara para su transcripción en acta en presencia de las partes. Por lo menos aquí hemos recibido muy pocas pruebas a lo menciona.</p>	<p>La exclusión de las pruebas digitales impugnadas por las partes se pueden reiterar el ofrecimiento de los medios de prueba inadmitidos en audiencia de control invocando el inciso 3) del artículo 373, asimismo invocando el artículo 374 el fiscal durante el juicio podrá ampliar su acusación e introducir una prueba nueva.</p>	<p>La prueba digital siempre va a ser cuestionada por el defensor de la otra parte en el juicio oral, por tal razón es que debe cumplir que en su obtención no debe afectar los derechos, de caso contrario será excluida ya sea como prueba ilícita o irregular.</p>	<p>Según el Art. 187º toda prueba digital presentada por las partes debe pasar por una audiencia de visualización para su transcripción en acta en presencia de las partes, que definitivamente se da en la fase de investigación preparatoria.</p>
Valoración	<ul style="list-style-type: none"> ▪ Licitud ▪ Informática forense 	<p>Como toda prueba normal no debe ser ilícita o prohibida, para que la prueba tenga valor probatorio lo derivamos a la División de Investigación de la policía para su pericia respectiva, de manera que en juicio oral el juez pueda valorarlo, y evitar de esta</p>	<p>El problema más común de los peritajes de las evidencias digitales es el plazo, dado que tenemos que derivar a la DIVINDAT, si en caso de apertura de la investigación preliminar por 60 días, y ampliar a 120 días de investigación preparatoria entonces la demora en el peritaje, afecta,</p>	<p>Tuve dos casos, primero presenté una demanda de una conversación de WhatsApp y Facebook de acoso, el cual fue derivado a DIVINDAT en el cual la PNP determinó a quién correspondía los mensajes. En el otro caso se presentó una captura de pantalla de un mensaje de WhatsApp de</p>	<p>En el año 2017 de los 6 fiscales que se entrevistó, solo uno menciona que tuvo un caso de prueba digital que contenía los mensajes en Facebook del abusador de violación sexual de una menor, el cual fue derivado a DIVINDAT el informe pericial fue valorado por el juez para</p>

		forma las futuras impugnaciones de parte de la defensa técnica.	dado que las partes nos podría interponer un control de plazo.	amenaza y acoso el cual no fue meritado por lo que notenia una certificacion de un perito; por lo que había borrado el mensaje de su equipo y tampoco Presentó el mismo celular.	una sentencia del agresor, dado que en la pericia se determino al autor del mensaje, como, cuando, y los detalles. Luego otro caso que una victima Presentó pantalla de captura de WhatsApp el cual no se merituo.
--	--	---	--	--	--

3.3. Metodología

En la presente investigación se ha citado al reconocido Valderrama (2007), quién sostuvo que el método “es un conjunto de actos prediseñados que permite seguir un procedimiento, de manera a través de esta secuencia de pasos se podrá llegar a obtener resultados de la investigación propuesta” (p.131).

Enfoque

La presente investigación está orientado al uso del método con enfoque cualitativo (es inductiva), seguida por una diversidad de procesos sistemáticos de investigación, que implica investigación, exploración recolección y análisis de datos basados en la descripción, rasgos y característicos, así como su interrelación y discusión, para realizar análisis y descripción de los datos recabada y lograr nuevas conclusiones del fenómeno de estudio.

Diseño

Respecto al Diseño de investigación ejecutado o aplicado en el estudio ha sido eminentemente de corte descriptivo, y Teoría Fundamentada, en razón a que “se aplicó una secuencia de procedimientos de inducción, el cual origina una nueva teoría explicativa del fenómeno de estudio; donde las normas, conceptos, jurisprudencias, datos de los expertos han sido analizados e sistematizados para obtener nuevos resultados”. (Strauss y Corbin, 2002).

3.4. Escenario de estudio

Balcazar, Gonzáles-Arratia, Gurrola y Moysen (2013), quienes sostuvieron que: “el escenario de estudio más apropiado para una investigación cualitativa, implica que el observador tiene fácil acceso y tiene la posibilidad de establecer una relación cercana e inmediata con los expertos sobre el tema de investigación”.

Por lo explicado es preciso definir como escenario de estudio y recojo de información se hizo a través de las entrevistas, considerando como escenario de estudio la provincia constitucional del Callao donde se encuentran los especialistas sobre el tema materia de investigación. Se eligió este lugar por lo que mi vivo en

este distrito y además mi trabajo como abogado litigante me ha permitido llevar casos de esta naturaleza en esta sede fiscal y sobre todo según reporte de INEI existe un aumento de criminalidad donde los delitos dejan evidencia en las redes sociales, Internet, email, pagina web entre otros. Por el uso masivo de las tecnologías de la información y comunicación.

3.5. Caracterización de sujetos

Dentro del fenómeno de estudio es importante definir los agentes expertos que nos permitirán con fuente de información relevante, a través de experiencia, conducta, etc. Los que son personas profesionales, hechos, sucesos, procesos, casos, organizaciones o instituciones de naturaleza jurídica (Hernández et al, 2014, p.)

Los sujetos que constituyen el presente escenario de investigación son profesionales en Derecho Penal Jueces, Fiscales y Abogados del distrito de Ventanilla de la provincia del Callao, y además el especialista en peritaje de informática forense de Divindat-PNP de patrullaje cibernético involucrados y conocedores de temas relacionados a la materia de investigación, quiénes tienen la mayor potencialidad de emitir un criterio y juicio adecuado y pertinente sobre el tema, dado su larga trayectoria y experiencia.

Tabla2: Caracterización de los Sujetos**Perfil académico de los expertos**

Nº	PROFESIÓN	GRADO ACADÉMICO	CARGO ACTUAL
01	Abogado y Docente	Doctor	<ul style="list-style-type: none"> ▪ Juez superior Reos en Cárcel-Lima Norte. ▪ Autor de diferentes publicaciones de libro de derecho penal. ▪ Conferencista Internacional del Colegio de Abogados del Perú.
02	Abogado	Magister	Juez Superior del Juzgado Investigación Preparatoria del Callao
03	Abogado	Magister	Fiscal Provincial de la segunda Fiscalía Penal Corporativa de Ventanilla
04	Abogado	Magister	Fiscal Adjunto Provincial de la segunda Fiscalía Penal Corporativa de Ventanilla
05	Abogada	Magister	Asistente en función de la 5ta. Fiscalía Provincial penal Corporativa del distrito Judicial de Ventanilla
06	Abogada		Asistente en función de la 1ra. Fiscalía Provincial penal Corporativa del distrito Judicial de Ventanilla
07	Abogado	Magister	Docente Universitario y expositor del Colegio de Abogados de Lima
08	Abogado	Magister	Fiscal Adjunto de la Cuarta Fiscalía Provincial Penal Corporativa del distrito de Ventanilla

09	Abogado	Magister	Fiscal Adjunto de la Cuarta Fiscalía Provincial Penal Corporativa del distrito de Ventanilla
10	Abogada	Magister	Fiscal Provincial Titular de la Cuarta Fiscalía Provincial Penal Corporativa del distrito de Ventanilla
11	Sub 3 PNP	Perito Analista en sistemas	Perito en Informática forense de la División de Investigación de Delitos a Alta tecnología DIVINDAT-PNP
12	Ingeniería Informática y de Sistemas	Perito informático Perú	Peritaje Informático Computadoras, servidores, tablets, móviles, cámaras; chats, redes sociales, whatsapp, transcripciones de mensajes amenazantes por email, resolvemos delitos informáticos.

3.6. Procedimientos Metodológicos de Investigación

Recogida de Datos.

Los datos se recopilarán a través de una fuente directa con entrevista a los expertos tanto a jueces, fiscales, abogados litigantes y peritos en informática forense, el instrumento mediador, permitirá ver la realidad del tratamiento de la prueba digital ofrecida por las en el Proceso Penal de Ventanilla.

Análisis de Datos.

Para el análisis de datos se aplicará diferentes métodos los cuales nos permitirá responder apropiadamente al problema de investigación y obtener conclusiones.

Método inductivo: “es una aproximación a la realidad mediante el cual el investigador concreta los argumentos más concretos que van desde un aspecto particular a lo general, sustentada en una serie de evidencias eminentemente

empíricas”. (Ávila, 2006, p. 7). En este orden de ideas, este método de la presente investigación ha permitido el uso de que los resultados obtenidos en la presente investigación de respectiva muestra sean generalizables a la población general estudiada.

Método Exegético: a través de este método se ha analizado las normas, tanto la constitución, el código penal procesal penal, como jurisprudencias se analizó manera aislada e independiente considerando su contenido con el tema de investigación.

Método sistemático: a través de este método se ha analizado de manera sistemática con interpretación sistemática y articulada de norma, código penal, doctrina, jurisprudencia y aportes de los expertos de manera que permita una conclusión de la investigación.

3.7. Técnicas e Instrumentos de Recolección de Datos

Según el especialista metodólogo Valderrama (2013) sostuvo que las técnicas establecidas para llevar a cabo una investigación cualitativa son tres, tales como (a) Observación, (b) Entrevista, (c) Grupos de discusión (Focus Groups) y los instrumentos de recolección de datos, más usados y conocidos por los investigadores, son: la guía de entrevista, ficha de observación, lista de cotejo check list entre otros.

Para culminar con la presente investigación se recolecto los datos a través de las siguientes técnicas de recolección de datos:

Técnicas

- a) Entrevista.** - Esta técnica permitió al investigador formular preguntas a los funcionarios públicos judiciales (Jueces y Fiscales de la Sede Fiscal de la sede Fiscal de Ventanilla), Peritos especialista de la división de Investigación de Delitos de Alta Tecnología – DIVINDAT-PNP. Las preguntas de la entrevista fueron formuladas de acuerdo a los requerimientos de las categorías y sub categorías de la investigación, teniendo como eje central los problemas, los objetivos y los supuestos del estudio. Los datos recolectados mediante esta

técnica fueron analizados mediante un cuadro comparativo para contrastar los supuestos.

- b)** Análisis documental: la presente técnica me permitió analizar e sintetizar los conceptos más importantes de las fuentes bibliográfica documentales, conformado por Artículos, textos, revistas, informes periciales, casos y otras fuentes de naturaleza documental, y otras vinculadas con el tema de investigación, con la finalidad de determinar, si existe un tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.
- c)** Análisis Jurisprudencial: esta técnica nos permitió analizar las dos sentencias que representan precedentes vinculantes sobre tema exclusión de evidencia digital del proceso, emitida por el Tribunal Constitucional, relacionada con el tema de investigación, y establecer si la fiscalía dio un tratamiento adecuado la prueba ofrecida por el Ministerio Público en contra de Alberto Quimper.

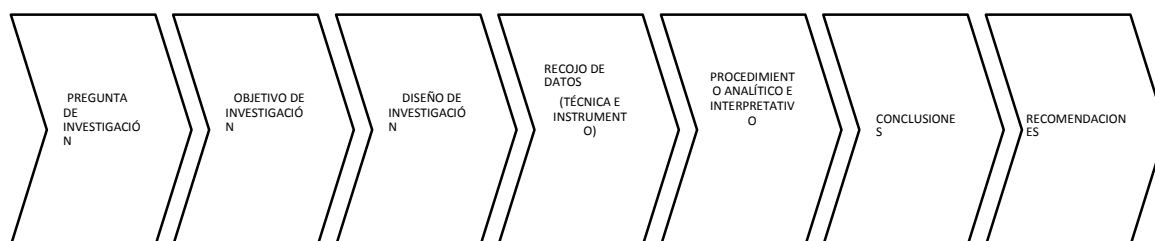
Instrumentos

- a). Cuestionario. - Este instrumento contiene preguntas abiertas, donde el entrevistado tenga la posibilidad de argumentar sus respuestas con mayor libertad de acuerdo a su experiencia. Estas preguntas, se plantearon partiendo del tema de sub preguntas del problema principal y de los objetivos y teniendo como horizonte los supuestos. El mismo que estuvo compuesta por 8 preguntas abiertas.
- b). Ficha de análisis de fuentes documentales: En aplicación de este instrumento de investigación se ha recopilado información valiosa sobre el tema objeto de estudio, esto es, el tratamiento que se ha hecho a nivel doctrinario por los especialistas en la materia.
- b). Ficha de análisis jurisprudencial: En aplicación de este instrumento de investigación se ha recopilado información acerca de la postura del Tribunal Constitución, sobre la validez de la prueba digital y sus excepciones establecidos en las jurisprudencias vinculantes.

3.8. Mapeamiento

La presente investigación se ha desarrollado en el Distrito Judicial del Ventanilla, se escogió este escenario dado que la mayor parte de la criminalidad se realiza en el Callao y Ventanilla no es la excepción; también otro de los factores que influyeron para determinar el estudio fue la cercanía y las facilidades porque mi persona como abogado litiga en esta Jurisdicción y he visto casos respecto al fenómeno de estudio, asimismo cuento con relaciones amicales con algunos jueces y fiscales lo cuales son una ventaja para el recojo de la información con mayor facilidad y precisión.

Esta se objetiviza mediante el siguiente mapa de procesos:



3.9. Rigor Científico

Según, Ramirez y Zwerg (2012), sostuvo que en el rigor científico “el investigador debe ser consciente en su forma de ver el mundo y sus limitaciones, cumplir con las condiciones que exige el método y la rigurosidad”. (p.94).

La presente investigación, ha respetado y respetara las normas establecidos por el método científico, de modo que nos desprenderemos de nuestros criterios personales para dar prevalencia al campo de mundo científico.

Credibilidad

Según, Rodriguez Gomez, citado por Manuel Cortez, señaló; “la credibilidad es la confianza en la veracidad de los descubrimientos realizados en una investigación y hace referencia a la necesidad que exista isomorfismo entre los resultados de la investigación y las percepciones que los sujetos participan en la realidad estudiada”. (p.43).

Transferibilidad

Según, Palacios, B., Sanchez,C., y Gutierrez, A (2011), señaló “este criterio corresponde a la validez externa en la investigación cualitativa. Se refiere al estudio que es representativo del universo al cual pueden extenderse los resultados obtenidos (p.583).

Seguridad

Se ha redefinido la confiabilidad –*reliability, fiability*– como seguridad o auditabilidad

–*dependability*–. *La repetición de datos permite lograr la credibilidad fundamental de las ciencias exactas* donde el investigador somete a distintas mediciones y repeticiones confiables.

Confirmabilidad

El criterio objetivo del investigador está definido como confirmabilidad, de modo que el investigador va construyendo el conocimiento de investigación cualitativa. De manera que permite que otro investigador pueda continuar con complementar con nuevos conocimientos (Marshall y Rossman, 1999).

IV. Resultados

4.1. Descripción de Resultados

4.1.1. Resultados del análisis de los trabajos previos.

El presente trabajo de investigación abordó una importante fuente de trabajos previos realizados con cierto grado de similitud. Lo que permitió ahondar en la problemática, de modo que nos permitió comprender y analizar con mayor agudeza las dimensiones de la estructura del trabajo. Enseguida citaré los aportes de mayor relevancia:

Bueno de Mata (2013), en su investigación de tesis doctoral titulada, *a prueba electrónica en el marco de una administración de justicia informatizada*. El tipo de investigación con enfoque cualitativa y nivel descriptivo, sustentada en la Universidad Nacional de Salamanca; escuela de posgrado con la finalidad de obtener el grado de magister en Derecho; presentó las siguientes conclusiones, “el Derecho Penal no ha tenido otra opción que volverse permeable al avance vertiginoso de la tecnología y ceder espacio a la informatización de sus contenidos. Los emails, páginas web, SMS, Whatsapp, imágenes digitales, videos conferencias, y otros son elementos que constituyen elementos digitales, denominado prueba electrónica, las mismas que necesitan una secuencia de procedimientos tecnológicos que la administración de justicia no cuenta para una valoración eficaz” (p.130).

13

Pareira (2013), en su Tesis titulada *“la exhibición de documentos probatorios y soportes informáticos”*, sustentada en la Universidad Nacional de Girona, Cataluña de España; presentó las siguientes conclusiones que a modo de resumen se detallan “La aplicación Hash es una técnica informática de la más alta tecnología que permite el aseguramiento de la integridad de las pruebas digitales. Están basadas en la obtención de datos de los medios electrónicos denominado copia espejo el que identifica el origen de la información en los dispositivos electrónicos como una copia única. Las funciones que cumple el criptográfico hash, es mitigar las dificultades o errores de los sectores de los dispositivos de almacenamiento de la información que pudieran afectar la integridad de los datos, dando una alta fiabilidad de autenticidad e integridad de la información” (p.419).

Sequeiros (2015), en su Tesis titulada, *vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano-2015*; el tipo de investigación No experimental enfoque cualitativo, sustentada en la Universidad Nacional Huánuco facultad de Derecho y Ciencias Políticas, para obtener el Título de Abogado; en el cual Presentó las siguientes conclusiones que a modo de resumen se detallan “la naturaleza virtual de los delitos informáticos, puede generar lagunas en la tipificación y subsunción entre el hecho del delito y encuadramiento de la norma penal, ya que la informática no tiene límites, que a nivel general, existen modalidades de comercio electrónico, asimismo distintas formas de delitos informáticos, por lo que se debe crear instrumentos legales eficaces que afronten este problema social.

Baudelio (2011), en su Tesis titulada, *la prueba ilícita penal en la administración de justicia en el Perú Petroaudios Vladivideos*; el tipo de investigación enfoque cuantitativo; sustentada en la Universidad Nacional de Trujillo, Facultad de Derecho, para obtener el grado Doctor en Derecho y Ciencias Políticas; en su investigación Presentó las siguientes conclusiones que el resumen se detallan a continuación “uno de los elementos de mayor relevancia para impartir justicia y conocer la verdad está constituido por la consistencia de la prueba, consecuentemente su obtención, incorporación y valoración probatoria debe realizarse bajo la observancia de los principios constitucionales de legitimidad, licitud y legalidad; y, principalmente; teniendo en cuenta el primer Artículo de nuestra carta magna el respeto de la persona humana y su dignidad humana. Cabe señalar que en la época actual, la actuación y valoración de la prueba está sujeto a los conocimientos técnicos y científicos de los peritos, pues su valoración y eficacia depende de la facultad discrecional de los jueces, quienes deciden a través de las reglas de la sana crítica y las máximas de experiencia; vale decir por la observancia de las pruebas sometidas a los criterios de la ciencia y la tecnología de manera que los dictámenes periciales corroboren fiabilidad y autenticidad para las decisiones judiciales”(p.172).

Pareja (2017), presentó su tesis doctoral titulada, *modelo de control constitucional para la admisión de la prueba de cargo con violación a derechos fundamentales en el sistema jurídico peruano*. Sustentada en la Universidad Pontificia Católica del

Perú; en la escuela de posgrado con la finalidad de optar el grado de Magister en Derecho Procesal Penal; quién en su investigación presentó la siguiente conclusión “los derechos fundamentales de las personas consagrado en la Constitución constituyen la base y piedra angular de principios y garantías sobre la cual se erige todo el ordenamiento jurídico como protección de los conflictos y mantener la armonía de la sociedad; en consecuencia es importante el reconocimiento pleno de los derechos constituciones de las personas” (p.116).

4.1.2. Resultados del análisis de la doctrina.

La etapa para la actuación de la prueba es en el juicio oral, tales como incorporación de la prueba, debate contradictorio y sobre todo la valoración de la prueba, bajo la observancia obligatoria de los principios de oralidad, publicidad, inmediación y de contradicción, así como lo tipifica el Artículo 356^o.1 del NCPP. Las oralización de los principios permiten a las partes controlar a los sujetos procesales sobre la legitimidad de la prueba y al juez valorar (Talavera, 2009, p.40).

La era digital en la que nos encontramos la comunicación virtual ha convertido en un instrumento crucial para la comunicación y según informe de INEI de cada 100 personas 93 tiene acceso a Internet, redes sociales, páginas web, etc. Lo cual hacer que las personas dejen evidencia digital en las redes de las conductas ilícitas, de modo que el Ministerio Público debe contar con la implementación adecuada para afrontar los nuevos retos. (INEI, ver anexo 2).

El Ministerio Público a nivel nacional carece de una implementación tecnológica para dar un tratamiento adecuado a las pruebas digitales, además carecen de software, equipos y salas especializadas de visualización para una adecuada transcripción de los medios digitales (Entrevista: Quiroz, 2018).

Pericia Informática es una disciplina criminalística de una secuencia de procedimientos con el objeto de investigar los sistemas informáticos de datos de hechos delictivos con relevancia jurídica para determinar través de los valores Hash la autenticidad o veracidad de un hecho. Este procedimiento se lleva a cabo en un laboratorio especial denominado Workflow. (Sebastián, 2009, p.3).

La ilicitud es la vulneración a la legitimidad de la prueba relacionada a las prohibiciones en la obtención de la prueba, su vulneración les convierte en prueba ilícita, por el cual el juez está prohibido en valorarla por ser atentatorio a los derechos fundamentales (Talavera, 2009, p.18). También el Tribunal supremo STC N° 2053-2003-HC/TC, define la prueba ilícita como la vulneración de la legalidad procesal y de los derechos fundamentales que deviene en la ineficacia de la valoración.

La Academia Nacional de la Magistratura en su publicación respecto a la prueba consignada en el Nuevo Código Procesal Penal, tipifica, “las prohibiciones probatorias están referida estrictamente a la legitimidad probatoria, asimismo advierte que la prueba irregular o defectuosa no es más que la prueba ilícita”. En la misma postura también se pronuncia la doctrina, al señalar que los inconvenientes de validez de la evidencia digital radican en la volatilidad, lo que implica, que es sensible a la manipulación y/o alteración, es decir, las evidencias digitales no gozaran de valoración en los procesos judiciales, si han sido obtenidos de manera ilícita, así como también, por falta de autenticidad e integridad. Las partes que lo invocan deberán probar su autenticidad con un informe de un peritaje de informática forense; en los casos de alteración o fotomontaje digital, las partes del proceso pueden presentar una oposición, así como el Ministerio Público y el Juez puede solicitar un examen por un especialista en pericia informática.

En esta sección de la investigación se muestra los resultados obtenidos para la unidad de análisis propuesta, lo que permitirá presentar una respuesta al objetivo planteado “Describir el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017”.

4.1.3. Resultados del análisis de la jurisprudencia.

Nuestra legislación nacional, el Tribunal Constitucional peruano se pronunció en su fundamentación “la actuación probatoria representa un derecho constitucional que consiste en el respeto de los derechos fundamentales y al ordenamiento jurídico, de modo que, en la obtención, recepción, incorporación, y valoración se debe tomar en cuenta no transgredir este precepto constitucional”. Este colegiado refiere, para que la prueba sea legítima debe cumplir dos aspectos

esenciales, primero la obtención de la prueba debe adquirirse bajo el respecto de los presupuestos constitucionales, vale decir, con el respeto estricto de los derechos fundamentales, y como segundo aspecto que su obtención no transgredan el ordenamiento jurídico, es decir con respeto a las normas y leyes establecidas; sólo cumpliendo estos dos requisitos la prueba será legítima (STC. N° 1014-2007-PHC/TC, f.15).

Invalidez de la prueba, no genera efectos las evidencias digitales obtenidas directa o indirectamente con evidente vulneración de los derechos protegidos, los que concretamente este órgano constitucional protege los derechos tales como, el derecho al secreto de las comunicaciones, secreto financiero, a la intimidad de las personas, estos son los derechos que se deben ponderar al momento de valorar los medios probatorios”. El tribunal refiere que los derechos constitucionales merecen una ponderación de máxima protección frente a los demás derechos, en tanto los operadores jurídicos deben garantizar el respeto de los derechos consagrados y además son los encargados de aplicar la teoría de la exclusión probatoria (STC. N.º 1915-2005-PHC/TC, f.j9).

En el caso específico de la ilicitud en la obtención prueba digital con vulneración de derechos fundamentales, que hemos conocido por la prensa mediática, fue la absolución del caso de Alberto Quimper, la Corte Suprema de Justicia en la sentencia absolvió, señalando que la prueba digital (audio) materia de acusación, había sido obtenido con vulneración a sus derechos fundamentales, por lo tanto, era prueba ilícita o prohibida. Lo que implica de ninguna manera se puede valorar las pruebas obtenidas con vulneración a los derechos constitucionales, el audio que se utilizó en el proceso fue una grabación de una interceptación telefónica, es decir, fue una evidencia digital, lo cual no fue valorado por el juez, por lo que en su obtención se vulneró el derecho al secreto de las comunicaciones, en consecuencia, se excluyó porque se consideró como una prueba ilícita (STS N.º 00655-2010-PHC/TC).

Según la posición del Tribunal Constitucional, el derecho a la presunción de inocencia se halla de un principio, incluso teniendo una relación directa con el derecho de dignidad humana tipificado en el Artículo 1º de la norma fundamental,

así como en el principio pro hómine que es una categoría de los Derechos Humanos [STC 10107-2005-PHC/TC]. En esta misma perspectiva la prueba digital tiene las mismas prerrogativas que la prueba tradicional, es decir, representa la garantía constitucional de la presunción de inocencia, que deben ser valorados por el juzgador dentro de la etapa de juicio de un proceso judicial.

4.1.4. Resultado de posición de los expertos.

Tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal Del 2004 de manera puntual y específica No existe, no hay regulación actual como prueba digital, sin embargo el Art. 185 del código procesal penal reconoce al contenido de un audio visual o audio grabado como prueba documental, si entre las fuentes de prueba de un hecho ilícito se encontrara un audio, o un video grabación u otro soporte digital o electrónico, simplemente el desahogo probatorio o actuación probatorio se efectúa en observación del artículo 382 del código procesal penal del 2004. Asimismo El Ministerio Público a nivel nacional carece de una implementación tecnológica para dar un tratamiento adecuado a las pruebas digitales, además carecen de software, equipos y salas especializadas de visualización para una adecuada transcripción de los medios digitales (Entrevista: Quiroz, 2018).

El Nuevo Código Procesal Penal del 2004, señala en el Art. 185 de pruebas documentales, dentro de ello se considera los documentos, audios, videos y todo medio electrónico, es decir el todo tratamiento digital ingresa a por ese tratamiento, pero exclusivamente un tratamiento especial en Código Procesal Penal no está establecido (Entrevista: Zavala, 2018).

La División de Investigación de Delitos de Alta tecnología de la Policía Nacional, el analista en peritaje de informática, sostiene si cuenta con instrumentos técnicos y un laboratorio equipado para determinar: Donde se almaceno o publico la información, cuando, es decir la fecha en la que se borró o publico la información, como se almaceno y publico la información, incluso detecta los sectores dañados del dispositivo en caso de pérdida de datos, etc. Los resultados de los informes deben estar con los formularios A6 y A7 debidamente rotulados y debe estar en cadena de custodia. El procedimiento es a los discos duros se extrae un imagen

forense al cual se le aplica el HASH que consiste en un algoritmo matemático que asigna un Código Valor que Autentica el contenido de la información. El resultado depende del caso, si es sencillo o complejo, incluso desde 24 horas se puede entregar los informes periciales. Sugerencia a todos los agraviados que cuenten con evidencias digitales, cuyo contenido estén en algún dispositivo electrónico, tales como: USB, CD, DVD, Tablet, Pc, Teléfono móvil, cámara digital u otro. No eliminar las evidencias de los dispositivos conservarlos, hasta interponer la denuncia, asimismo ofrecer como medio de prueba el mismo aparato original como prueba del delito. Asimismo los informes periciales que se practicaron en esta institución el 100% han sido valorados por el Juez, incluso después del debate de contra peritaje de parte, contamos con laboratorios acorde con la tecnología; dado que los delitos informáticos han evolucionado, nosotros somos policías que custodiamos el ciberespacio. . En el caso de que la evidencia se encuentre en algún medio electrónico como email, pagina web, twitter, facebook, whatsapp, u otros. Transcribir el contenido en un soporte de papel, porque ahí se encuentran todos los detalle de los datos como fecha y hora de envió, destinatario, emisor, etc. El cual será corroborado con un peritaje para identificar la autenticidad (Entrevista: Zababuru, 2018).

Según Paz *Rubio*, sostuvo que la interpretación extensiva de la prueba prohibida consiste “en una desmesurada ampliación del ámbito de la prueba prohibida”. Lo que refiere el autor es que, la prueba prohibida o llamada prueba ilícita en nuestro país, según el autor debe ser interpretada de manera amplia, lo que implica que no debe dejar de sancionar al responsable del hecho, para ello, incluso propone excepciones que se debe tomar en cuenta al momento de valorar, tales como el grado de afectación, la magnitud del hecho, ponderación de intereses, grado de complejidad del problema, entre otros.

Asimismo el doctrinario Jurista, sostiene, que la obtención de pruebas con violación a los derechos fundamentales de la persona, no puede tener eficacia alguna en el proceso. No puede ser objeto de valoración en el proceso, por lo que no constituye en sentido estricto prueba judicial válida, por lo que, debe reputarse inexistente, como tal, establece tres criterios: a) es insubsanables, esto es, una prueba obtenida con vulneración de derechos fundamentales, no puede ser

convalidada por ningún otro medio, dado que ya incurrió a la ilicitud; en este caso opera la “regla de exclusión” es imperativa. b) la ineficacia de la prueba no trasciende al plano fáctico, lo que significa que, si bien los hechos descubiertos inconstitucionalmente no sirven para sustentar una prueba válida, ello no significa que no existieron en la realidad o que son otros distintos, de suerte que eventualmente es posible tanto a su acreditación por otros medios de prueba (v. gr.: confesión). c) excepcionando la prueba independiente, por lo general la exclusión se extiende a todas aquellas evidencias conseguidas o practicadas de forma ilícita que se basan, derivan o tienen su origen en informaciones o datos conseguidos en la práctica de una diligencia inconstitucional (Muñoz, s/f).

El pronunciamiento refiere, a que tanto la prueba tradicional como las pruebas electrónicas o digitales en su obtención no deben vulnerar los principios y derechos fundamentales, asimismo deben haber sido obtenidos bajo el conducto regular del respeto a los procedimientos y protocolos de ley, de caso contrario sería una prueba irregular. Sin embargo existe un conjunto de excepciones a la regla de exclusión de valoración probatoria, los cuales son cinco: primero es la fuente independiente, el descubrimiento inevitable, segundo es la buena fe, tercero es la infracción constitucional beneficiosa para el imputado, cuarto el principio de proporcionalidad o de ponderación de intereses en conflicto, asimismo el nexo causal atenuado del hecho, quinto la destrucción de la mentira de la persona imputada y sexto es la teoría del riesgo y la doctrina de la eficacia de la prueba ilícita para terceros o la infracción constitucional ajena.

4.1.5. Interpretación y análisis de las entrevistas.

La información recopilada a través de las técnicas e instrumentos de la entrevista a expertos operadores del derecho en temas de manejo de la prueba digital, básicamente a los de la Fiscalía Provincial Penal Corporativa de Ventanilla, y para complementar del Callao, de la Corte de Lima Norte, Perito de la División de investigación de Delitos de Alta Tecnología Lima y Abogados Litigantes y Docentes, que luego se analizó e interpretó, con el fin de dar respuesta a los objetivos planteados. En tal sentido los resultados han sido interpretados en función de la opinión emitida por cada sujeto de estudio, a continuación, se describe:

De la aplicación del instrumento con relación al objetivo general, respecto a la pregunta¹ se obtuvo el siguiente resultado:

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?

Interpretación

Todos los entrevistados manifiestan que la prueba digital no tiene un tratamiento especial en Nuevo Código Procesal Penal del 2004, sin embargo su regulación está bajo la observancia del Art. 185^o, considerada como pruebas documentales; es decir, toda evidencia electrónica, tanto como mensajes a través de email, Cloud Computing, imágenes, audio, video, u otro soporte digital son considerados como prueba documental. Si entre las fuentes de prueba de un hecho ilícito se encontrara evidencias digitales, la actuación probatoria se efectuara bajo la observancia del Art. 382 del Nuevo Código Procesal Penal.

Análisis

Del análisis de las respuestas de los expertos podemos concluir, que efectivamente no existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal, implica que las pruebas ofrecidas por la partes pueden ser impugnadas debido a falta de un manejo para su valoración y eficacia probatoria.

2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?

Interpretación

La mayoría de los entrevistados sostienen que las evidencias digitales obligatoriamente debe entrar en cadena de custodia, para su conservación y custodiar, de manera que se pueda mantener la originalidad, para evitar la manipulación; luego el Ministerio Público debe enviar a la DIVINDAT para una pericia de informática forense a fin de obtener un código valor Hash de autenticidad e integridad, de manera que se pueda presentar a la audiencia de debates de juzgamiento para su valoración y no sea producto de exclusión probatoria.

Análisis

Del análisis de la postura de los expertos podemos concluir, para la inclusión de la prueba digital en la fase probatoria; es indispensable que la prueba entre en cadena de custodia por su alto grado de volatilidad, luego debe ser sometido a una pericia de informática forense de aplicación de Código valor Hash, el cual garantizara la autenticidad para una valoración eficaz.

3. ¿El Ministerio Publico cuenta con la implementación tecnológica suficiente para brindar seguridad y custodia a las pruebas digitales ofrecida por las partes?
¿Por qué?

Interpretación

La mayoría de los entrevistados sostienen que el Ministerio Público de Ventanilla no cuenta con los recursos suficientes para implementar con recursos tecnológicos para brindar un tratamiento adecuada a las pruebas digitales, y todas las pruebas que necesita pericia lo envían a la Av. España a DIVINDAT de la Policía. No tenemos software que permita identificar la originalidad de los medios digitales.

Análisis

De la opinión de los especialistas podemos concluir que el Ministerio Publico no cuenta con una implementación tecnológica adecuada, para brindar un tratamiento a las pruebas digitales ofrecida por las partes, y el mismo hecho de enviar al DIVINDAT genera una afectación con el plazo de la investigación y una demora y estrés en el agraviado.

4. ¿El Ministerio Publico cuenta con salas de visualización de video, audio, foto y otros documentos digitales que permita su transcripción confiable de la prueba digital?

Interpretación

La mayoría de los Jueces y Fiscales de Ventanilla afirman que el Ministerio Publico no cuenta con salas de visualización, de fotos, reproducir audio, y otras evidencias digitales, por lo que se ven obligados a realizar las transcripción digitales

a soporte de papel, desde su computadora personal de su oficina, las mismas que incluso no cuentan con audio y menos una buena resolución, motivo por el cual no se aprecian bien los videos.

Análisis

De la entrevista de los fiscales de Ventanilla, se concluye que el Ministerio Publico de ventanilla no cuenta con una sala adecuada para la visualización de pruebas digitales, lo que afecta el Derecho a ofrecer los medios probatorios, que es un Derecho Constitucional.

5. ¿Cuáles son las instituciones anexos al Ministerio Publico encargados de practicar la pericia de informática forense y cuál es el tiempo de resultados?
¿Cuál es su sugerencia?

Interpretación

La mayoría de los entrevistados señalaron que existe un centralismo en Lima sobre el peritaje, todas las pericias del a nivel nacional se lleva a cabo en la capital, específicamente en la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú, lo que afecta los plazos del proceso por la distancia y también la carga procesal del mismo centro de peritaje.

Análisis

De la opinión de los expertos se concluye que existen dos entidades anexos al Ministerio Publico para practicar peritajes, el DIVINDAT de la Policía Nacional y el Centro de Peritaje del Ministerio Público, que queda en la Av. Aramburu. Pero para el caso de pericia de informática forense el único y más implementado es la División de Investigaciones de Delitos de Alta Tecnología de la Policía. Motivo por el cual existe un centralismo, por lo que es el único a nivel nacional.

6. Cuales son los requisitos que debe cumplir una prueba digital para su admision e incorporacion al proceso? ¿Cuáles son?

Interpretacion

De la entrevista a los expertos la mayoría señalaron que las evidencias digitales para tener una validez en la sede judicial debe ser examinada por un perito informático, luego debe ser incorporada a la estación procesal a través de un debate en audiencia pública en el cual el perito ratifica, sometidos al derecho contradictorio de los peritos de parte, cumplido estas fase la valoración y producción de la prueba queda a discrecionalidad del juez.

Análisis

La conclusión es que toda prueba digital para su admisión e incorporación al proceso no debe haber afectado los Derechos Fundamentación en su obtención, además debe someterse a un examen de pericia informática, de manera que se pueda garantizar la valoración y eficacia procesal.

7. Según su experiencia y análisis probatorio ¿Cuáles son los problemas más comunes que impiden la valoración de la prueba digital? ¿Por qué?

Interpretación

La mayoría de los Jueces y Fiscales coincidieron que los problemas se presentan en la obtención, muchas veces los agraviados lo borran por temor a represalias, algunos solo presentan un pantallazo de WhatsApp, así como también no preservan el mismo equipo donde se encuentra la evidencia, son los problemas más comunes que afectan y también los problemas se presentan en la audiencia de visualización para su transcripción en acta, por falta de una buena implementación tecnológica para el tratamiento de las pruebas digitales.

Análisis

Podemos concluir afirmando que los agraviados no están preparados en la obtención de las pruebas digitales, y menos el Ministerio Publico no cuenta con la Implementación, razón por la cual existe un conjunto de problemas de impugnación probatoria que impide su valoración.

8. ¿En qué fase del proceso se ve disminuida la eficacia jurídica de la prueba digital? ¿Por qué?

Interpretación

La mayoría de los entrevistados señalaron que la fase en la que se ve disminuida la eficacia jurídica de prueba digital es en la etapa intermedia, con el control de acusación y también en el juicio oral, con el debate contradictorio de la prueba pericial, que da lugar al contraperitaje, objeciones e impugnación que puede originar su exclusión.

Análisis

Del análisis de la entrevista podemos concluir la fase en la prueba digital pasa un control estricto es en la etapa intermedia, donde es sometido a un debate de contradicción e impugnaciones por parte del abogado de la defensa. En el cual se pueden dar dos condiciones, uno su incorporación a juicio para su valoración o en todo caso su exclusión por tratarse de una prueba ilícita o irregular.

9. ¿Cuáles son las causales para la exclusión de la prueba digital? ¿Por qué?

Interpretación

Los expertos coincidieron en su mayoría, que las causales para la exclusión de la prueba digital es ilícita cuando en su obtención haya afectado uno derechos fundamentales, motivo por el cual el Juez según el Art. 159 del Código Procesal Penal está impedido de valorar, dado no podrá utilizar, directa o indirectamente, las fuentes o medios de prueba obtenidos con vulneración de los derechos fundamentales. Otro de las causales también se presenta cuando la prueba es irregular, por lo que en su actuación procesal no se respecto los procedimientos establecidos.

Análisis

Los causales para la exclusión de la prueba digital son dos, uno es cuando en su obtención afecto uno de los Derechos Fundamentales, en ese caso el Juzgador está impedido de valorar según la prohibición del Art. 159 de CPP y otro de los factores cuando en la actuación haya incurrido en alguna irregularidad procesal.

4.1.6. Resultados de las Entrevistas

Para culminar los resultados de la investigación se presentarán el análisis de la técnica de la entrevista aplicada. Este instrumento permitió interpretar la información de manera sistemática y ordenada. Asimismo dicha investigación permite conocer el modo de interacción de las personas agraviadas que acuden al Ministerio Público, lo que piensan, opinan, sienten, esperan, de la justicia. (Visauta, 1989, p. 259).

En tal sentido consideramos se aplicó esta técnica con el objetivo de dar respuesta y confirmar los supuestos planteado en esta investigación. Los instrumentos se aplicaron del 10 junio al 30 de julio del año 2018, el cual estuvo dirigida Jueces, Fiscales, Peritos y Abogados de la Fiscalía Provincial Penal Corporativa de Ventanilla, que a continuación detallo su perfil profesional:

La entrevista realizada entrevista de fecha 22 de junio de 2018. Juez Superior del 4to Juzgado Penal de Reos en Cárcel de la Corte Superior de Lima Norte, Expositor Internacional del Colegio de Abogados, Profesor de la Academia de la Magistratura, y Autor de distintas publicaciones de textos de Derecho; asimismo la entrevista realizado al Juez Superior del 4to Juzgado Penal de Investigación Preparatoria de Proceso Inmediato de la Corte Superior del Callao, Expositor del Colegio de Abogados del Callao; al Analista en sistema de fecha 22 de junio de 2018. *Perito Analista* de la División de Investigaciones de Delitos de Alta Tecnología del Perú (DIVINDAT) de la estructura orgánica de la DIRINCRI – PNP encargado de custodiar y patrullar el ciberespacio respecto de los delitos informáticos; Perito Informático Perú expertos en peritaje de informática forense representado por la empresa; fiscales titulares y adjuntos de la Segunda Fiscalía Penal Corporativa de Ventanilla, Asistente de la Primera Fiscalía Provincial Penal Corporativa de Ventanilla; Asistente de la Quinta Fiscalía Provincial Penal Corporativa de Ventanilla. Provincia Constitucional del Callao; Fiscal Titular Provincial de la Cuarta Fiscalía Provincial Penal Corporativa de Ventanilla. Provincia Constitucional del Callao, Constitucional del Callao. Fiscal Adjunto Provincial de la Cuarta Fiscalía Provincial Penal Corporativa de Ventanilla. Provincia Constitucional del Callao,

Constitucional del Callao; Fiscal Adjunto Provincial de la Cuarta Fiscalía Provincial Penal Corporativa de Ventanilla. Provincia Constitucional del Callao, se obtuvo los siguientes resultados:

La mayoría de los entrevistados coincidieron en que la prueba digital no solo es insuficiente, sino, no cuenta con un tratamiento especial en el Nuevo Código Procesal Penal del 2004, dado que el manejo se lleva a cabo bajo la observancia del Artículo 185º del Código Procesal Penal como prueba documental.

La mayoría de los expertos sostuvieron que, el Ministerio Público cuenta con una insuficiente implementación tecnológica para brindar un manejo adecuado que garantice la valoración de la prueba digital y en cuanto a los peritajes de informática forense están centralizados a nivel nacional en la Av. España en la División de Investigación de Delitos de Alta Tecnología.

Los entrevistados sostuvieron que los procedimientos para la incorporación, primero que la obtención de las pruebas digitales debe ser bajo la observancia y respeto de los derechos fundamentales, luego que entre en cadena de custodia, y sea examinada por un perito profesional en informática forense, que tenga un código valor Hash, una vez cumplido este protocolo su incorporación y valoración están asegurados, porque va ponderar la autenticidad y licitud en el debate probatorio del juicio oral.

Los especialistas sostuvieron que existe dos aspectos que impiden la valoración de la prueba digital, el primero es en la obtención se haya vulnerado los Derechos Fundamentales y segundo es cuando en su actuación haya incurrido a una irregularidad procesal, en cualquiera de esos dos aspectos, el Juez está impedido de valorar, tal como lo dispone el Artículo 159º de Código Procesal Penal.

En conclusión, a partir de los resultados de las entrevistas podemos afirmar que los supuestos quedan demostradas, toda vez que la mayoría de los entrevistados afirman que no existen un tratamiento especial de la prueba digital en el Nuevo Código procesal Penal del 2004; asimismo señalaron que el Ministerio Público no cuenta con una suficiente implementación tecnológica para garantizar la autenticidad de la prueba digital, tanto así, que a falta de cadena de custodia, o a

falta de peritaje en informática forense y la afectación de los Derechos fundamentales en la obtención de la prueba digital acarrearía el impedimento, en la incorporación y exclusión probatoria, por considerarse como prueba ilícita o irregular, afectando a un conjunto de personas agraviadas.

V. Discusión

En esta parte se compara y contrasta los antecedentes con los resultados de la nueva investigación y con el aporte de los expertos entrevistados se obtendrá nuevos resultados que permitirán determinar los objetivos planteados. Asimismo, se presentaron un conjunto de debilidades los que dificultaron la investigación.

Del contraste de los trabajos previos con los nuevos resultados de la investigación, respecto al *objetivo general*: En los resultados obtenidos en el antecedente del trabajo de León, quién determino que el manejo de custodia sobre el contenido digital no es suficientemente seguro, dado que los profesionales de Derecho tanto, jueces, fiscales y abogados no están capacitados en el manejo y procedimientos de las técnicas digitales (p.95). Asimismo, Mata, determinó que el derecho penal no ha tenido más remedio que volverse permeable al avance tecnológico y ceder a su empuje abriendo espacio a la informatización de sus contenidos.

Actualmente tenemos los Correos electrónicos (e-mails), publicaciones a través de páginas web, Whatsapp, imágenes digitales, videos conferencias a través de skype, entre otros que constituyen elementos digitales, también denominado prueba electrónica, las mismas que necesitan un tratamiento especial para una valoración eficaz (p.130). No solamente el manejo de la evidencia digital es insuficiente, no existe un tratamiento especial en el Nuevo Código Procesal Penal del 2004, respecto al manejo de evidencias digital o electrónica. El presente trabajo de investigación releva la postura anterior puesto que, no solo es insuficiente, sino que Nuevo código Procesal Penal del 2004 no tipifica una regulación especial al tratamiento de las evidencias digitales, solo limitándose al Artículo 185º considerando a la evidencia digital dentro de las pruebas documentales.

Del mismo modo los entrevistados tanto el Juez superior de Reos en Cárcel de la Corte Superior de Lima Norte, y el Juez Superior de Investigación Preparatoria de la provincia del Callao, y los fiscales de Ventanilla, coincidieron en señalar que el tratamiento de la evidencia digital en Nuevo código Procesal Penal, como tal no existe, sin embargo, el Art. 185 del Nuevo código Procesal Penal, reconoce a las pruebas digitales dentro de la prueba documental. Si entre las fuentes de prueba de un hecho ilícito se encontrara en un audio, video u otro soporte digital, la

actuación probatoria se efectuará bajo la observancia del Artículo 382 del Código Procesal Penal, es decir como una prueba material lo que implica, que serán exhibidos en el debate para ser examinados por las partes. He aquí el gran problema de las pruebas digitales necesitan un tratamiento especial, dado que, en esta fase del proceso una de las partes podría impugnar cuestionando la legitimidad e integridad de las evidencias digitales y pueden ser excluidas del proceso, si previamente el Ministerio Público no ha cautelado a través de un tratamiento especial para su valoración.

Asimismo el especialista de la División de Investigación de Delitos de Alta Tecnología – PNP en peritaje de Informática Forense, sostuvo, que el Ministerio Público al recibir las pruebas digitales como evidencia del delito debe derivar a DIVINDAT de la Av. España, que es la unidad institución a nivel nacional encargada de practicar pericias, para lo cual se debe seguir los siguientes procedimientos técnicos: estar debidamente rotulado y lacrado para evitar su adulteración y contaminación, contar con la cadena de custodia, contar con la autorización del Juez a través de una resolución judicial, de este modo se estaría garantizando el derecho a presentar y valorar los medios probatorios tipificados en los Art. 139, 3 y Art. 3 de la Constitución y así como también el Art. IX.1 del Nuevo código Procesal Penal el Derecho a utilizar los medios de prueba pertinentes. De no tomar las medidas en cuanto al tratamiento adecuado de las pruebas digitales, el Ministerio Público expondría en riesgo de vulnerabilidad los principios de ofrecer los medios probatorios (Art. 155.2), el derecho a que se admitan (Art. 155.2, 385), derecho a recepcionar las pruebas (Art. 375), y el derecho a que se actúen y valoren.

Tal como lo afirma, Bravo (2010), en su conclusión, la prueba dentro de cualquier proceso es fundamental, porque de ella se va a obtener la verdad procesal; de modo que el Juez de acuerdo al principio de inmediación, conoce de manera directa el ofrecimiento de los medios probatorios y en base a ello se formara una convicción y, su decisión será en base a las reglas de la sana crítica y las máximas de la experiencia, declarando la responsabilidad penal del acusado. Finalmente el mismo perito de acuerdo a su experiencia sugiere a los agraviados que cuenten con evidencias digitales, cuyo contenido estén en algún dispositivo

electrónico, tales como: USB (Universal Serial Bus), CD (Disco Compacto), DVD (Disco Video Digital), Tablet, Pc, Teléfono móvil, cámara digital u otro., no eliminar de los dispositivos, conservarlos, hasta interponer la denuncia, y al momento de ofrecer se debe adjuntar el mismo aparato original cuyo contenido contiene los hechos del delito.

También sugiere de contar con evidencia que se encuentre en algún medio o dirección electrónica como email, pagina web, Twitter, Facebook, WhatsApp, u otros. No borrar y transcribir el contenido en un soporte de papel, por lo que, es donde se encuentra los detalles de hecho ilícito, tales como fecha y hora de envío, destinatario, emisor, receptor, etc. El cual será corroborado con un peritaje para identificar la autenticidad. Por las razones expuestas por los especialistas y operadores en el Derecho, las evidencias digitales necesitan de un tratamiento especial, de modo que el Ministerio Público cuente con la implementación necesaria, para garantizar la autenticidad e integridad de las evidencias de digitales y así asegurar su valoración dentro del proceso.

El Jurista y reconocido Bueno de Mata (2014), sostuvo que el tratamiento de las pruebas digitales está considerado como *numerus apertus* vale decir, que la prueba digital está considerada como un medio de prueba con independencia y autonomía que no está sujeto a la tipificación de algún Artículo del código penal, dado que su tratamiento procesal carece de regulación (p.103).

Los entrevistados sostuvieron que no existe una regulación sobre el tratamiento de la prueba digital en el nuevo Código Procesal Penal, el cual sería una afectación al derecho a ofrecer los medios probatorios y así como también un impedimento al derecho a conocer la verdad, dado que si no se les da un tratamiento adecuado a las pruebas serán pasibles de ser excluido del proceso y no valorados por el juez. En este caso muchos delitos quedarán impune y las personas agraviadas sin justicia atentando el Artículo 1º de la Constitución que señaló la defensa de la persona humana y su dignidad.

Tal como lo ha señalado el Máximo Tribunal en la Jurisprudencia vinculantes Exp. N°010-2002-AI/TC el derecho fundamental a probar es una garantía constitucional que representa uno de los elementales esenciales del derecho

fundamental al debido proceso, por ende, al derecho a la defensa y a la tutela procesal efectiva. En el mismo criterio también se ha pronunciado el Acuerdo Plenario Extraordinario N°1-2011/CIJ-116, al sostener que “la valoración de la validez de la prueba debe realizarse sin limitaciones ni control alguno bajo la observancia de las garantías constitucionales”.

Enseguida se tomará en cuenta el contraste del objetivo específico uno y los nuevos resultados con respecto a los trabajos previos de la investigación. En ese mismo orden de ideas Sequeiros, en su tesis sustentadas en la Universidad Nacional Huánuco facultad de Derecho y Ciencias Políticas, concluye señalando, la naturaleza virtual de los delitos informáticos puede generar lagunas en la tipificación y subsunción entre el hecho del delito y encuadramiento de la norma penal”; el presente estudio releva la postura de la conclusión del investigador considerados en los antecedentes, puesto que, los delitos informáticos pueden generar lagunas en la tipificación y subsunción del hecho del delito.

Estos vacíos de la norma penal, se presenta precisamente porque las evidencias digitales no tienen un tratamiento especial en el Nuevo código Procesal Penal, por el multiuso de la informática que rompe todo tipo de protocolo, más aún si no cuenta con una regulación especial; configurándose en distintas formas delitos informáticos; motivo por el cual se debe crear un procedimiento especial respecto al manejo de la prueba digital que afronte este problema social del contexto virtual.

En consecuencia, el Estado, los operadores jurídicos deben crear instrumentos de control y seguridad en el uso de la informática. En esta misma línea el Dr. William sostuvo que; el Ministerio Público no cuenta con herramientas para la guarda, también las grabaciones en audio y en video no cuenta con los instrumentos tecnológicos para dar un tratamiento a las pruebas digitales, asimismo necesariamente en observancia del Artículo 382 del Nuevo código Procesal Penal, requiere que, entre la cadena de custodia, que tenga procedimientos técnicos y el ministerio público puede custodiarlos y conservarlos. Que bien podían estar en el laboratorio, iniciado la etapa intermedia debería estar en manos del ministerio público o también debería estar en depósito que el ministerio debe implementar.

Sin embargo, la propia institución como persecutor del delito encargado de la búsqueda de la verdad no cuenta con la implementación para el manejo de la prueba digital. También el Dr. Zavala coincidió con afirmar que existe una insuficiencia respecto a la implementación tecnológica en las fiscalías a nivel nacional para el tratamiento de las evidencias digitales (no cuenta con sala de visualización de pruebas digitales, solo lo realizan en la computadora de su escritorio) y lo más preocupante existe un centralismo a nivel nacional para practicar el examen de pericias; no solamente para las pruebas digitales, sino también para las tradicionales. Motivo por el cual las evidencias de todo tipo de delito que requerirá una pericia el ministerio público de todas las provincias se ven obligadas enviar hasta la capital de Lima, específicamente a la División de Investigación de delitos de alta tecnología –DIVINDAT, PNP ubicado en la avenida España, asimismo advierte que no existe ninguna sede en Lima Metropolitana y menos en la Provincia Constitucional del Callao.

En esa misma línea el fiscal sostuvo que el Ministerio Público no cuenta con los recursos suficientes para implementar con tecnología de punta para el tratamiento de la prueba digital, sin embargo, hace 15 días se ha implementado una sala de visualización para las audiencias de visualización y transcripción en soporte de papel (acta de transcripción) en presencia de las partes. Cabe señalar que esta sala de visualización no se encuentra en este local, sino en la otra sede.

Porque antes de ello toda la visualización lo realizábamos en la computadora de mi oficina. Frente a esta realidad que se observa en el Ministerio Público, que no solamente el Ministerio Público adolece de implementación tecnológica, sino también, en la práctica judicial no estamos capacitados en el sistema de acceso a las pericias de estas naturaleza, dado que puedan quedar impunes por falta de conocimientos y/o capacitación de los operadores de derecho.

Principalmente por el desconocimiento, es decir los magistrados como los operadores de derecho no son expertos en el manejo de este sistema digital, excepcionalmente se han recibido capacitación en algunos eventos sobre el manejo de información de última generación, pero no está generalizado, y

concluye señalando, el manejo de las evidencias digitales es un lenguaje técnico especializado que requiere de asesoría de parte de las instituciones especializadas.

Por su parte el Juez vigente también complementa y recomienda a todos los profesionales abogados, fiscales y jueces, señalando lo siguiente. Todos tienen que tener conocimiento de lo que hoy día la tecnología ha revolucionado, estamos viviendo un gobierno digital de una nación; si es que no lo implementan es responsabilidad de sus autoridades, si esta vigente el código penal a partir del 1º de julio del 2004, lo único que tiene que hacer es prepararse, el problema es que esta materia es un poco desfasada para algunos profesionales que tienen edades más de 40 o 50 años no la entienden, pero no es imposible de entender, lo tiene que hacer es aprender, incluso ahora se habla de un examen que lo realiza un antropólogo y se habla de las pruebas de análisis facial y somatológico, entonces si se tiene ese tipo de reconstrucciones de cotejo y comparaciones y gracias a las cámaras municipales y vecinales, la grabación no permite ver los rostros, sin embargo los antropólogos están haciendo reconstrucciones a través de posibles características y para ello tenemos que conocer de evidencia digital, porque se va a tener que hacer una interpolación de traslado de información de un soporte a otro, ahí va a ver contaminación, al existir una serie de actos netamente técnicos, el abogado, el fiscal y el juez debe conocer de lo contrario, cabe la posibilidad de que el perito también lo manipule, para que los datos del posible sujeto coincida con la imagen física que se ha grabado, entonces acá se requiere conocer mucho sobre la evidencia digital.

Continuando la discusión se tomará en cuenta el contraste del objetivo específico del estudio con relación a los antecedentes y los nuevos resultados obtenidos: Continuando con la discusión de los expertos, Pareja en su Tesis sustentada sobre la admisión de la prueba, concluye como antecedente, señalando, los derechos fundamentales constituyen la piedra angular sobre la cual se sostuvo todo ordenamiento jurídico; el presente estudio sobre la evidencia digital coincidió con la postura de la conclusión del antecedente antes mencionado, toda vez que, cualquier prueba obtenida con vulneración de los derechos fundamentales, carecerá de valor probatorio y por ende es susceptible de exclusión.

probatoria. En ese mismo orden de ideas, Pereira, en su Tesis sobre *soportes informáticos* sustentada en la prestigiosa Universidad pública de Girona de España; concluye que, las funciones de Hash constituyen una técnica informática de aseguramiento de la prueba digital, el cual se basan en la obtención de datos a través de una copia espejo, garantizando de este la autenticidad e integridad de las evidencias digitales a través de un código valor; según el autor estos procedimientos garantizan su incorporación la eficacia probatoria, de caso contrario estará sujeto a la contradicción, incluso de ser posible la exclusión del proceso, ya sea como prueba ilícita o como prueba irregular.

Por su parte el actual Juez sostuvo que, las evidencias digitales al ser recolectadas y obtenidas en la investigaciones, tiene que ser descargada de la evidencia electrónico del soporte electrónico a través de un programa informático; el cual debe tener correspondencia con el soporte y con el programa que se utiliza para descargar los archivos de sus compartimientos, luego ser sometidos a un dictamen pericial informático, que tendrá que ser suscrito por una persona versada en materia de informática y que tenga expertise y haga explicación de todo lo que aparece en la memoria, del video, audio registro de imágenes, eliminadas, archivadas, incluso si alguno de sus compartimientos estuviera deteriorada, es decir todas las características y datos para que la autoridad lo pueda utilizar; el entrevistado aclara que conforme al Artículo 382., la prueba obligatoriamente tiene que entrar en cadena de custodia, dado que se tiene que observar preservar, conservar, custodiar, para que no sea alterado y goce de la originalidad para lograr el principio de mismidad de la evidencia. El magistrado vuelve advertir que si no se sigue estos los procedimientos la exhibición, autenticación, actuación, reproducción, y con el principio de contradictorio carecen de incorporación y valoración.

Además el especialista perito informático de DIVINDAT-PNP en la entrevista recomienda; que el Ministerio Público al recibir las pruebas digitales como prueba del delito debe solicitar a la Juez la autorización para un examen de pericia informático y luego deriva a la División De Investigaciones De Delitos De Alta Tecnología ubicado en la Av. España. Para lo cual debe tener en cuenta los siguientes procedimientos técnicos: como mínimo la prueba debe estar

debidamente rotulado y lacrado para evitar su adulteración, así como también debe contar con la cadena de custodia respectiva, contar con la autorización del Juez competente.

Del mismo modo declara que la División de Investigaciones De Delitos De Alta Tecnología, cuenta con implementación tecnológica para dar tratamiento adecuado a las pruebas; tales como recuperar información de las cuentas de Twitter, Facebook, correos electrónicos, páginas web, CloudComputing, llamadas telefónicas y entre otros dispositivos hardware como: disco duro, Pendrive, USB, teléfono móvil, cámaras digitales, etc. Y además se puede determinar cómo, dónde, cuándo se almacenó, la fecha en la que se borró o publicó la información; incluso detecta los sectores dañados del dispositivo en caso de pérdida de datos, etc. Agrega señalando que el 100% de las pericias prácticas han sido valoradas por el Juez, pese a contar con contra peritajes de parte, y resalta la gran importancia del Hash que consiste en un algoritmo matemático que asigna un código valor que autentica el contenido de la información.

Chavarry en su investigación sustentada en la Universidad Nacional de Trujillo; citada como antecedente concluye, en el Proceso Penal uno de los elementos de mayor relevancia está constituido por la prueba, consecuentemente su obtención debe realizarse con observancia de los preceptos de legitimidad, licitud y legalidad; y, fundamentalmente, con observancia del respeto de la persona humana; sin embargo el Dr. Racchumi Fiscal Provincia de Ventanilla, en la entrevista sostuvo las pruebas digitales a pesar de ser excluidas e impugnadas, es posible reiterar el ofrecimiento de los medios de prueba inadmitidos en audiencia de control invocando el inciso 3) del artículo 373, y el artículo 374 el fiscal durante el juicio podrá ampliar su acusación e introducir una prueba nueva.

En esa misma línea la Fiscal provincia adjunta de Ventanilla, sostuvo que la prueba digital siempre va a ser cuestionada por el defensor de la otra parte en el juicio oral, por tal razón es que debe cumplirse que en su obtención no debe afectar los derechos; de caso contrario será excluida ya sea como prueba ilícita o irregular. A manera de conclusión según los entrevistados Jueces, Fiscales y perito en informática, en su mayoría sostuvieron, la prueba digital debe tener seguir un

procedimiento acorde a la Ley, tanto en su obtención e incorporación para su eficaz valoración del juez, de lo contrario será excluido por contravención a los derechos fundamentales de la persona.

Respecto al contrato del objetivo específico tres con respecto a los antecedentes y los nuevos resultados obtenidos en esta investigación: Culminado con la discusión de los expertos, Baudelio en su Tesis sustentada en la Universidad Nacional de Trujillo sobre la prueba ilícita de los Petroaudios, concluye como antecedente, señalando, uno de los elementos de mayor relevancia para impartir justicia está constituido por la consistencia de la prueba, por ende su obtención, elaboración e incorporación debe estar sujeto bajo la observancia de los principios constitucionales de legitimidad, licitud y legalidad; asimismo el autor advierte que la actuación y valoración está condicionado a la credibilidad de los conocimientos técnicos y científicos de los profesionales expertos, y finalmente su valoración y eficacia depende del principio discrecional de los jueces, que consiste en la aplicación de las reglas de la sana crítica y las máximas de experiencia.

Tal como confirma el Juez de Lima Norte en la entrevista, se excluye la evidencia digital no prueba, desde ahora se llama evidencia, porque se convierte en prueba cuando el juez ha valorado; en caso de infracciones de los derechos fundamentales, conforme al Art.159 del Nuevo código Procesal Penal que señaló el juez no podrá utilizar, directa o indirectamente las fuentes y medios con vulneración a los derechos fundamentales. También el Juez de Investigación Preparatoria complementa, la exclusión probatoria tiene diversos controles, en la audiencia de control de la etapa intermedia las partes solicitan la exclusión de las pruebas por la mala producción, denominado como prueba ilícita por atentar contra los derechos fundamentales protegidos, también cuestionan como prueba irregular, por lo en el proceso no se respetó los protocolos y procedimientos procesales, aunque no es muy frecuente.

Precisamente al amparo de los derechos constitucionales el caso de Alberto Quimper fue absuelto a través de una sentencia como producto de la exclusión de la prueba ilícita por haber sido obtenido con vulneración de los derechos fundamentales para ser más específico por afectar el derecho al secreto de sus

comunicaciones. Sin embargo Duarte cita al reconocido Jurista Carlos Santiago Nino, en su Tesis titulada, *Valoración probatoria de los documentos audiovisuales*; en la Universidad Nacional Mayor de San Marcos, de la Facultad de Derecho, que concluyó, la filmación en documentos audiovisuales en la comisión de un delito no vulnera el derecho a la intimidad, precisando que el derecho a la intimidad comprende principalmente aquellas acciones privadas que no afecten o dañen a terceros, los cuales se suscitan fuera del ámbito del conocimiento de los demás.

En consecuencia las grabaciones ya sea en audio o video de un delito representa pruebas consistentes, útiles y pertinentes que acreditan los actos ilícitos, acto que debería ser sancionados, más aun cuando se trate de los intereses de Estado, en la misma línea se pronuncia el Jurista español Gálvez Muñoz respecto a la prueba ilícita; para lo cual se debe recurrir a las excepciones de la prueba ilícita, específicamente la ponderación de intereses en conflicto; de manera que para operativizar la ponderación ha planteado varios criterios, los cuales son: primero, la gravedad o entidad objetiva de la infracción; segundo, la intencionalidad del infractor; tercero, la naturaleza y entidad objetiva que tenga el hecho investigado por el infractor; cuarto, la dificultad probatoria; quinto, la naturaleza rígida o flexible del derecho fundamental afectado; sexto, la inevitabilidad o no del descubrimiento de la prueba por medios lícitos; y finalmente, las consecuencias de la aplicación de la regla de exclusión sobre otros bienes y valores dignos de protección (Aranzandi, 2003, pp.125-126).

Conuerdo con el jurista español en el sentido que las pruebas ilícitas de personas que cometieron delito contra el Estado y que represente delito debería de ser sancionado y no debe ser excluido como prueba ilícita, de lo contrario queda impune, y da pie a muchos funcionarios públicos a escudarse a la ilicitud de las pruebas. En estos casos como señaló el jurista debe aplicarse las excepciones de ponderación de intereses en conflicto y considerar los criterios de la gravedad, intencionalidad, dificultad probatoria, derecho afectado, inevitabilidad del descubrimiento y las consecuencias. De lo contrario la corrupción seguirá enquistado dentro del poder de la administración pública.

VI. Conclusiones

Primero

A pesar de que el Derecho Penal ha cedido la presión del avance tecnológico de la informática no existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004, ya que el manejo se da bajo la observancia del Art. 185º dentro de la prueba documental; es decir, las evidencias de los delitos que se cometen a través de los e-mails, publicaciones a través de páginas web, WhatsApp, redes sociales como Twitter, Facebook, video conferencias a través de Skype, entre otros que constituyen evidencia digital, lo que necesitan un tratamiento especial para su valoración eficaz; sin embargo los operadores del derecho tanto, jueces, fiscales y abogados litigantes no están capacitados en el manejo de procedimientos de las técnicas digitales; la regulación está fundamentada en la teoría analógica que considera a la prueba digital como semejante con la prueba documental, tipificado en el artículo 185º del Código Procesal Penal; es decir, todas las evidencias de mensajería electrónicas, evidencia digital cuyo contenido tenga como evidencias de hechos delictivos, son considerados como prueba documental, y su actuación probatoria se efectuara bajo la observancia del Art. 382 del Nuevo código Procesal Penal.

Segundo

El Ministerio Público no cuenta con la implementación tecnológica suficiente a nivel de las Fiscalías para dar un tratamiento adecuado que aseguren la valoración de las pruebas digitales (no cuentan con sala de visualización de video por lo que se ven obligados a visualizar las evidencias digitales en la computadora de su escritorio) debido a falta de presupuesto económico del Estado. En caso de necesidad de pericia informática existe un centralismo por lo que necesariamente se tiene que enviar a la División de Investigación de Delito de Alta tecnología DIVINDAT de la Av. España; es más los magistrados y operadores del derecho no están capacitados en el manejo de este sistema digital, lo que implica una falta de control de seguridad de la tecnología e informática que puede generar lagunas en la tipificación y subsunción entre el hecho del delito y encuadramiento de la norma penal; lo cual tienen que ver con el tratamiento adecuado de las pruebas digitales.

Tercero

Los procedimientos para la incorporación de la prueba digital son respetar los Derechos Fundamentales en la obtención de la prueba, solicitar la inmediata cadena de custodia, practicar la pericia informática, obtener el código valor Hash, respetar los plazos de la actuación procesal, entre otros, los que permiten la incorporación de la prueba digital y por ende garantizan la eficacia probatoria. La relevancia de los derechos fundamentales constituyen la piedra angular sobre la cual se sostiene todo ordenamiento jurídico, toda vulneración de estos derechos acarreará como consecuencia la exclusión probatoria. Lo que implica que toda evidencia digital al ser recolectada y obtenida dentro o fuera del proceso, tiene que ser descargada de la evidencia electrónico del soporte electrónico a través de un programa informático; el cual debe tener correspondencia con el soporte y con el programa que se utiliza para descargar los archivos de sus compartimientos, luego ser sometidos a un dictamen pericial informático de funciones Hash para obtener el código valor de autenticidad; luego ingresar a una cadena de custodia; dichos procedimientos permitirán la exhibición, autenticación, actuación, reproducción, y con el principio contradictorio se garantiza la incorporación para su posterior valoración.

Cuarto

La vulneración de los Derechos Fundamentales al secreto de comunicaciones, a la inviolabilidad de domicilio, a la intimidad personal y familiar y a la reserva financiera en la obtención de la prueba digital; así como también el incurrir en irregularidades en actuación procesal impide la valoración de la prueba digital; Motivo por el cual el Juez está impedido de valorar, tal como lo dispone el Artículo 159º sobre las prohibiciones de la valoración, advierte al juzgador, señalando el Juez no podrá utilizar, directa o indirectamente las fuentes y medios con vulneración a los derechos fundamentales. El impedimento también se puede invocar en la audiencia de control de prueba, así como también cuestionando como prueba irregular, por lo en el proceso no se respetó los protocolos y procedimientos procesales. Un ejemplo tenemos el caso del Sr. Alberto Quimper fue absuelto a través de una sentencia como producto de la exclusión de la prueba ilícita por haber sido obtenido con vulneración de los derechos al secreto de sus comunicaciones. Otra postura

encontramos en el jurista español Gálvez Muñoz, quien sostiene, en caso de las pruebas ilícitas, se debe recurrir a las excepciones específicamente a la ponderación de intereses en conflicto; y la manera de operativizar es considerando los criterios de la gravedad, intencionalidad, dificultad probatoria, derecho afectado, inevitabilidad del descubrimiento y las consecuencias. La postura del autor es lo apropiado, de lo contrario la corrupción seguirá enquistado dentro del poder de la administración pública, sobre todo la ponderación debe ser en personas que cometieron delito contra el Estado, que de ser sancionado y no debe ser excluido, de lo contrario queda impune, y da pie a muchos funcionarios públicos a escudarse a la ilicitud y queda impune los delitos.

VII. Recomendaciones

Primero

Teniendo en cuenta que la prueba digital no cuenta con un tratamiento especial en el Nuevo Código Procesal Penal del 2004, y su regulación está implícito dentro de la prueba documental tipificado en el Artículo 185º del Código Procesal Penal; sugerimos una regulación especial, sobre el tratamiento adecuado de la prueba digital, tal como sostiene el Jurista Bueno de Mata, por lo que la prueba digital es independiente y autónoma, implementando un laboratorio de pericia, pero con fiscales especializados, con la finalidad de garantizar la autenticidad y valoración procesal. Esta sugerencia encuentra su justificación en la inevitable informatización de este gobierno digital que ha cambiado nuestras vidas y el modo de comunicarnos, según encuesta del año 2017 reportado por INEI señaló que de cada 100 personas 93 usan la tecnología con acceso a Internet, lo que implica una interacción permanente que la delincuencia se ha estacionado en la red, producto de ello dejan evidencias de los actos delictivos en las redes sociales, correos electrónicos, páginas web, Cloud Computing, WhatsApp entre otros. Frente a esta realidad el estado todavía no ha implementado un tratamiento especial en el Código Procesal Penal respecto al manejo adecuado de las pruebas digitales; por lo que recomendamos también no eliminar las evidencias de los dispositivos, conservarlos, hasta interponer la denuncia, y al momento de ofrecer se debe entregar también el mismo aparato, lo cual también se debe transcribir el contenido en un soporte de papel (impresión).

Segundo

Sugerimos que el Ministerio Público gestione una partida presupuestal, tanto para equipos tecnológicos como para capacitación, con tecnología de punta que permita crear instrumentos de control y seguridad en el uso de la informática, con el objeto de mejorar tratamiento de la prueba digitales y el así también crear un órgano de peritaje de Fiscales en cada sede, y capacitar a los Fiscales y adjuntos de manera que se afronte este problema social del contexto virtual. La insuficiencia de recursos del Ministerio Público no ha permitido la implementación tecnológica para el tratamiento adecuado de la prueba digital, más aun siento el ente persecutor del delito en búsqueda de la verdad, y bagaje de evidencias de

evidencias delitos que circulan por la red, va en aumento los agraviados y cada vez más ofrecen las evidencias en las Fiscalías para acreditar los hechos ilícitos; sin embargo el Ministerio Público no están en la capacidad de dar respuestas a estos casos, puesto que no cuentan con sala de visualización de video, y menos otros equipos que aseguren la eficacia probatoria. Solo en casos complejos envían a una peritaje informática a la División de Investigación de Delito de Alta tecnología DIVINDAT de la Av. España; generando una demora en el plazo generando una afectación al agraviado.

Tercero

Sugerimos, que el Ministerio Público implemente tanto con equipos de última generación como implementación al personal, para que se garantice el derecho a que se valore las pruebas; de manera que se pueda asegurar la eficacia procesal de las pruebas digitales; dado que existe incumplimiento constante de los requisitos y procedimientos en la obtención de la prueba que vulnera los Derechos fundamentales, el no asegurar con la cadena de custodia, así como la falta de una pericia en informática forense por falta de implementación tecnológica, también las irregularidades en la actuación procesal son causales constantes que impiden la incorporación de la prueba digital. También es importante conocer estos dos supuestos: primero si la obtención de la prueba de delito se da por una de las partes intervinientes en la comunicación, ya sea tomando foto, enviando recibiendo mensaje, grabación de audio, video, etc.; entonces no existe vulneración de los derechos y tampoco se configura como prueba ilícita, en este caso la prueba sería legítima y su incorporación no sería materia de objeción. El segundo supuesto se da cuando no interviene ninguna de las partes, sino interviene un tercero ajeno en el cual observa el hecho delictivo y decide obtener ya sea mediante films, grabación de voz, interceptación telefónica, captura de pantalla, mensaje de texto, etc. La prueba obtenida por éste último si vulnera los derechos constitucionales de la persona, por tanto, es materia de exclusión probatoria.

Cuarto

Recomendamos que debe haber una modificatoria en el art. 159 del CPP en caso de la prueba ilícita, es decir, no debe afectar a los funcionarios públicos que han

sido elegidos por voto popular, cargo de confianza y cargos importantes en la Administración Pública, dado que la obtención de la prueba digital con vulneración de los Derechos Fundamentales o irregularidad procesal, son causales de impedimento de valoración de la prueba, en este caso, el Juez no podrá utilizar, directa o indirectamente las fuentes y medios con vulneración a los derechos fundamentales, y se ha dado en varios casos;. Tal como ocurrió en el caso del Sr. Alberto Quimper que fue absuelto como producto de la exclusión de la prueba ilícita por vulneración de los derechos al secreto de sus comunicaciones. La historia nos ha demostrado los vladivideos de montesinos, entre otros siguen impune escudándose en la prueba ilícita, pese a que el delito está demostrado de manera consistente en los audios y videos. Fundamento mi recomendación con la postura del jurista español Gálvez Muñoz, quien sostiene, en caso de las pruebas ilícitas, se debe recurrir a las excepciones específicamente la ponderación de intereses en conflicto; y la manera de operativizar es considerando los criterios de la gravedad, intencionalidad, dificultad probatoria, derecho afectado, inevitabilidad del descubrimiento y las consecuencias. La postura del autor es lo más atinado; de lo contrario, la corrupción seguirá enquistado dentro del poder de la administración pública, sobre todo la ponderación debe ser en personas que cometieron delito contra el Estado, que de ser sancionado y no debe ser excluido, de lo contrario queda impune, y da pie a muchos funcionarios públicos a escudarse a la ilicitud y queda impune los delitos.

VIII. Propuesta

Modificatoria de la prohibición de la prueba ilícita tipificado en el Código Procesal Penal del 2004, que señaló, el juez no podrá utilizar, directa o indirectamente las fuentes y medios con vulneración a los derechos fundamentales, en tanto debe excluida de la actividad probatoria; mi propuesta es una modificatoria en el Artículo 159º que se debe agregar el segundo numeral (2), que debe regular en caso de la prueba ilícita, el cual no debe afectar a los funcionarios públicos que han sido elegidos por voto popular, cargo de confianza y cargos importantes en la Administración Pública. Tal como ocurrió en el caso del Sr. Alberto Quimper que fue absuelto como producto de la exclusión de la prueba ilícita por vulneración de los derechos al secreto de sus comunicaciones. La historia nos ha demostrado los vladivideos de montesinos, actual congresistas Mamani, el caso del Sr. Quimper, y los actuales videos de la Organización criminal de la Corte Suprema del Callao entre otros siguen impune escudándose en la prueba ilícita, pese a que el delito se evidencia de manera consistente en los audios, y videos. Fundamento mi propuesta con la postura del jurista español Gálvez Muñoz, quién sostuvo, en caso de las pruebas ilícitas, se debe recurrir a las excepciones específicamente la ponderación de intereses en conflicto; y la manera de operativizar es considerando los criterios de la gravedad, intencionalidad, dificultad probatoria, derecho afectado, inevitabilidad del descubrimiento y las consecuencias. La postura del autor es lo apropiado, de lo contrario la corrupción seguirá enquistado dentro del poder de la administración pública, sobre todo la ponderación debe ser en personas que cometieron delito contra el Estado, que debe ser sancionado y no debe ser excluido de una responsabilidad penal; de lo contrario seguirá la impunidad, y dando pie a otros funcionarios públicos a escudarse en la ilicitud de los delitos.

IX. Referencias

- Acurio del pino, S. (2012). *Libro Derecho y Nuevas Tecnologías*.
- Aguirre, H. (2012). *Criminalística y cadena de custodia*. Revista de Derecho Penal y el Derecho Procesal. PIR.
- Aguirre, H. (2012). *Derecho Penal y procesal penal, área de criminalística y cadena de custodia del Ministerio Público del Perú*. (Fecha de acceso 05/07/2018).
- Aldama, C. (2017). *Nuevas tecnologías y en los últimos 9 años*. Perito informático y director de Aldama Informática Legal. Consultor y auditor.
- Aldama, C. (2017). *Nuevas tecnologías y en los últimos 9 años*. Perito informático y director de Aldama Informática Legal. Consultor y auditor.
- Baudelio, E. (2011). En su Tesis titulada, *la prueba ilícita penal en la administración de justicia en el Perú* (Tesis doctoral) sustentada en la Universidad Nacional de Trujillo, Facultad de Derecho, para obtener el grado Doctor en Derecho y Ciencias Políticas. Trujillo, Perú.
- Bradford, P. & Ray, D.(s/f) . *An Online Algorithm for Generating Fractal Hash Chains Applied to Digital Chains of Custody*.
- Bravo (2010). *La prueba en el proceso penal*. (Tesis doctoral). Sustentada en la Universidad Nacional Universidad de Cuenca facultad de jurisprudencia. Cuenca, Ecuador.
- Bueno de Mata, F. (2013). *La prueba electrónica en el marco de una administración de justicia informatizada*. (Sustentada en la Universidad Nacional de Salamanca). Salamanca, España.
- Cárdenas, C. (2015). *La comunicación digital mediante Redes sociales de organizaciones Públicas* (Tesis de licenciatura) sustentada en la Universidad

Nacional Mayor de San Marcos, Facultad de Letras y Ciencias Humanas de Lima, Perú.

Carnelutti, F. (2000). *La Prueba Civil*. (20^{va}. Edic.): Depalma. Buenos Aires, Argentina.

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. (2da. Edic). Estados Unidos de Norteamérica.

Casey, E. (2011). *Digital Evidence and Computer Crime, Third Edition: Forensic Computer*.

Chavarry, E. (2011). *La prueba ilícita penal en la administración de justicia en el Perú* (Tesis doctoral) sustentada en la Universidad Nacional de Trujillo, Perú.

Colquitt, J. (1990). *Alabama Law of Evidence*. The Mitchie Company–Law Publishers, Charlottesville, VA.

Corte Suprema de Justicia, Acuerdo Plenario N° 2-2007/CJ-116. Precedente vinculante, de fecha dieciséis de noviembre de dos mil siete, Lima, Perú.

Delgado, J. (2013). La prueba electrónica en el proceso penal, Diario La Ley, N° 8167, sección doctrina: La ley.

Duarte, L. (2012). En su Tesis titulada, *Valoración probatoria de los documentos audiovisuales*. (Tesis de Magister), sustentada para obtener el grado Magister en Derecho Procesal. Lima, Perú.

Echandía, D. (2002). *Teoría General de la Prueba Judicial*.: Editorial Temis S.A., Bogotá, Colombia.

Esquivel, G. (2005). *La Prueba en el Juicio Fiscal Federal*,(4^a. edic.), México.

Extraído:

http://www.mpfm.gob.pe/escuela/contenido/actividades/docs/2381_criminalistica_y_cadena_de_custodia_nov_2012.pdf

Extraído:

http://www.mpfm.gob.pe/escuela/contenido/actividades/docs/2381_criminalistica_y_cadena_de_custodia_nov_2012.pdf

[12.pdf](#)

- Gálvez, L. (2003). *La ineficacia de la prueba obtenida con violación de derechos fundamentales*.
- Gines, N. (2011). Prueba electrónica, colección de formación continua Facultad Derecho ESADE, Serie Estudios Prácticos sobre los medios de prueba, (5ta. edic.). Barcelona, España.
- Ginés, N. (2011). Prueba electrónica. Colección de Formación continua Facultad Derecho ESADE: Serie Estudios Prácticos sobre los medios de prueba. Barcelona, España.
- Guerrero, W. (2004). *Derecho Procesal Penal*, Tomo III, Pudeleco Editores S.A., Quito, 2004
- Guevara, M. (23 de junio de 2018). *Entrevista [respuesta escrita]*. Fiscal Provincial de a Segunda Fiscalía Penal Corporativa de Ventanilla. Provincia Constitucional del Callao.
- Gutiérrez, W. (2018). Perito Informático Perú. Analista de Sistemas. Con amplia experiencia de haber laborado en el Ministerio Público. Acreditado con REPEJ 25000192013
- Jauchen, E. (2002). *Tratado de la prueba en materia penal*: Rubinzal – Culzoni Editores, Buenos Aires, Argentina.
- Jurado, A. (2011). Valor probatorio del documento electrónico: Revista de Ciencias Jurídicas de la Universidad Rafael Urdaneta. Maracaibo, Venezuela.
- León, J. (2015). *Procedimiento de cadena de custodia sobre contenido digital y su valoración como prueba documental dentro del código orgánico integral penal* (tesis de pregrado para obtener título de abogado). Universidad de Loja, Ecuador.
- López, M. (2012). Libro análisis forense digital.
- McKemmish (1999), citado por Beckett, J. (s/f). Forensic Computing: A

Deterministic Model for Validation and Verification through an Ontological Examination of Forensic Functions and Processes. Adelaide South Australia, January 2010. School of Computer and Information Science. Division of Information Technology, Engineering, and the Environment, University of South Australia.

Muñoz, L. (2009). *Introducción a la probática*. Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch: La ley, Madrid, España.

National Institute of Justice. (2011). USA. *Crimes Scene Guides*. (Acceso febrero 2018). Extraída: [htTitulo Preliminar://www.ojp.usdoj.gov/nij/topics/lawenforcement/investigations/crime-scene/guides/glossary.htm](http://www.ojp.usdoj.gov/nij/topics/lawenforcement/investigations/crime-scene/guides/glossary.htm).

Organización Internacional de Pruebas de Ordenador

Palacio, L. (2000). *La prueba en el proceso penal*. Abeledo-Perrot: Buenos Aires, Argentina.

Pareja, B. (2017). *Modelo de control constitucional para la admisión de la prueba de cargo con violación a derechos fundamentales en el sistema jurídico peruano*. (Sustentada en la Universidad Pontificia Católica del Perú). Lima, Perú.

Peñaranda, H. (2008). *Ius cibernética: Interrelación entre el Derecho y la Información*. Caracas: Venezuela.

Pereira, S. (2013). *La exhibición de documentos probatorios y soportes informáticos*. (Escuela de posgrado) sustentada en la Universidad Nacional de Girona. Cataluña, España.

Pérez, J. (2014). *La prueba electrónica: Consideraciones*.

Puig, S. (s/f). *La prueba electrónica y sus implicancias en la seguridad de la empresa*. (Tesis doctoral) sustentada en la Universidad Nacional Ramón Llull; Barcelona, España.

Quiroz, W. (22 de junio de 2018). *Entrevista [respuesta escrita]*. Juez Superior del

4to Juzgado Penal de Reos en Cárcel de la Corte Superior de Lima Norte, Expositor Internacional del Colegio de Abogados, Profesor de la Academia de la Magistratura, y Autor de distintas publicaciones de textos de Derecho.

Racchumi, L. (22 de junio de 2018). *Entrevista* [respuesta escrita]. Fiscal Adjunto de la Segunda Fiscalía Provincial Penal Corporativa de Ventanilla. Provincia Constitucional del Callao.

Reyes, A. (2010). *Cyber Crime Investigations*.

Rivera, R. (2012). *Manual de Derecho Procesal Penal*. (2da Edición). Barquisimeto. Librería J. Rincón G. C.A.

San Martín, C. (2006). *Derecho Procesal Penal*. Tomo II. 2da edición. Lima: Grijley, 2006.

Sánchez, J. (2016). *WhatsApp, prueba válida en juicio*. Revista del Ilustre Colegio de Abogados de Salamanca, España.

Sentis, S. (1979). *La prueba. Los grandes temas del derecho probatorio*: Ediciones Jurídicas Europa América, Buenos Aires, Argentina.

Strauss, A & Corbin, J. (2002). *Bases de la investigación cualitativa, Técnicas y procedimientos para desarrollar la teoría fundamentada*. Bogotá: Editorial Universidad de Antioquia.

Téllez, J. (2007). *Derecho Informático*, (3ª. Edic.). México.

Velasco, E. (2013). *Diligencias de investigación penal de redes*: La Ley, Madrid, España.

Zabarburu, W. (2 de junio de 2018). *Entrevista* [respuesta escrita]. *Perito Analista* de la División de Investigaciones de Delitos de Alta Tecnología del Perú (Divindat) de la estructura orgánica de la Dirincrí – PNP encargado de patrullar el ciberespacio de los delitos informáticos.

Zavala, Jorge (s/f): op. cit., p. 21.

Zavala, W. (28 de junio de 2018). *Entrevista* [respuesta escrita]. Juez Superior del 4to Juzgado Penal de Investigación Preparatoria de Proceso Inmediato de la Corte Superior del Callao, Expositor del Colegio de Abogados del Callao.

X. Anexos

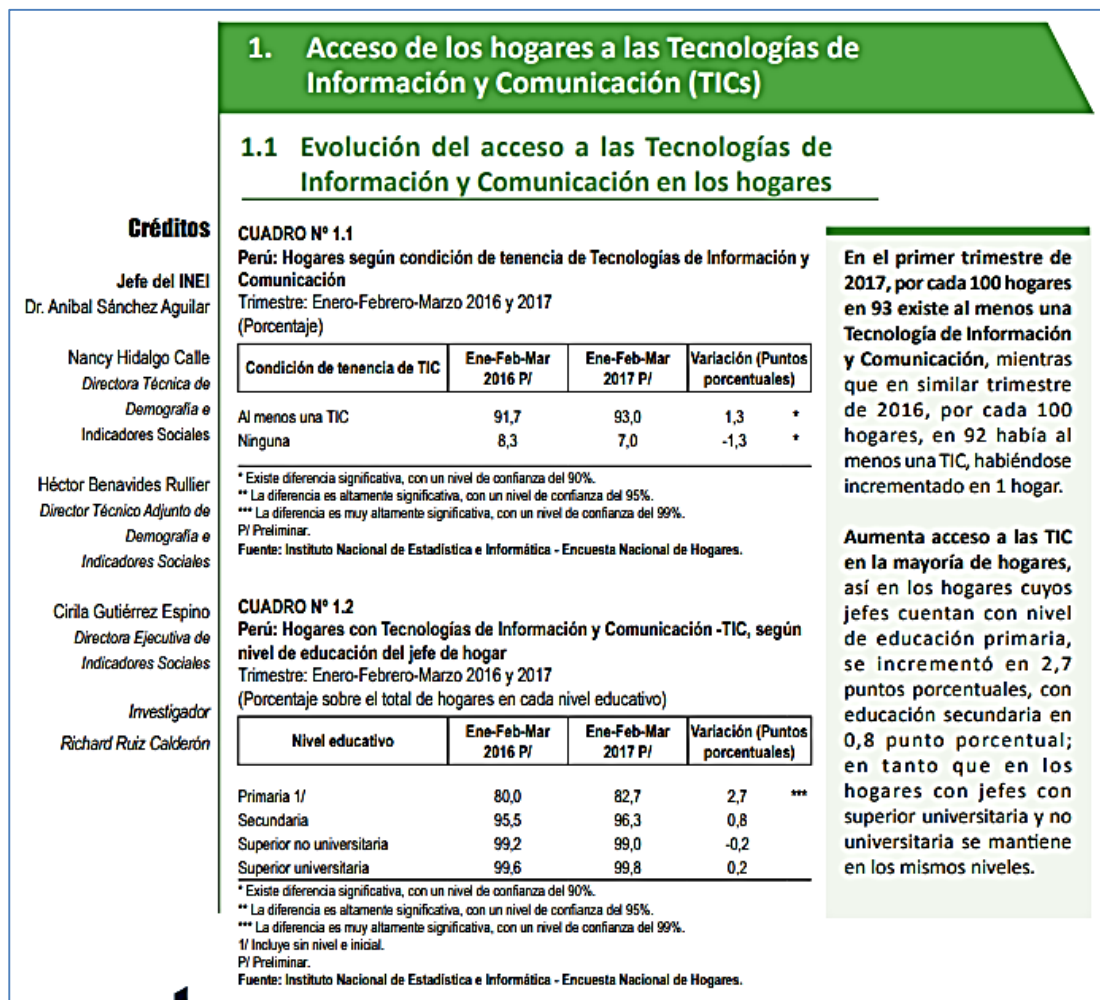
Anexos 1. Gráfico de evidencia digital



Extraído de: artículo publicado de "evidencia digital en el sistema judicial, publicado por Santiago Acurio del Pino.

<http://www.sites.oas.org/cyber/Documents/2016%20-%20Evidencia%20Digital%20en%20el%20Proceso%20Judicial-Santiago%20Acurio.pdf>

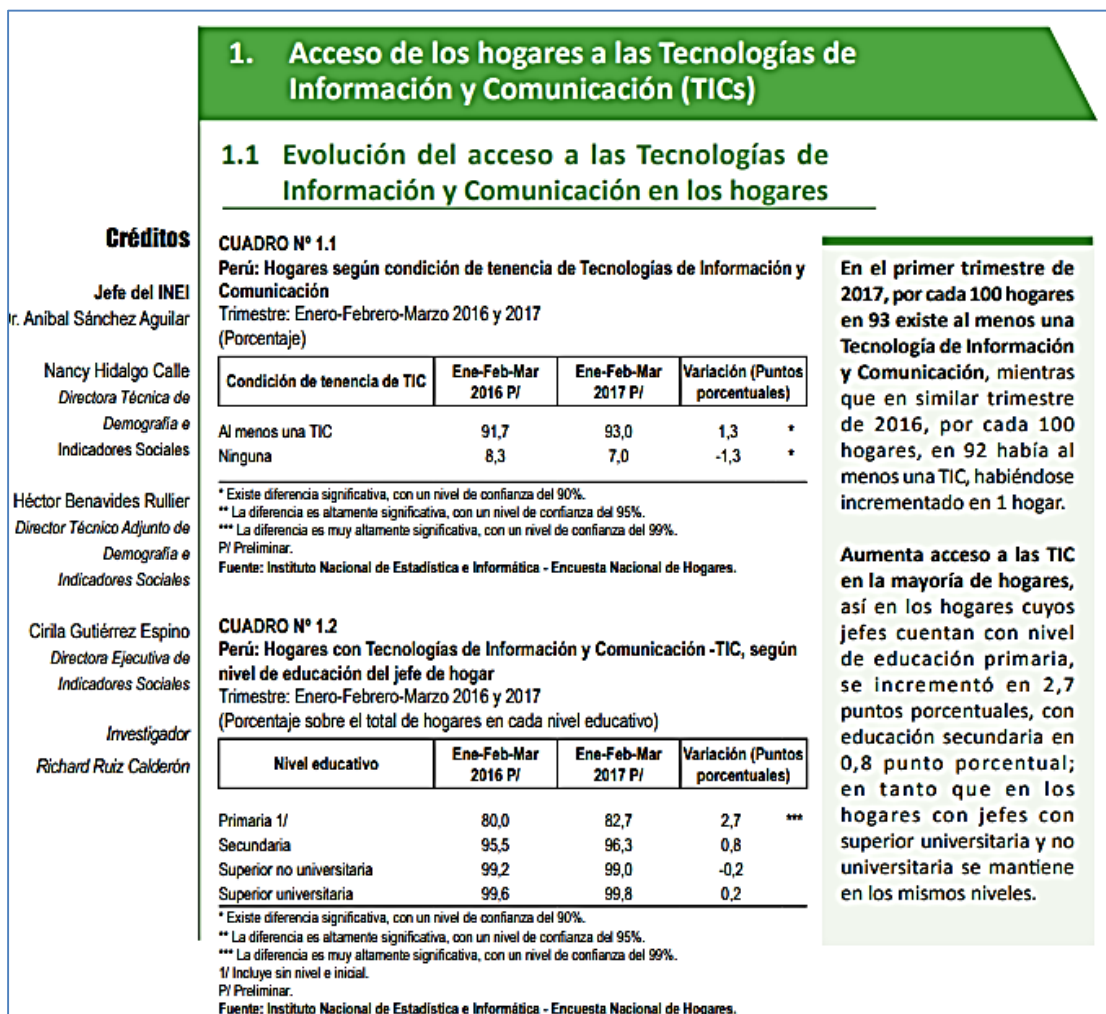
Anexos 2. Gráfico de acceso de información a la red



Extraído: Institución Nacional de Estadística e Informática – INEI

http://www.inei.gob.pe/media/MenuRecursivo/boletines/02-informe-tecnico-n02_tecnologias-de-informacion-ene-feb-mar2017.pdf

Anexos 3. Gráfico de acceso de los hogares a las Tecnologías de la información y comunicación



Estriado: Institución Nacional de Estadística e Informática – INEI

[htTitulo Preliminar://www.inei.gob.pe/media/MenuRecursivo/boletines/02-informe-tecnico-n02_tecnologias-de-informacion-ene-feb-mar2017.pdf](http://www.inei.gob.pe/media/MenuRecursivo/boletines/02-informe-tecnico-n02_tecnologias-de-informacion-ene-feb-mar2017.pdf)

Anexos 4. FODA del Ministerio Publico

OPORTUNIDADES	AMENAZAS
<ul style="list-style-type: none"> ☞ Proceso de cambios organizacionales técnico científicos para la modernización del Ministerio Público ☞ Necesidad y demanda de los servicios de información ☞ Dación de la ley del libro ☞ Disposición en el mercado de contar con tecnología de información para la biblioteca (Internet, bases de datos, soportes digitales, etc.) ☞ Política sectorial favorable para la Biblioteca. 	<ul style="list-style-type: none"> ☞ Restricción presupuestal en el sector público ☞ Remuneraciones y condiciones laborales diferenciadas por la existencia de regímenes diferentes (DL. 728 y DL 276) ☞ Trámites engorrosos y burocráticos en atender las demandas urgentes de la Biblioteca ☞ Costos elevados de parte de los proveedores de material bibliográfico ☞ Ausencia de nuevas inversiones en tecnología de la información ☞ Las unidades de información que ofrecen productos y servicios de información actualizados con apoyo de la tecnología de información ☞ Presión de los usuarios por requerir información actualizada en forma oportuna ☞ Internet, medio más solicitado para la búsqueda y recuperación de la información
FORTALEZAS	DEBILIDADES
<ul style="list-style-type: none"> ☞ Recursos humanos especializados ☞ Atención personalizada ☞ Alto nivel de identificación del personal con la biblioteca ☞ Infraestructura adecuada para los ambientes y servicios que proporciona la Biblioteca ☞ Relación directa con los proveedores ☞ Valioso acervo bibliográfico de las Ciencias Jurídicas ☞ Colección completa de normas legales ☞ Sistema de Información Jurídica ☞ Servicio de fotocopiaa ☞ Colección de videos únicos en su género 	<ul style="list-style-type: none"> ☞ Poquísimas adquisiciones del material bibliográfico ☞ Insuficiente instrumentos técnicos normativos para los procesos técnicos: tesauros, sistemas de descripción ☞ Servicios de información insuficientes ☞ Limitados medios para la promoción ☞ Mobiliario y equipo insuficiente ☞ Tecnología de información insuficientes y desactualizados ☞ Insuficiente material bibliográfico ☞ Visión, misión y objetivos no formulados formalmente ☞ Limitado presupuesto para las adquisiciones del material bibliográfico ☞ Ausencia de programas de capacitación y actualización para el personal ☞ Baja imagen institucional ☞ Limitado número de bases de datos y de registros ☞ Base de datos no disponibles a través de Intranet e Internet ☞ Ausencia de un plan de modernización ☞ Lentitud y limitado abastecimiento de insumos y recursos

Extraído: del Artículo “tesis digitales” UNMSM, plan de modernización del Ministerio Publico, publicado por Granda Alanya Elizabeth.

[htTitulo](#)

[Preliminar://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Human/grande_am/cap3.pdf](http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Human/grande_am/cap3.pdf)

Anexos 5. Delitos más comunes cometidos por la Red-Internet publicado por la dirección de investigación criminal y apoyo a la justicia (DIRINCRI).

DIVINDAT

DELITOS MÁS COMUNES



	<ul style="list-style-type: none"> ● Clonación de Tarjetas y Hurto de Fondos 		<ul style="list-style-type: none"> ● Operaciones Financieras/Comerciales Fraudulentas por Internet
	<ul style="list-style-type: none"> ● Amenazas por e-mail 		<ul style="list-style-type: none"> ● Pornografía Infantil en Internet
	<ul style="list-style-type: none"> ● Extorsión 		<ul style="list-style-type: none"> ● Acceso no autorizado a base de datos
	<ul style="list-style-type: none"> ● Chantaje sexual y económico 		<ul style="list-style-type: none"> ● Intrusiones (Hacking, Cracking)

Extraída: De la publicación de la dirección de investigación criminal y apoyo a la justicia (DIRINCRI) división de investigación de delitos de Alta tecnología “Delitos Informáticos En El Perú”.

htTitulo Preliminar://www.ical.org.pe/files/criminalistica/delito.pdf

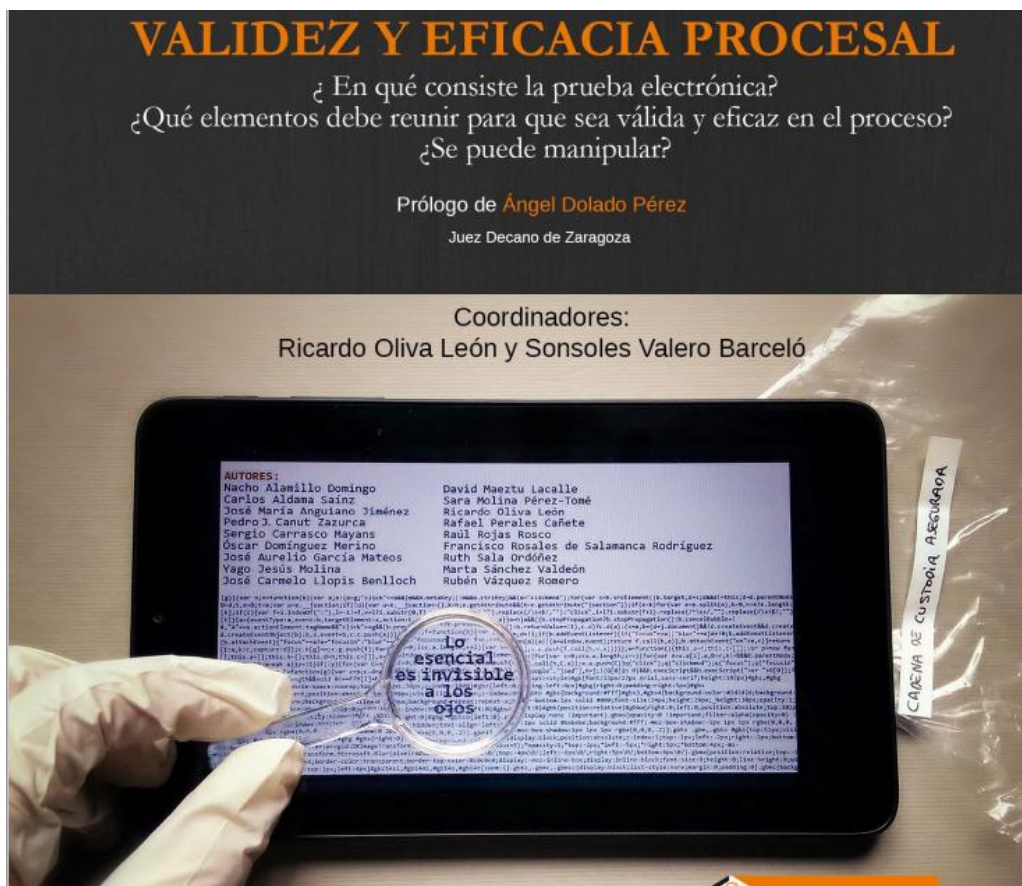
Anexos 6. Delitos más comunes cometidos por la Red-Internet publicado por la dirección de investigación criminal y apoyo a la justicia (DIRINCRI).

TENDENCIAS CYBERCRIMINALIDAD							
DIVINDAT							
	DELITOS/ AÑOS	2008	2009	2010	2011	2012	TOTAL
	HURTO DE FONDOS	239	523	384	705	401	2252
	PORNOGRAFIA INFANTIL	43	65	90	151	136	485
	DELITOS INFORMATICOS	128	125	161	184	147	745
	OTROS: Amenazas, chantaje,	53	223	299	468	184	1227
	TOTAL	463	936	934	1508	868	4709

Extraída: De la publicación de la dirección de investigación criminal y apoyo a la justicia (DIRINCRI) división de investigación de delitos de Alta tecnología “Delitos Informáticos En El Perú”.

htTitulo Preliminar://www.ical.org.pe/files/criminalistica/delito.pdf

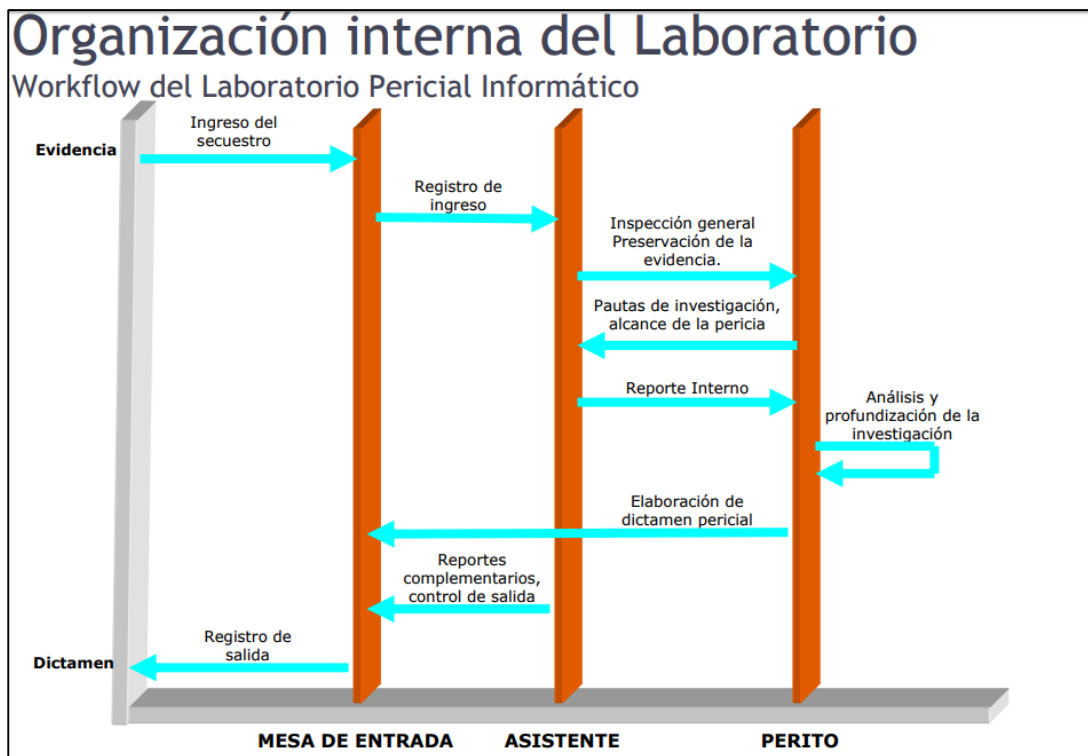
Anexos 7. Examen pericial de informática forense



Extraída: de la publicación del Juez Decano de Zaragoza – España, Colección: Desafíos Legales # Reto JCF Juristas con Futuro.

[htTitulo Preliminares://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf](http://titulos.preliminares://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf)

Anexos 8. Organización interna del laboratorio de pericia informático



Extraída: de la publicación del Artículo Hernán Herrera perito informático del país de Argentina.

[htTitulo](#)

[Preliminar://www.neuquen.gov.ar/seguridadinformatica/pdf/Informatica%20Forense%20-%20Hernan%20Herrera.pdf](http://www.neuquen.gov.ar/seguridadinformatica/pdf/Informatica%20Forense%20-%20Hernan%20Herrera.pdf)

Anexos 9. Componentes del sistema informático



Extraída: de la publicación del Artículo ()

[htTitulo](#)

[Preliminar://www.juntadeandalucia.es/institutodeadministracionpublica/publico/anexos/empleo/c2.1000/TEMA%2011.pdf](http://www.juntadeandalucia.es/institutodeadministracionpublica/publico/anexos/empleo/c2.1000/TEMA%2011.pdf)

Anexo 10. Matriz de categorías y sub categorías:

Subcategoría	Preguntas a sujetos perteneciente al cargo de Jueces	Preguntas a sujetos perteneciente al cargo de Fiscales	Preguntas a sujetos perteneciente al cargo de peritos en informática	Preguntas a sujetos pertenecientes al cargo de Abogado litigante.
- Tratamiento de la prueba digital	¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad?.	¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria?	¿Cuáles son los procedimientos que debe tener en cuenta el Ministerio Público para derivar la evidencia digital a la División de Investigación de Delitos de Alta Tecnología (DIVINDAT)?	¿Cuál es el procedimiento que debe seguir un abogado, respecto a las evidencias digitales de su patrocinado antes de ofrecer al Ministerio Público?
- Implementación tecnológica	¿Los Juzgados Penales cuenta con la implementación tecnológica suficiente para brindar seguridad y custodia a las pruebas digitales ofrecida por las partes?	¿El Ministerio Público cuenta con salas de visualización de video, audio, foto y otros que permita su transcripción confiable de la prueba digital?	¿La DIVINDAT cuenta con la implementación tecnológica para dar respuestas inmediatas a las pericias de informática forense?	¿El Ministerio Público cuenta con salas de visualización de video, audio, foto y otros que permita su transcripción confiable de la prueba digital?
- Incorporación de la prueba digital	Según su experiencia y análisis probatorio ¿Cuáles son los problemas más comunes que impiden la valoración de la prueba digital?	¿Cuáles son los requisitos que debe cumplir una prueba digital para su admisión e incorporación al proceso?	¿Cuáles son los procedimientos técnicos que garantizan la autenticidad e integridad de la prueba digital?	¿Cuáles son las causas de exclusión probatoria de las evidencias digitales?
- Valoración de la prueba digital	¿Cuáles son las causas para la exclusión de la prueba digital?	¿Cuáles son las causas para la exclusión de la prueba digital?	¿Cuál es la eficacia de las pericias de informática forense practicadas por DIVINDAT?	¿Cuáles son los procedimientos que recomienda usted, para que las evidencias digitales sean eficazmente valoradas por el Juez?

Anexo 11. Matriz investigación
Tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao
-2017

Problema general	Objetivo General	Supuestos	Categoría	Sub Categorías	Técnicas	Instrumento
¿Cuál es el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla – Callao 2017?	Describir el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla – Callao 2017	Es insuficiente el tratamiento de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla – Callao 2017.	Prueba digital	<ul style="list-style-type: none"> ▪ Naturaleza ▪ Medio, fuente y Objeto ▪ Modalidades, procedimientos y límites. ▪ Tratamiento de la prueba digital ▪ Actuación de la prueba digital. ▪ Legitimidad de la prueba digital. 	<ul style="list-style-type: none"> • Observación • Entrevista 	<ul style="list-style-type: none"> • Guía de observación
Problema específico ¿Cuál es la implementación tecnológica para el tratamiento de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017?	Objetivo específico Determinar la implementación tecnológica para el tratamiento de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017.	Supuesto específico Es insuficiente la implementación tecnológica para el tratamiento de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.		Implementación		
¿Cuáles son los procedimientos para la incorporación de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017?	Describir los procedimientos para la incorporación de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.	El incumplimiento de los procedimientos, tales como el respeto de los Derechos Fundamentales, la cadena de custodia, peritaje de informática forense impide la incorporación de la prueba digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.	Incorporación	<ul style="list-style-type: none"> ▪ Obtención, Pertinencia, necesidad y utilidad ▪ Admisión, oportunidad de incorporación. ▪ Principio de contradicción ▪ Cadena de custodia 		
¿Cuáles son los derechos fundamentales afectados que impiden la valoración de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017?	Determinar los derechos fundamentales afectados que impiden la valoración de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao - 2017.	La vulneración de los derechos fundamentales impiden la valoración de la prueba de digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla, Callao -2017	Valoración	<ul style="list-style-type: none"> ▪ Conservación ▪ Contradicción ▪ Ilícitud ▪ Ilegalidad ▪ Excepciones ▪ Forense informática ▪ Autenticidad ▪ Integridad. ▪ Impugnación 		

Anexo 12. Matriz de triangulación

PREGUNTA	A1	A2	A3	A4	A5	A6	CONVERGENCIA	DIVERGENCIA	INTERPRETACION
1.- ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?	De manera puntual y específica No existe, no hay regulación actual como prueba digital, sin embargo el Art. 185° del Código Procesal Penal reconoce al contenido de un audio visual o audio grabado como prueba documental.	El Art. 185° de Código Procesal Penal reconoce como pruebas documentales, dentro de ello los audios, videos y todo medio electrónico, pero un tratamiento especial en Código Procesal Penal no está establecido.	El MP debe derivar a la División De Investigaciones De Delitos De Alta Tecnología (DIVINDAT) las pruebas digitales para una pericia de informática forense con su debida cadena de custodia y autorización judicial.	El Código Procesal Penal del 2004 lo regula como prueba documental, pero no prueba digital y su tratamiento es como una prueba tradicional con lo mismo que estipula el Artículo 185°.	No se encuentra especificamente en el Código Procesal Penal del 2004 como prueba digital se trata con las mismas características de una prueba documental, conforme lo establece el Artículo 185° CNPP	Conforme el Código Procesal Penal explícitamente no hay un Artículo que lo desarrolle como prueba digital, ya que solo comprende como prueba tradicional o documental.	La mayoría de los entrevistados considera que no existe un tratamiento especial en el Código Procesal Penal respecto a la prueba digital, que su regulación está bajo la observancia del Art. 185° considerado como prueba documental.	No todas las digitales ofrecidas por las partes, son derivadas a una pericia, hecho que podría causar la impugnación de la prueba.	La Prueba digital no tiene un tratamiento especial en Código Procesal Penal sin embargo su regulación está en el Art. 185° considerada como pruebas documentales, es decir todo las evidencias electrónicas, tanto como mensajes a través de email, Cloud Computing, imágenes, audio, video, u otro soporte digital son considerados como prueba documental. Si entre las fuentes de prueba de un hecho ilícito se encontrara evidencias digitales, la actuación probatoria se efectuara bajo la observancia del Art. 382 del Código Procesal Penal.
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?	Con la cadena de custodia se logra la autenticidad y por ende el principio de mismidad. Cumpliendo los requisitos de exhibición, autenticación, actuación, reproducción, y principio contradictorio para su valoración.	Con un peritaje que perenne y armen la cadenas de custodia para su conservacion y se pueda presentar a la audiencia contradictorio de juzgamiento; de modo que se evite el cuestionamiento o exclusion.	El peritaje de las cuentas de correos, página web y entre otros dispositivos hardware como: disco duro, USB, memoria flas, teléfono móvil, cámaras digitales, etc para la valoración de la prueba digital.	Las pruebas digitales deben ser obtenidas conforme a Ley, para no incurrir en causalidad o fraude, falsificación u otro similar. En caso de las evidencias digitales tienen que presentarlo con el mismo equipo que fue grabado	Las denunciante s no presentan las pruebas, por temor a las venganzas por esta evidencias , pese a existir aumento de delito hay pocos que denuncian..	Los agraviados a través de la red no presentan pruebas, y muy pocas personas presentan denuncias de este tipo.	En mayoría los entrevistados para inclusión la prueba digital en la fase probatoria, debe ingresar a una cadena de custodia y examen de pericia informática de modo que sea valorado por el juez en la sentencia.	En una minoría sostuvon que existe gran parte de los agraviados que no denuncian por temor a las represalias o en todo caso borran las evidencias por vergüenza de ventilar su intimidad.	Las evidencias digitales obligatoriamente debe entrar en cadena de custodia, para conservar, conservar y custodiar para mantener la originalidad logrando el principio de mismidad y evitar la manipulación; luego el MP debe enviar a la DIVINDAT para una pericia de informática forense a fin de obtener un código valor HASH de autenticidad e integridad, de manera que se pueda presentar a la audiencia contradictorio de juzgamiento para su valoración y no sea producto de exclusion probartoria.

3.- ¿El Ministerio Público cuenta con la implementación tecnológica suficiente para brindar seguridad y custodia a las pruebas digitales ofrecida por las partes? ¿Por qué?	El MP no cuenta con herramientas para la guarda; las grabaciones en audio y en video, necesariamente debe pasar en observancia del Art. 382, y el MP puede custodiarlos y conservarlos.	Existe una insuficiencia de implementación de laboratorios a nivel nacional y existe un centralismo en todo el Perú para las pericias de pruebas digitales se sigue haciendo en Lima.	El Ministerio Público no cuenta con la implementación necesaria para practicar las pericias, es por ello tiene que enviar al Centro de Pericias de	Aquí en la Fiscalía de Ventanilla no contamos con recursos suficientes para la implementación tecnológica.	Hace 15 días se ha implementado una sala de visualización pero no se encuentra en este local, sino en la otra sede.	No contamos con sala de visualización de evidencias digitales, porque lo hacemos cada uno de los fiscales en la computadora de la oficina.	Los entrevistados coinciden en que el Ministerio Público no cuenta con implementación suficiente para el tratamiento de las pruebas digitales.	No hay divergencias.	La delincuencia en el distrito de Ventanilla va en aumento, y las evidencias en su mayoría se encuentran en las redes sociales, correos, WhatsApp y otros sin embargo el Ministerio Público como persecutor del delito no cuenta con los recursos suficientes y menos con la adecuada implementación tecnológica suficiente para garantizar la autenticidad y la valoración de los pruebas digitales.
4.- ¿El Ministerio Público cuenta con salas de visualización de video, audio, foto y otros documentos digitales que permita su transcripción confiable de la prueba digital?	Las pruebas digitales deben estar en manos del ministerio público o también debería estar en depósito que el ministerio debe implementar.	Incluso para los delitos informáticos es más complejo se tiene que remitir a DIVINDAT-PNP de la Av. España y dicha división no existe en el Callao.	No cuenta con implementación tecnológica tampoco con capacitación a los fiscales y jueces en el manejo de este nuevo sistema.	Necesitamos una implementación en cuanto al manejo de las pruebas digitales, porque muchos desconocemos.	La visualización lo realizábamos en la computadora de mi oficina	Falta presupuesto para la implementación y capacitación del personal.	La mayoría de los entrevistados coinciden en que el Ministerio Público no cuenta con una sala adecuada de visualización y transcripción de las evidencia digitales.	Solo un fiscal adjunto señaló que ya hay una sala de visualización de la prueba digital en la otra sede central.	Los Jueces y Fiscales de Ventanilla afirman en las entrevistas que el Ministerio Público de esta sede no cuenta con la implementación tecnológica para dar un manejo apropiado de las pruebas digitales y menos han recibido de parte del Estado capacitaciones en este sistema digital.
5.- ¿Cuáles son las instituciones anexos al Ministerio Público encargados de practicar la pericia de informática forense y cuál es el tiempo de resultados? ¿Cuál es su sugerencia?	Existen dos entidades uno del Ministerio Público es el Instituto de Medicina Legal y Ciencia Forense, área de Alta Tecnología y el DIVINDAT la división de investigación de delitos de alta tecnología de la PNP.	El Laboratorio Forense Digital de la Policía Nacional del Perú, que estará encargado de emitir peritajes de acústica forense, telefonía forense y cómputo forense, a solicitud del MP y del Poder Judicial.	El DIVINDAT – PNP de la av. España.	El centro de peritaje de la Av. Abancay.	El centro de peritaje del Ministerio Público ubicado en la Av. Aramburu.	Los entrevistados coinciden que la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú.	Un grupo de entrevistados considera que debería descentralizarse en diferentes provincias.	La mayoría de los entrevistados señalaron que existe un centralismo en Lima sobre el peritaje, todas las pericias del a nivel nacional se lleva a cabo en la capital, específicamente en la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú, lo que afecta los plazos del proceso por la distancia y también la carga procesal del mismo centro de peritaje.	

6. ¿Cuáles son los requisitos que debe cumplir una prueba digital para su admisión e incorporación al proceso? ¿Cuáles son?	Las evidencias digitales se incorporan bajo el principio de la licitud y con el principio contradictorio, es decir después del debate contradictorio a través de la oralización.	Las pericias determinan la validez de la prueba en la sede judicial, ratificadas en la audiencia pública con el principio contradictorio.	A los dispositivos se extrae una imagen forense al cual se le aplica el HASH que consiste en un algoritmo matemático que asigna un código valor que autentica el contenido de la información.	Según dispuesto en el Art. 187° todo documento de video debe visualizarse para su transcripción en acta en presencia de las partes.	La prueba siempre va ser cuestionada en juicio oral, por tal razón es que debe cumplir que en su obtención no debe afectar los derechos fundamentales.	Según el Art. 187° toda prueba digital presentado por las partes debe pasar por una audiencia visualizara para su transcripción en acta en presencia de las partes.	La mayoría de los entrevistados señalaron que las pruebas deben ser transcritos en presencia de las partes además de la pericia, debe haberse sometido a un debate contradictorio en audiencia solo así podrá ser valorado por el juez.	No hay divergencias.	La mayoría de los entrevistados señalaron que las evidencias digitales para tener una validez en la sede judicial debe ser examinada por un perito informático, luego debe ser incorporada a la estación procesal a través de un debate en audiencia pública en el cual el perito ratifica, sometidos al derecho contradictorio de los peritos de parte, cumplido estas fase la valoración y producción de la prueba queda a discrecionalidad del juez.
7. Según su experiencia y análisis probatorio ¿Cuáles son los problemas más comunes que impiden la valoración de la prueba digital? ¿Por qué?	Las evidencias digitales como grabaciones, de audio y video No tengan cadena de custodia, en caso de prueba digital la volatilidad de la información, sensible de alteración.	La obtención de la prueba que haya afectado algún derecho fundamental.	Eliminar los datos que forma parte de la evidencia digital de los dispositivos electrónicos o digitales y no haber transcrito en un soporte de papel.	Por lo menos aquí hemos recibido muy pocas pruebas a lo menciona.	La exclusión de la pruebas impugnadas se pueden reiterar los medios de prueba inadmitidos en audiencia de control.	La falta de pericias de informática forense y la afectación a los derechos fundamentales de la persona.	Los entrevistados coincidieron en que la naturaleza del delito de asesinato por lucro responde a la afectación del bien jurídico protegido como es la vida.	No hay divergencias	Según el Art. 187° toda prueba digital presentado por las partes debe pasar por una audiencia que visualizara para su transcripción en acta en presencia de las partes, asimismo la exclusión de la pruebas digitales impugnadas por las partes se pueden reiterar el ofrecimiento de los medios de prueba inadmitidos en audiencia de control invocando el inciso 3) del Artículo 373.
8.- ¿En qué fase del proceso se ve disminuida la eficacia jurídica de la prueba digital? ¿Por qué?	En la fase de control de acusación, control de pruebas, y en el debate pericial.	En la etapa intermedia y en juicio oral.	En la fase intermedia de control de pruebas el cual será corroborado con un peritaje para identificar la autenticidad	Como toda prueba normal no debe ser ilícita o prohibida, para que la prueba tenga valor probatorio	Captura de pantalla de MSN de whatsApp fue impugnado en la parte de control de pruebas por no contener certificación de un perito.	En control de pruebas de acusación en la fase intermedio y en la fase de debate contradictorio del juicio oral.	Todos los entrevistados consideran que la fase intermedia es la que se ve disminuido la eficacia procesal de la prueba digital.	No hay divergencias.	La eficacia procesal de la prueba digital se ve disminuida en la fase intermedia, con la programación del control de acusación y en el juicio oral con el debate contradictorio de la prueba pericial, que da lugar la valoración o la exclusión.
9. ¿Cuáles son las causales para la exclusión de la prueba digital? ¿Por	Por las infracciones de los derechos fundamentales, existe el Art.159	En la audiencia de control en la etapa intermedia las partes solicitan	Que las pruebas hayan sido obtenidas por tercero ajeno	La prueba digital no debe ser ilícita.	Por afectación a los derechos fundamentales es.	Afectar la dignidad de la persona humana en la obtención de	En mayoría los entrevistados coincidieron que deben establecerse criterios que	En minoría los entrevistados señalaron que debería modificarse su	Las evidencias digitales son excluidas del proceso como prueba ilícita cuando en su obtención haya afectado uno derechos fundamentales, el Art. 159 del Código

qué?	del Código Procesal Penal sobre las prohibiciones probatorias, tanto las fuentes y medios de prueba que se actúen en juicio oral.	la exclusión de las pruebas por la mala producción, como prueba ilícita, prueba irregular, por lo que no se ha respetado los procedimientos procesales en la producción	a las partes y con afectación a los derechos constitucionales.	las pruebas.	definan las diferencias de ambos tipos penales para una correcta aplicación.	regulación o en todo caso derogarse a fin de no crear confusión en el operador de justicia.	Procesal Penal señaló el Juez no podrá utilizar, directa o indirectamente, las fuentes o medios de prueba obtenidos con vulneración de los derechos fundamentales, asimismo la prueba irregular puede ser excluido si en su actuación no se respecto los procedimientos procesales.
------	---	---	--	--------------	--	---	---

Anexo 13. Entrevista a los peritos de informático Perú



25 jul. (hace 5 días)

GERENTE de G&S INVERSIONES Y SERVICIOS EIRL

Estudios INGENIERIA INFORMATICA Y DE SISTEMAS

Disculpa la demora:

Cuáles son los procedimientos que debe tener en cuenta el Ministerio Público para derivar la evidencia digital para un peritaje?

Aver comencemos, te hablare específicamente lo que ocurre en la oficina de ANALISIS DIGITAL FORENSE:

La evidencia digital (disco duro, memoria usb, celular u otro) tiene que seguir una correcta intervención desde el su recojo hasta la llegada a la oficina de peritaje; Eso se llama cadena de custodia la cual debe seguir estos pasos:

1. identificar a el(las) personas que cometen un delito usando un medio tecnológico
2. concurrir al lugar (casa, oficina) del presunto delincuente con un representante del MP junto con la policía y si se puede un perito informatico.
3. filmar y fotografiar la escena, ubicar la evidencia digital y fotografiarla para ser guardada en un sobre hermético con la firma de los participantes; llenar un acta describiendo la situación encontrada y los detalles técnicos de la evidencia digital que será firmada por los actores(persona,MP. Policia) }
3. la evidencia será llevada a la oficina de la fiscalía para luego ser remitida a la oficina de ANALISIS DIGITAL FORENSE donde se indicará que se quiere analizar.
4. luego esta oficina emite un informe pericial con los hallazgos

¿Cual es la implementacion tecnologica con las que cuenta ustedes para dar respuestas inmediatas a las pericias de informatica forense?

Contamos con profesionales como ingenieros de sistemas y electrónicos, además contamos con hardware y software forense de análisis informático

¿en que consiste la autenticidad e integridad de la prueba digital?

Consiste en que la evidencia digital debe seguir su correcta cadena de custodia desde la incautación hasta llegada a la oficina de ANALISIS DIGITAL FORENSE, sin que esta sea abierta o manipulada en el trayecto por ninguna persona NO autorizada. De esta manera se garantiza que la evidencia no ha sido manipulada desde la incautación

Además, el análisis forense que realiza el MP puede ser auditable, quiere decir que otro perito puede realizar el mismo análisis forense y va a encontrar los mismos resultados que el MP

¿Cuál es la eficacia probatoria de las pericias de parte en informatica forense?

La eficacia probatoria se puede decir que: Los hallazgos encontrados por la oficina de ANALISIS DIGITAL FORENSE son ciertos, exactos y no están sujetos a duda ya que en el campo de la informática cuando analizamos una evidencia podemos decir que por ejemplo si existe o no pornografía en un disco duro, esta ciencia forense es exacta!

Cual es la eficacia de las pericias de parte con respecto a las pericias que realiza el DIVINDAT?

En este país existen 2 entidades del estado que pueden realizar pericias OFICIALES en el campo informático y son la DIVINDAT y el MP.

Ahora existen peritos de parte que son: del colegio de ingenieros del Perú y del Poder judicial (Siempre que ellos representen a una empresa privada o persona natural). La eficacia se mide en que un perito tiene que trabajar con ética y verdad, si los dos siguen estos principios sus informes tendrán los mismos resultados

Anexo 14. Entrevista a los jueces y fiscales

ANEXOS

Anexo 01: Instrumentos

Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista

Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Entrevistado:

[Redacted area]

Breve resumen curricular:

[Redacted area]

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?

Anexo 14-A. Entrevista a los jueces y fiscales

Objetivo Especifico 1

Determinar la implementación tecnológica del tratamiento de la prueba digital ofrecida por las partes en el proceso penal del distrito fiscal del Ministerio Público de Ventanilla, Callao -2017.

3. ¿El Ministerio Público cuenta con la implementación tecnológica suficiente para brindar seguridad y custodia a las pruebas digitales ofrecidas por las partes? ¿Por qué?
4. ¿El Ministerio Público cuenta con salas de visualización de video, audio, foto y otros documentos digitales que permita su transcripción confiable de la prueba digital?
5. ¿Cuáles son las instituciones anexas al Ministerio Público encargadas de practicar la pericia de informática forense y cuál es el tiempo de resultados? ¿Cuál es su sugerencia?

Objetivo Especifico 2

Describir los procedimientos para la incorporación de la prueba digital ofrecida por las partes en el proceso penal del distrito fiscal del Ministerio Público de Ventanilla, Callao - 2017.

6. ¿Cuáles son los requisitos que debe cumplir una prueba digital para su admisión e incorporación al proceso? ¿Cuáles son?
7. Según su experiencia y análisis probatorio ¿Cuáles son los problemas más comunes que impiden la valoración de la prueba digital? ¿Por qué?
8. ¿En qué fase del proceso se ve disminuida la eficacia jurídica de la prueba digital? ¿Por qué?

Objetivo Especifico 3

Determinar la vulneración de los derechos fundamentales que impidan la valoración de la prueba de digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao -2017.

9. ¿Cuáles son las causales para la exclusión de la prueba digital? ¿Por qué?

Tiene algo más que agregar

Gracias por su aporte académico.

Mg. WILLIAMS ABEL ZAVALA MATA
JUEZ SUPLENTERARIO
Ministerio Público
PODER JUDICIAL DEL PERU

PODER JUDICIAL DEL PERU
Mg. WILLIAMS ABEL ZAVALA MATA
JUEZ SUPLENTERARIO
Ministerio Público
PODER JUDICIAL DEL PERU

Anexo 14-B. Entrevista a los jueces y fiscales

ANEXOS

Anexo 01: Instrumentos
Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista

Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Resumen Curricular

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?

PAOLA FRANCESCA ORDÓZ CHALLCO
Asistente en Función Fiscal
Quinta Fiscalía Provincial Penal Corporativa
Distrito Fiscal de Ventanilla

Anexo 14-C. Entrevista a los jueces y fiscales

ANEXOS

Anexo 01: Instrumentos
Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista

Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Entrevistado:

[Redacted area]

Breve resumen curricular:

[Redacted area]

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?


KATIA NÓMELA AREVALO GUTIÉRREZ
Asistente en Función Fiscal
1ra Fiscalía Provincial Penal Corporativa
Del Distrito Fiscal de Ventanilla

Anexo 14-D. Entrevista al Perito Analista de Divindat-PNP

ANEXOS

Anexo 01: Instrumentos

Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista

Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Entrevistado:

Breve resumen curricular:

Wuilman ZABARBURU VARGAS
SOT. PNP

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad?
¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?

Anexo 14-E. Entrevista a docente universitario

ANEXOS

Anexo 01: Instrumentos
Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista

Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Entrevistado:

[Redacted area]

Breve resumen curricular:

[Redacted area]

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?

Gracias por su aporte académico.

Elder J. Miranda
Elder J. Miranda
ABOGADO
REG. CAL. 32435

Anexo 14-F. Entrevista a Fiscal Provincia de Ventanilla

ANEXOS

Anexo 01: Instrumentos

Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista

Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Entrevistado:

Resumen Curricular

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?


 Rina Huanca Caspe
 Fiscal Provincial
 Atto. Fiscalía Provincial Penal Corporativa

Anexo 14-G. Entrevista a Fiscal Provincia de Ventanilla

ANEXOS

Anexo 01: Instrumentos
Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista

Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Entrevistado:

Resumen Curricular

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?

Gracias por su aporte académico.

Perry Francisco Baraybar Cuzque
Fiscal Adjunto Provincial
Cuarta Fiscalía Provincial Penal Corporativa
D.F. VENTANILLA

Anexo 14-H. Entrevista a Fiscal Provincia de Ventanilla

ANEXOS

Anexo 01: Instrumentos

Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista


Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Resumen Curricular

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?


 LUIS ANTONIO RACCHUMI SIADÉN
 Fiscal Adjunto Provincial Penal (P)
 2da. Fiscalía Provincial Penal Corporativa
 de Ventanilla

Anexo 14-I. Entrevista a Fiscal Provincia de Ventanilla

ANEXOS

Anexo 01: Instrumentos
Entrevista a especialistas peritos, Jueces y Fiscales



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POST GRADO

Entrevista

Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao-2017

Entrevistado:

Resumen Curricular

Objetivo General

La presente investigación tiene como finalidad describir el tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público del distrito Fiscal de Ventanilla, Callao – 2017.

1. ¿Existe un tratamiento especial de la prueba digital en el Nuevo Código Procesal Penal del 2004 que garantice la autenticidad e integridad? ¿Cuáles son?
2. ¿Desde la perspectiva del Derecho Procesal Penal existe un procedimiento especial para la inclusión de la prueba digital en la fase probatoria? ¿Cuáles?


Robert Z. Espinoza Caspedes
Fiscal Adjunto Provincial
4ta. Fiscalía Provincial Penal Corporativa
DF Ventanilla

Anexo 15- Acta de Transcripción de prueba digital en la Fiscalía de Ventanilla

ACTA DE VISUALIZACIÓN, TRANSCRIPCIÓN DE CONTENIDO DE CD Y AUDIO VIDEO.

--- En el Distrito de Ventanilla, siendo las 10.00 horas del día 01-JUN-2017, presente el instructor en una de las Oficinas del DEPINCRI VENTANILLA, y el Representante del Ministerio Público Fiscal Provincial de la 4ta. Fiscalía provincial Penal Corporativa de Ventanilla, presente la denunciante _____), quien al ser preguntado por sus generales de Ley, dijo llamarse como queda escrito ser natural de Ancash, estado civil soltero acupación ama de casa, con 5to de educación secundaria, identificada con DNI. Nro. _____ y domiciliada en la Mz F6 Lote 14 AA.HH. Las Lomas de Ventanilla – Ventanilla, presente el investigador _____ (48), quien al ser preguntado por sus generales de Ley dijo llamarse como queda escrito ser natural Piura, estado civil casado, ocupación conductor, grado de instrucción secundaria completa, identificado con DNI., nr _____ 4, y domiciliado en la Mz F 6 Lote 18 AA.HH. Las lomas de Ventanilla – Ventanilla, quien se encuentra en presencia de su abogado defensor e _____

_____, DNI. _____, domicilio procesal Mz A Modulo 5d Urb. Pedro Cueva – Ventanilla Callao, ref. vecino de Electra, correo electrónico _____ (Movistar); procediéndose a la presente diligencia con el siguiente resultado:-----

En este acto se procede a abrir un sobre manila el cual se encuentra cerrado y es de color amarillo inscrito dos firmas (anexo 1-C) con letras de color rojo anexo 20, en cuyo interior se aprecia un porta CD. Transparente marca DISC compact recordable, dentro del cual se encuentra un CD. color blanco, **MARCA PRINCO DVD-R (4.7.GB SP 120 MIN) 1-4xspeed (DVD R R4.7 4X/1X), serie externa B147300457-29127**, con el rotulo a plumón color negro "ANEXO 1-C, procediendo a la presente diligencia con el siguiente resultado: -----

Se procede a intrucir el CD, en mención a la Laptop Marca TOSHIBA, perteneciente al S8. PNP SANCHEZ MONDRAGON, Nil. Jhoan, al abrir EN Equipo –Unidad de DVD RW ,PRUEBAS_USURPACI, aparece tres archivos con el nombre. **PRIMER VIDEO:** Nombre Video1_Instantes en que se apropia, destruyendo los perímetros, fecha_18.12.2016, fecha de modificación 18/12/2016 12.00 tipo VLC media file (.mp4) tamaño 426,142 KB, **SEGUNDO VIDEO:** nombre Video2_luego_de_usurpado condicionando fecha_18.12.2016, fecha de modificación 12/01/2017 04.25 tipo VLC media file (.3gp), tamaño 3.817 KB, **TERCER VIDEO:** Nombre Video3_rompe_con violencia_mi



31675759
Sanchez Mondragon

Andre Enrique Chiriquiano
Fiscal Provincial
4ta. Fiscalía Provincial Penal Corporativa
DE Ventanilla

400
Cuerpo
Criminal
400

Benigno B

CAZ 9701

Anexo 15-A- Acta de Transcripción de prueba digital en la Fiscalía de Ventanilla

CASO SGF4006014501-2017-43-0

ACTA DE VISUALIZACIÓN Y TRANSCRIPCIÓN DE VIDEO

En el Distrito de Ventanilla, en las instalaciones de la Primera Fiscalía Provincial Penal Corporativa- Cuarto Despacho, siendo el día 29 de mayo del 2018, a las 12.22 horas, la representante del Ministerio Público, [redacted] junta Provincial de la Primera Fiscalía Provincial Penal Corporativa de Ventanilla, en las diligencias preliminares del caso signado con c [redacted] inicio a la diligencia de Visualización y Transcripción de video, que fuera programado para el día de hoy con el siguiente resultado, por lo que se procede al deslacrado del sobre manila que obra de folios 49 la misma que contiene el CD - R 52X marca MASTER-G.

OBJETO DE LA DILIGENCIA

Conforme a lo ordenado por este Despacho Fiscal, se procede a realizar la diligencia de visualización y transcripción de un CD-R 52X marca MASTER-G, diligencia que fuera programado para el día de hoy a las 11:00:

PARTICIPANTES EN LA DILIGENCIA

- [redacted] Provincial de la Primera Fiscalía Provincial Penal Corporativa de Ventanilla.

AGRAVIADO

- F [redacted]

Abogado defensor de la parte antes indicada, [redacted].

INVESTIGADO

Se deja constancia que el señor J [redacted] rrió a la presente diligencia, pese estar debidamente notificado tal como se puede corroborar de la Cedula de notificación número 009114, siendo la misma con fecha 15 de mayo de 2018 – bajo puerta-; de mismo en cuanto al Abogado Defensor Público no concurrió a la presente pese estar Oficiado con el Oficio N° 43-2017-1° era F.P.P.C.V-MP-FN.

ARTÍCULO 187 DEL CPP. - TRANSCRIPCIÓN Y VISUALIZACIÓN DE VIDEO:

1. Todo documento redactado en idioma distinto del castellano, será traducido por un traductor oficial.
2. Cuando el documento consista en una cinta magnetofónica, el Juez o el Fiscal en la investigación Preparatoria dispondrá, de ser el caso, su transcripción en un acta, con intervención de las partes.
3. Cuando el documento consista en una cinta de video, el Juez o el Fiscal en la Investigación Preparatoria ordenará su visualización y su transcripción en un acta, con intervención de las partes.
4. Cuando la transcripción de la cinta magnetofónica o cinta de video, por su extensión demande un tiempo considerable, el acta podrá levantarse en el plazo de tres días de realizada la respectiva diligencia, previo traslado de la misma por el plazo de dos días para las observaciones que correspondan. Vencido el plazo sin haberse formulado observaciones, el acta será aprobada inmediatamente; de igual manera, el Juez o el Fiscal resolverán las observaciones formuladas al acta, disponiendo lo conveniente.

PARA QUE DIGAN: El señor I [redacted] nte diligencia requieren la presencia de un abogado? Dijeron Si por lo que se encuentra presente

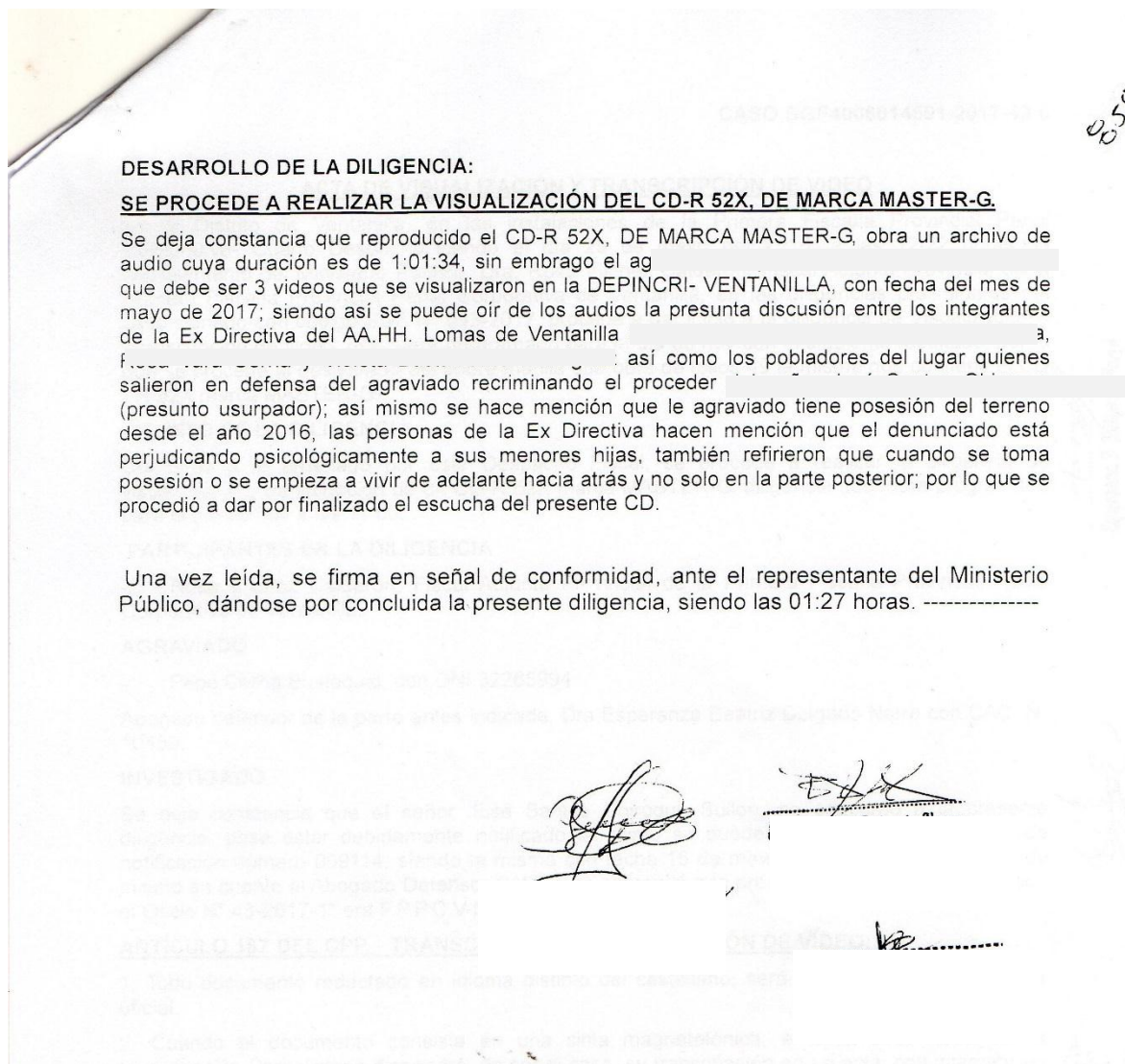
[redacted] con domicilio procesal ubicado en Casilla Judicial N°

[redacted] : Y1 lote 19 Ventanilla Alta- Ventanilla, [redacted].

[Handwritten signature]
Esperanza B. Pelgajo Narro

[Handwritten signature]
Rosa Vilchez Calderón
Fiscal Adjunta Provincial
1ra. Fiscalía Provincial Penal Corporativa
DE M. P. U. P. S.

Anexo 15-B- Acta de Transcripción de prueba digital en la Fiscalía de Ventanilla



Anexo 15-C. de acta de transcripción

43-2017

CARPETA FISCAL 43-2017

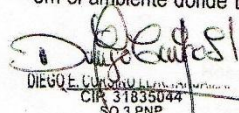
88
87
y net

ACTA DE DESLACRADO Y VISUALIZACION DE TOMAS FILMICAS DE DVD

En el Distrito de Ventanilla, siendo las 10:10 horas del día 22 de Junio del 2017, presente el instructor, el agraviado [redacted] le Ancash, nacido el 18 de Junio de 1971, hijo de D [redacted] soltero (Conviviente), Albañil de construcción, identificado [redacted] domiciliado en MZ. F-6 LOTE S/N AA.HH. LAS LOMAS DE VENTANILLA - CALLAO, el Investigado la persona de Jose Santos CHIROQUE SULLON (48), natural de Catacaos - Piura, nacido el 07 de Octubre de 1969, hijo de [redacted] y domiciliado en la MZ. F-6 LOTE 18 AA.HH LAS LOMAS DE VENTANILLA DE LA PAN. NORTE - VENTANILLA - CALLAO; quien en presencia de su abogado defensor el D [redacted] representante del Ministerio Público la [redacted] Fiscal Adjunto Provincial de la 1° Fiscalía Provincial Penal Corporativa de Ventanilla - Callao; se procedió a realizar la presente diligencia de visualización cuyo resultado es el siguiente:-----

1. En este acto se procede apertura el sobre manila lacrado con cinta adhesiva y con una firma ilegible de la [redacted], que contiene un DVD-R marca "PRINCO 1-4x speed" de color blanco y con las inscripción con lapicero azul "ANEXO L-G - video de la presunto Delito contra el patrimonio - Usurpación agravada en su contra, Caso: carpeta fiscal N° 4006014501-2017-43-0. Al abrir se observa TRES archivos que son los siguientes:
 - Video1_instantes en que se apropia, destruyendo los perimetros, Fecha 18/12/2016 12.00p.m, tipo: VIDEO MP4, tamaño: 426,142 KB
 - Video2_luego_de_usurpado condicionando, Fecha 12/01/2017 04:25 tipo : 3GP File tamaño 3,817KB
 - Video3_rompe_con violencia_mi propiedad_de 3mts mas a la propiedad de Carmen soto de Fecha 18/12/2016 04:11 tipo : Video MP4 de tamaño 156,659 KB

Seguidamente al abrir la primera toma con el archivo Video1_instantes en que se apropia, destruyendo los perimetros, Fecha 18/12/2016 12.00p.m, tipo: VIDEO MP4, tamaño: 426,142 KB, observándose en la parte superior los dígitos mencionados y MEDIA PLAYER CLASSIC HOME CINEMA - V1.2.1008.0, observando en el **00.01** minuto a la persona [redacted] de color negro ubicados en un ambiente de material de madera desordenado, con desmonte, palos, piedras, una malla, bolsas, costales en el suelo, ladrillos y en el **00.04** minutos observamos que la persona mencionada líneas arriba se encuentra trasladando los materiales que se encuentran en el ambiente descrito que son palos, piedras, ladrillos, mallas y en el **00.26** minuto se observa que la [redacted] del lado **01.03** minuto observamos que la persona mencionada vuelve a salir para volver a sacar las maderas que se encuentran plantadas en la tierra y las mallas colgadas con los costales ingresando el **01.24** minuto al ambiente del lado trasladando maderas, costales, ladrillos y en el **03.14** minutos se observa que la grabación se encuentra en sentido contrario de cabeza observando a la persona de [redacted] en el ambiente donde trasladaba el desmonte, madera, palos, costales, se encuentra una persona [redacted]


 DIEGO C. SULLON
 CIR 31835044
 SO.3 PNP

Rosa Viterbo Castellón
 Fiscal Adjunta Provincial
 1ra. Fiscalía Provincial Penal Corporativa
 de Ventanilla

Jose Santos Chiroque
 Callao

Anexo 15-D. de acta de transcripción

88
88
Cabrera
y otros

no distinguiendo bien, y en el **05.00** minutos no se observar bien porque se encuentra la filmación de cabeza con dirección al cielo, el **06.00** minuto la misma persona mencionada se encuentra sacando desmonte, palos, madera, esterni, costales, ladrillos y el **07.07** minuto termina la grabación pudiéndose observar al señ _____, se encuentra parado sacando una madera plantada en el suelo. _____

Seguidamente al abrir la primera toma con el Video2_luego_de_usurpado condicionando, Fecha 12/01/2017 04:25 tipo : 3GP File tamaño 3,817KB, observando los dígitos mencionados y MEDIA PLAYER CLASSIC HOMECINEMA - V1.2.1008.0, observando que la _____ ndido sacando tierra para luego en el **00.14** minuto pararse y clavar una especie de madera en la hueco que se encontraba realizando luego en el **00.35** minuto no se puede visualizar bien el video y en el **00.41** minuto se observa a una persona de sexo femenino, con una camiseta de color rojo con negro, un short color oscuro y con una especie de palo en la mano, para que en el **00.44** minuto culmine dicha grabación. _____

Seguidamente al abrir la primera toma con el Video3_rompe_con violencia_mi propiedad_de 3mts mas a la propiedad de Carmen soto de Fecha 18/12/2016 04:11 tipo : Video MP4 de tamaño 156,659 KB, los dígitos mencionados y MEDIA PLAYER CLASSIC HOMECINEMA - V1.2.1008.0, se observa una especie de pared de madera **00.14** minuto se puede observar que en la parte posterior de la pared de madera unas personas de sexo masculino sacando madera y en el 00.46 minuto se observa a la persona de _____, unos sujetos de sexo masculino en la parte posterior de la pared de madera, se encuentran acomodando y moviendo maderas, en el **01.13** minutos se observa la persona mencionada líneas arriba con una especie de fierro en la mano para que luego no pudiendo visualizar bien y en el **01.40** minutos se observa que la cámara filmadora se encuentra distorsionada no pudiendo observar bien hasta el **02.36** minuto que culmina el dicha grabacion. _____

---Asimismo la persona de _____, no da su conformidad al video materia de investigación por cuanto no corresponde a los hechos materia de la denuncia ni a la fecha que dice se cometió el acto de usurpación, asimismo dicho video fue presentado en una denuncia contra el _____ esta agravada _____

---Asimismo que en el video salí _____


Siendo las 11:50 hrs del mismo día de la fecha se dio por finalizada la presente diligencia, firmando y colocando la impresión dactilar de su índice derecho en señal de conformidad las partes en presencia del abogado defensor de la parte imputada R.M.P el instructor quien certifica. _____

EL INSTRUCTOR    

S.O.3 PNP

R.M.P


ABOGADO DEFENSOR.

 CAL 9700

Min. Justicia Provincial Penal Corporativa
DF Ventanilla

Anexo 16. Audiencia de Visualización de prueba digital

69



Ministerio Público

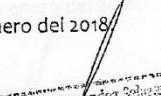
MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN
 PRIMERA FISCALÍA PROVINCIAL PENAL CORPORATIVA
 DE VENTANILLA DISTRITO JUDICIAL DE VENTANILLA

CÉDULA DE NOTIFICACIÓN FISCAL
CARPETA FISCAL NRO. 43-2017

DESTINATARIO: F
 DOMICILIO REAL: MZ. F6, LT. 14, AA.HH. LAS LOMAS DE VENTANILLA-CALLAO
 REF. Km 39 de la panamericana norte

Por disposición de la Señorita Fiscal Adjunta Provincial _____ en de la Primera Fiscalía Provincial Penal Corporativa de Ventanilla, me dirijo a usted a fin de ponerle en conocimiento que debe apersonarse el día 20 de febrero del 2018, a las 09:00 horas, a este Despacho Fiscal, sito en la Mz. C-1, Lt. 08, Ex Zona Comercial e Industrial- Ventanilla, a fin de que se lleve a cabo la diligencia de visualización del contenido de los CDs que obran en autos presentados por la parte denunciante en la presente investigación, asimismo se le adjunta la Disposición N°122-2017, de fecha 23 de octubre del 2017, emitida por la Primera Fiscalía Superior Penal de Ventanilla, a fojas 8 y la Disposición N°04-2018, de fecha 15 de enero del 2018, a fojas 3.

Ventanilla, 22 de enero del 2018.



RECIBIDO POR: _____

FECHA: _____

HORA: _____

NOTA:
 DEJAR BAJO PUERTA de no encontrarse persona alguna en las visitas efectuadas por personal de COURRIER (Art. 161 del C:P.C).



Acta de Aprobación de originalidad de Tesis

Yo, Edwin Alberto Martínez López, docente de la Escuela de Posgrado de la Universidad César Vallejo filial Lima Norte, revisor de la tesis titulada "Tratamiento de la prueba digital ofrecida por las partes en el proceso penal del Ministerio Público de Ventanilla, Callao -2017" del estudiante Edgardo Simón Zarzosa Cadillo y habiendo sido capacitado e instruido en el uso de la herramienta Turnitin, he constatado lo siguiente:

Que el citado trabajo académico tiene un índice de similitud de 13 % verificable en el reporte de originalidad del programa turnitin, grado de coincidencia que cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lima, 14 de agosto del 2018

Dr. Edwin Alberto Martínez López

DNI:09080039

Docente de la EPG - UCV

Feedback Studio - Google Chrome
Es seguro | https://ev.tumitin.com/app/carta/es/?lang=es&x=1&o=986691024&u=1075197110

feedback studio Derecho /0 < 2 de 14 > ?

ESCUELA DE POSGRADO
UNIVERSIDAD CESAR VALLEJO

**Tratamiento de la prueba digital ofrecida por las partes
en el proceso penal del Ministerio Público de Ventanilla,
Callao -2017**

**TESIS PARA OPTAR EL GRADO ACADÉMICO DE
MAESTRO EN DERECHO PENAL Y PROCESAL PENAL**

AUTOR:
Br. Edgardo Simón Zarzosa Cadillo

ASESOR:
Dr. Edwin Alberto Martínez López

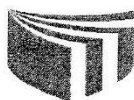
SECCIÓN:

Página: 1 de 136 Número de palabras: 40455 Text-only Report High Resolution Activado 17:09 1/02/2018

Resumen de coincidencias

13 %

1	Entregado a Universida...	2 %
2	www.scribd.com	1 %
3	Entregado a Pontificia ...	1 %
4	dspace.unitru.edu.pe	1 %
5	repositorio.unheval.edu...	1 %
6	docs.com	<1 %
7	www.mpfj.gob.pe	<1 %



UNIVERSIDAD CÉSAR VALLEJO

Centro de Recursos para el Aprendizaje y la Investigación (CRAI)
"César Acuña Peralta"

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN ELECTRÓNICA DE LAS TESIS

1. DATOS PERSONALES

Apellidos y Nombres: (solo los datos del que autoriza)

ZARZOSA CADILLO EDGARDO SIMON

D.N.I. : 320335441

Domicilio : Av. Jose GRANDD #3102 SMP

Teléfono : Fijo : Móvil : 972901970

E-mail : edgardozarzosa28@gmail.com

2. IDENTIFICACIÓN DE LA TESIS

Modalidad:

Tesis de Pregrado

Facultad :

Escuela :

Carrera :

Título :

Tesis de Posgrado

Maestría

Doctorado

Grado : MESTRO

Mención : DERECHO PENAL Y PROCESAL PENAL

3. DATOS DE LA TESIS

Autor (es) Apellidos y Nombres:

ZARZOSA CADILLO EDGARDO SIMON

Título de la tesis:

TRATAMIENTO DE LA PRUEBA DIGITAL OFRECIDA POR LAS PARTES EN EL PROCESO PENAL DEL MINUS TERMO PUBLICO DE VENTANILLA, CALLAO-2017

Año de publicación : 2018

4. AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:

A través del presente documento,

Si autorizo a publicar en texto completo mi tesis.



No autorizo a publicar en texto completo mi tesis.



Firma :

Fecha :

25/09/2018



ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Mitchell Alarcon

FORMATO DE SOLICITUD

SOLICITA:

Visto bueno de la Tesis

ESCUELA DE POSGRADO

Edgardo Zorrosa Cadillo con DNI N° *320335411*
(Nombres y apellidos del solicitante) (Número de DNI)
domiciliado (a) en *Av. José Granda # 3102 - SMP*
(Calle / Lote / Mz. / Urb. / Distrito / Provincia / Región)

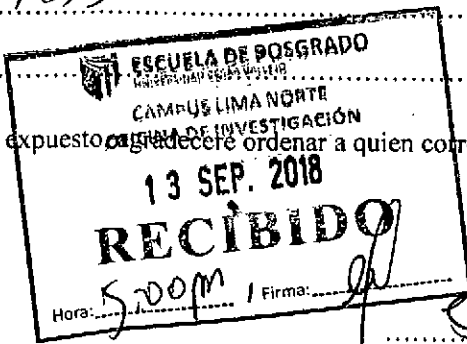
ante Ud. con el debido respeto expongo lo siguiente:

Que en mi condición de alumno de la promoción: *2018* del programa: *Maestría en Derecho Penal y procesal penal*
(Promoción) (Nombre del programa)
identificado con el código de matrícula N° *6000033755*
(Código de alumno)

de la Escuela de Posgrado, recorro a su honorable despacho para solicitarle lo siguiente:

Que, siendo un requisito para el empastado de la tesis el visto bueno, una vez sustentado y aprobado. Solicito a su despacho el visto bueno de la Tesis.

Por lo expuesto agradeceré ordenar a quien corresponde se me atienda mi petición por ser de justicia.



Lima, *13* de *setiembre* de 2018

[Signature]
(Firma del solicitante)

Documentos que adjunto:

- a. *01. Tesis anulada y corregida*
- b. *Copia Resol. Directoral*
- c. *Copia del dictamen*
- d. *Copia del puntillero Turnutin*

Cualquier consulta por favor comunicarse conmigo al:

Teléfonos: *992901970*

Email: *edgardozorrosa20@gmail.com*

VB para tesis

[Signature]