FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de **DERECHO Y CIENCIAS POLÍTICAS**

“LA EVIDENCIA DIGITAL EN EL CIBERCRIMEN - PERU 2022 ”

Tesis para optar al título profesional de:

ABOGADO

Autor:

Bryan Antonio Cadillo Quispe

Asesor:

Mg. Gregorio Wilfredo Roque Ventura

https://orcid.org/0000-0002-7854-760X

Lima - Perú

2022

JURADO EVALUADOR

Jurado 1 Presidente(a)	**Ysaac Marcelino Arcos Flores**	**06976352**
	Nombre y Apellidos	Nº DNI

Jurado 2	**Noe Valderrama Marquina**	**07173421**
	Nombre y Apellidos	Nº DNI

Jurado 3	**Elías Chávez Rodríguez**	**43304596**
	Nombre y Apellidos	Nº DNI

DEDICATORIA

Dedico este trabajo a mis padres, hermana, abuelo, a dios y a los estudiantes que día a día realizan diversos esfuerzos para lograr terminar su carrera con las limitaciones que puedan tener. Para todos ellos este pequeño presente.

AGRADECIMIENTO

A mis padres Sonia Esther Quispe Ayala y Porfirio Antonio Cadillo Obispo, las personas más valiosas en mi vida, mis ejemplos los cuales me demuestran día a día que todo se consigue con perseverancia, humildad y disciplina. También a mi hermana Keyla Cadillo Quispe. A ello a Don José y Don Jorge Samanta, personas especiales en la vida de mi familia al igual que la señora Patricia de Buenos Aires-Argentina. A ello, a mi tío Pablo Cadillo Obispo, quien desde pequeño me enseño y aún me enseña que la vida es difícil pero que siempre se debe ir para delante y nunca rendirse por más obstáculos que la vida pueda presentar.

A su vez a agradecer a mi asesor por el gran apoyo en el presente trabajo y a Dios que siempre nos mira y cuida.

Gracias.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tiene por objetivo identificar cual es el procedimiento normativo adecuado para la obtención de la evidencia digital en el cibercrimen, estando a que dicha evidencia conlleva un valor probatorio y puede encontrarse almacenada en un "Hardware", (terabyte, celulares, laptops, USB, DVD u otro), así como también pueda encontrarse en "Software" de repositorio (Google Drive, Dropbox y One Drive u otro) almacenamientos en la red.

La identificación normativa del procedimiento implica que el operador de justicia identifique el mecanismo normativo aplicado adecuado de aseguramiento de la evidencia digital, ya que su no aplicación conllevaría a que la evidencia digital en delitos abarcados en el Cibercrimen pueda ser alterada, dañada, destruida, y como resultado de ello, el operador experto "perito" no logre un resultado idóneo o en su defecto no pueda realizar el análisis del mismo con aras de elaborar un elemento probatorio que determine la conducta delictiva del sujeto activo a lo largo del proceso penal.

Es en esa medida, que la importancia del procedimiento normativo adecuado conlleva a que dicha evidencia digital tenga la categoría de "prueba digital", a nivel la etapa de juicio oral habiendo previamente pasado por el control del juez en la etapa intermedia.

Por ende, la valoración que conlleva la "evidencia digital", genera una calificación a nivel de delitos, ya que no en todos los tipos penal se encuentra como una evidencia "madre", estando a que su característica "digital" enerva el uso de herramientas distintas a la de una evidencia común, enfocados a delitos digitales.

Por lo que, la presente investigación busca determinar el procedimiento normativo para el tratamiento, preservación de la evidencia digital, y como tal ayude a contrarrestar el cibercrimen. Es en esa medida que abarcaremos la normativa nacional respecto a los delitos informáticos, así como el convenio de Budapest a nivel internacional, dispositivos jurídicos centrales que abarcan este tipo de conductas por parte de los ciberdelincuentes y los instrumentos que a la fecha se encuentran vigentes , que son las guías de la evidencia digital del Ministerio Público y Policía Nacional del Perú.

PALABRAS CLAVES: Evidencia digital, cibercrimen, ciberdelincuencia, prueba digital, cadena de custodia, código hash .

CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

La coyuntura social en el Perú sufre constantemente cambios y en esta oportunidad abarcaremos a la tecnología como tal, lo que nos conlleva a las conductas digitales delictivas que a lo largo del tiempo los dispositivos jurídicos se encuentran limitados de regular, pues estas en el día a día varían conforme al estilo de vida que el ser humano lleva. Es así , que esta investigación busca el poder identificar cual es el procedimiento normativo adecuado para la obtención y su posterior preservación de las "huellas digitales" que estás conductas dejan, llamadas "evidencias digitales" en el ámbito del cibercrimen, como elementos probatorios de relevancia jurídica para la determinación de responsabilidad penal.

A ello, se advertirá el poco conocimiento que el operador de justicia tiene respecto de estos temas de suma importancia, pues conlleva a que el tratamiento de una evidencia digital sufra alteraciones, daños y en los peores casos su eliminación, lo cual se va actualizando con el tiempo.

Es así que, la necesidad del conocimiento y/o identificación de la normativa jurídica ayudara a identificar el tratamiento, tipo de fuentes, características de una evidencia digital, para así poder realizar su debida obtención y preservación constante en el tiempo.

Como consecuencia de ello, ante la necesidad que surge a partir de estos tipos de conductas delictivas digitales, así como su consecuente carga procesal, surge la creación de las Fiscalías Especializadas en Ciberdelincuencia, como el resultado que una entidad competente del Estado (Ministerio Público) hace frente al cibercrimen en sus diferentes variantes.

Se suma a ello, la constante problemática en el tema logístico respecto de los análisis periciales, pues la falta de recursos humanos de expertos en el tema lleva la delantera, así como la falta de herramientas de análisis informático, esto según se advierte de lo mencionado por los expertos en el tema.

1.2. Antecedentes de investigación

1.2.1. Nacionales-Perú

(Escobedo, 2018) en su trabajo titulado **"La admisibilidad y el valor probatorio de la evidencia digital en el sistema jurídico peruano 2018"** concluye que*:*

> *"Los delitos informáticos en el ciberespacio se desarrollan en conexión con el internet para que así la ciberdelincuencia de lugar a delitos transnacionales donde las leyes no tiene alcance y jurisdicción, siendo estas conductas las que involucran a varios países en un solo hecho como tal".*

Teniendo en cuenta el concepto obtenido, se advierte que en efecto, estos delitos necesitan de las herramientas tecnológicas para su ejecución (mundo digital), pues conlleva a la utilización del "Internet" como medio de transporte de datos necesarios para la ejecución de dicha conducta digital delictiva, permitiéndole el afectar bienes jurídicos desde un lugar a otro sin discriminar la distancia, siendo esta metros, kilómetros e inclusive de un continente a otro, lo cual genera la dificultad de establecer la delimitación territorial y con ello el ordenamiento jurídico responsable de su atención y sanción.

(Terreros, 2014) en su trabajo titulado **"Delitos Informáticos-Cibercrimen**" concluye que:

> *"Los delitos con este tipo de características se encuentra difícil el establecer la información como el único bien jurídico, pues conlleva a un conjunto de bienes los cuales colisionan con diversos intereses colectivos".*

Al respecto, se resalta que la afectación del bien jurídico no podemos determinarlo como uno sino como un conjunto de bienes, pues estas conductas digitales delictivas afectan diversos intereses jurídicos, no siendo la información como el bien jurídico más importante, pero es innegable la importancia que tiene para los ciberdelincuentes.

(BALLESTEROS, 2014) En su trabajo titulado "**Cibercrimen: particularidades en su investigación y enjuiciamiento"** concluye que:

> *"Ante la delincuencia digital debido a su constante avance, genera una impunidad pues elude las coordenadas de la soberanía estatal, es necesario incrementar la cuota de solidaridad y cooperación internacional mediante la suscripción de tratados internacionales".*

Al respecto, el autor destaca la necesidad de la unión de estados mediante convenios interinstitucionales de las entidades encargadas de brindar la seguridad en el tratamiento de datos. Pues ello, se base en que este tipo de conductas no respetan límites de soberanía y que por lo tanto la cooperación internacional surge como una herramienta necesaria y vital para la reducción de este tipos de conductas delictivas.

(LIBARDO, 2020) En su trabajo titulado: **"Modelo de Gestión del Análisis Forense de Hechos Delictivos Informáticos en el Marco del Sistema de Justicia Peruano"** concluye que:

> *"La disponibilidad de recursos tecnológicos influencia significativamente en el análisis forense de hechos delictivos informáticos, pues conlleva al resultado de la eficiencia y eficacia del proceso en la comprobación de hechos delictivos informáticos".*

En este caso el autor critica que la implementación de gestión a niveles de este tipo de delitos solo se basa en la adquisición de herramientas informáticas las cuales son indispensable para un resultado eficaz y eficiente además de los operadores informáticos, pues son los responsables de una correcta aplicación a fin de erradicar este tipo de conductas punibles.

(CADILLO, 2018) En su trabajo titulado: **"Tratamiento de la Prueba Digital ofrecida por las partes en el Proceso Penal del Ministerio Público de Ventanilla Callao-2017"** concluye:

> *"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; siendo necesario un tratamiento especial para su valoración eficaz".*

Es decir, toda las evidencias de mensajería electrónicas, "evidencia digital" cuyo contenido tenga como elemento probatorio hechos delictivos digitales, son considerados como prueba documental, y su actuación probatoria se efectuará bajo la observancia del Art. 382 del Código Procesal Penal[1].Sobre esta conclusión, resulta pertinente señalar que en efecto es

[1] *Artículo 382°.- Prueba material 1. Los instrumentos o efectos del delito, y los objetos o vestigios incautados o recogidos, que obren o hayan sido incorporados con anterioridad al juicio, siempre que sea materialmente posible, serán exhibidos en el debate y podrán*

necesaria una aplicación especial de este tipo de pruebas pues su obtención se genera a partir de tratamientos especiales digitales por personal capacitado que originara las pericias respectivas.

1.2.2. Internacionales

COLOMBIA- (SICHACA, 2019) En su trabajo titulado **"Requisitos jurídicos para la validez jurídica de la prueba digital"** concluye:

> *"Existe regulación de la prueba digital pero no es suficiente, pues se debe mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y los procesos que permita una seguridad jurídica para la presentación idónea de las pruebas digitales".*

Es decir, la necesidad de que el operado jurídico tenga el conocimiento adecuado y constante de los avances de la tecnología en apoyo a las conductas digitales delictivas, lo cual conlleve a que la regulación jurídica contemple los supuesto necesarios para su debida erradicación, pero la necesidad de que el operador jurídico conlleve una actualización constante de dichas conductas delictivas digitales resulta de carácter obligatorio.

COLOMBIA (RUIZ, 2019) En su trabajo titulado: **"Contexto de la Evidencia en Colombia: Buenas Prácticas y Aplicación de Metodologías"** concluye:

---

ser examinados por las partes. 2. La prueba material podrá ser presentada a los acusados, testigos y peritos durante sus declaraciones, a fin de que la reconozcan o informen sobre ella.

> *"La relación que posee el Cibercrimen permite que sus ejes de acción la involucren directamente a distintas metodologías, siendo necesario el comprender la relevancia con el fin de establecer las circunstancias de tiempo, modo y lugar para determinar las características cometidas por el Ciberdelincuente".*

Al respecto, el autor señala que es muy importante para la identificación del ciberdelincuente, el establecer los parámetros del tiempo, modo y lugar, a fin de poder determinar el conocimiento del bien o bienes jurídicos afectados como consecuencias de las conductas delictivas digitales realizadas, siendo indispensable por parte del personal idóneo el establecer mediante el uso de las herramientas periciales más actuales la erradicación de dichas conductas. Es decir, la especialización por parte del personal idóneo permitirá en este tipo de actividades digitales vislumbrar la conducta atribuida al sujeto activo (ciberdelincuente).

COLOMBIA (MAYA, 2017) En su trabajo titulado **"El Cibercrimen y sus efectos en la Teoría de la Tipicidad: De una realidad física a una realidad virtual",** concluye:

> *"Los cibercrímenes representan el nacimiento de comportamientos que tienen lugar a realidades virtuales con el objeto de vulnerar bienes como datos, información y nuevos bienes jurídicos intermedios siendo realizados mediante técnicas particulares basados en sistemas binarios, que pueden ser traducidos a los humanos mediante infraestructuras informáticas o Hardware".*

Es decir, el autor indica que el comportamiento delictivo digital mediante el uso de sistemas de infraestructura informática como el hardware, brindan un acceso total a la información, datos u otros bienes jurídicos pasibles de ser vulnerados. En ese sentido, este tipo de conductas delictivas pueden ser pasibles de una sanción errada, siempre y cuando no

se utilicen las técnicas necesarias para la debida individualización del sujeto activo, así como que la conducta no se adecue al verbo rector del tipo penal en el planteamiento de la posible tesis fiscal, la inadecuada aplicación de la obtención de la evidencia digital, generando así una inimputabilidad jurídica en perjuicio de los bienes jurídicos tutelables.

1.3. Marco teórico General

A lo largo de esta investigación, se encontraron diversos estudios, artículos especializados, doctrina nacional e internacional que brindo una mejor concepción del tema de investigación, a fin de realizar un aporte a la comunidad jurídica sobre este tema muy poco trabajado a nivel nacional, donde es clara la falta de una regulación normativa respecto de su obtención y preservación, acorde al avance de la tecnología en referencia la "Evidencia Digital" en el cibercrimen, ejecutada en su diferentes variantes delictivas por parte de los ciberdelincuentes.

Aunado a ello, la presente investigación busca establecer el procedimiento idóneo para la obtención y preservación en el tiempo de la evidencia digital como elemento probatorio en los delitos del cibercrimen, a fin de que permita a los administradores de justicia una mejor y debida motivación para la resoluciones de "casos digitales" haciendo referencia a delitos informáticos y a su vez mayor información para la nueva generación de los "estudiosos del derecho" y los que deseen introducirse en este rama del derecho "digital". En ese sentido, se procede a analizar los dispositivos de nuestro ordenamiento jurídico, así como legislación comparada, doctrina nacional e internacional y/o casos emblemáticos, para una mejor

concepción a la denominación de la "evidencia digital", así como el poder identificar el actor principal para su obtención.

1.4. Marco Teórico Especifico de estudio

1.4.1. Respecto al Cibercrimen y Ciberespacio

Entendemos como "**Cibercrimen**" según (Maya, 2017):

> *Los cibercrímenes o (delitos informáticos en sentido estricto o propio), castigan los comportamientos que lesionan o ponen en peligro de manera ilícita la seguridad de las funciones informáticas; sin perjuicio de que ello implique la lesión o la puesta en peligro de otros bienes jurídicos tutelados. Desde esta perspectiva, no se trata de delitos tradicionales o comunes, sino de tipologías especiales realizadas a través de procedimientos informáticos, cuya riqueza técnica, su contexto virtual, la afectación de objetos inmateriales su deslocalización en el ciberespacio, rompen los esquemas teóricos y las dinámicas probatorias propias de los delitos comunes.*

Sobre el "**Ciberespacio"** según Miro Linares (LINARES):

> " *El ciberespacio es para las relaciones sociales, en ese sentido, tan real como el meatspace (que es un término utilizado para referirse al espacio físico frente al ciberespacio (Fielding, s.f.)) Y todos los comportamientos socialmente identificables que no requieren de un contacto físico directo pueden realizarse en él del mismo modo que en el espacio físico; esto es solo lo cualitativo, pues, en lo cuantitativo, el ciberespacio también potencia la capacidad de las personas para el contacto social al derribar las barreras del espacio físico "*

Asimismo, debemos entender que en el Cibercrimen conlleva a una conducta delictiva que acarrea el dolo, pues en muchos casos su conexidad con otros delitos conexos como el crimen organizado, narcotráfico, lavado de activos, extorsión, estafa; entre otros, dicha conducta delictiva se encuentra relacionada en la etapa de preejecución y/o ejecución. Es ahí

donde la ejecución de este tipo de delitos nos encontramos la vulneración de diversos derechos tales como lo señala (Francés, 2011), en el que se encuentran , la confiabilidad/ confidencialidad, integridad de sistemas informáticos y/o funcionamiento de sistemas que permiten el acceso a datos que conlleven a la lesión de bienes jurídicos de los sujetos pasivos:

*La **confiabilidad/confidencialidad**, esto es, el derecho a que los datos o la información no sean divulgados y los sistemas espiados.*	***La integridad**, exactitud y ausencia de alteraciones ilegales de los datos, la información, los sistemas informáticos y los procesos de tratamiento de información, busca garantizar la calidad, pureza, idoneidad y corrección de estos elementos.*	*La disponibilidad de los datos e infraestructuras permite garantizar su **funcionamiento, administración y acceso** adecuado.*

Figura 1: Fuente: Francés, M. L. (2011). La privacidad en el espacio virtual (riesgos y cauces de protección . Cuadernos de la Catedra de Seguridad Samantina .

A ello, resulta evidente que la teoría moderna aplicada al derecho penal resulta insuficiente ante este tipo de conductas delictivas, pues como ya se ha señalado, se basa en conductas exteriorizadas, (acción u omisión) los cuales para el operador de justicia genera una dificultad a la hora de poder condicionar dicha teoría a las conductas realizadas en el ciberespacio o mundo digital, pues ya solo el individualizar al sujeto activo conlleva a una dificultad ante este tipo de delitos digitales. Aunado a ello, se tiene en claro que la conducta humana constituye un objeto de valoración jurídica, esto es la tipicidad como tal, la antijuricidad y la culpabilidad en la "Teoría del Delito", siendo ahí la dificultad de comprobar la conducta realizada por el sujeto activo, pues al no ser exteriorizada y su difícil individualización genera una dificultad para el inicio de un proceso penal por parte del

representante de la sociedad (Fiscal), pues para ello debe reunir elementos de convicción que sustenten una tesis acorde a los hechos cometidos por el ciberdelincuente en el ciberespacio.

1.4.1.1. Elementos del Cibercrimen

Entre los elementos del cibercrimen como tal tenemos a la "virtualidad", pues conlleva a que la ejecución de la conducta delictiva por parte del sujeto activo sea realizada a través de una realidad virtual (mundo digital), mediante mecanismos no habituales para el operador de justicia y más difícil si el mismo no cuenta con conocimientos o especialización como tal. Es decir, conlleva a comportamientos realizados por el sujeto activo (ciberdelincuente) teniendo a la acción y decisión como principales pilares para la vía de ejecución de esta (dolo), siendo exteriorizadas a través de dispositivos informáticos, es desde esa postura que entendemos que la conducta realizada por el ciberdelincuente en el cibercrimen, consisten en una conducta dolosa.

A ello, se precisa que la cuestión de tener un dispositivo informático con acceso al internet (ciberespacio) no contempla a que una persona ya ejecutara una conducta delictiva como tal, pues es ahí donde debe aplicarse la razón y se constituyan los requisitos respectivos de conductas digitales delictivas según corresponda al tipo de delito ejecutado por el ciberdelincuente, pues resultaría inadecuado y/o atípico, imputar conductas delictivas a las personas que usan esas herramientas para el trabajo, estudio o simplemente diversión. A su vez, se debe tener siempre presente como punto de partida para la ejecución de las conductas digitales delictivas como tal la existencia del dolo, elemento indispensable a la hora de analizar este tipo de conductas digitales delictivas.

A su vez, se concuerda con lo señalado por el autor (Neira), respecto de la valoración jurídica sobre la conducta digital delictiva por parte del sujeto activo (ciberdelincuente) el cual sostiene que *"los actos preparatorios del delito inician cuando el sujeto entra en contacto con alguna pieza del hardware, considerado como un puente entre el campo del mundo físico y el inmaterial de la información y los datos informáticos, siendo este elemento vital para impartir órdenes al sistema informático a alcanzar con la finalidad criminosa del agente, que no es distinta a lesionar el bien jurídico; es decir el sujeto procede a captar dolosamente algún caudal informático para su provecho o el de terceros".*

Es decir, se tiene en la definición de los elementos de las conductas digitales la necesidad de que el sujeto activo conlleve al uso de un bien digital ya sea laptop, pc ,tablet u otro que le permita entrar al mundo digital y con su conducta dolosa mediante conocimientos previos busque su beneficio propio o de terceros. Sin embargo, ello se desvirtuaría en personas que no usen los bienes digitales como medio para la comisión de cualquiera de los supuestos de hecho presentes en la Parte Especial del Código Penal y la regulado en la Ley N°30096-Ley de Delitos Informáticos y su modificatoria con la Ley N° 30171, mientras no exista el dolo[2].Aunado a lo señalado, el sujeto que realiza este tipo de comportamientos no hace referencia a un sujeto especializado en temas informáticos, pues es suficiente el estar conectado virtualmente al sistema a vulnerar, en el sentido de realizar un tratamiento de información y/o sistemas de manera dolosa. En la doctrina internacional, nuevamente (Neira)

señala: *[…] dentro del concepto de tríada informática el primer elemento a tener en cuenta es el de usuario pues es la persona a satisfacer sus necesidades "informáticas" o de cualquier índole con un software dispuesta a impartirle órdenes para su funcionamiento*.

Como segundo elemento se encuentra el "software" pues el usuario para poder operar en el mundo digital, lo requiere como un elemento vital y finalmente el "hardware", que obra como un puente entre el campo del mundo físico y el de la información y los datos informáticos, por cuanto se refiere a los elementos de sistema que podemos apreciar con nuestros sentidos, es decir, son las piezas o partes físicas del mismo (tangibles). […] *Por lo que, los elementos referidos conllevan al conjunto de elementos necesarios y que deben estar o haber estado en contacto para que el sistema desarrolle alguna función; sin uno cualquiera de estos elementos el sistema sencillamente no opera*". [3]

1.4.2. Respecto a la diferencias entre la Prueba Digital y Evidencia Digital

Ante las características mencionadas en este tipo de conductas delictivas , encontramos que la necesidad de contar con la "prueba", siendo un elemento esencial para la aplicación del derecho, resulta pertinente, conducente y útil, pues es el elemento "probatorio" con el cual lograremos demostrar la conducta dolosa, lugar de ejecución, bienes jurídicos vulnerados y otros; los cuales conllevarán a la determinación de la conducta típica al sujeto activo mediante una debida motivación basado en un elemento probatorio y en consecuencia a la correcta administración de justicia ya sea en delitos informáticos y/o delitos conexos, lo cual finalizara

[3] Ibíd., pp. 39 y 40.

con un sentencia. En ese sentido, la "prueba" según el código procesal penal[4] señala que el juez debe tener en cuenta tres elementos importantes como las "reglas de la lógica", "la ciencia" y las "máximas de la experiencia", pues deberán ser usados para explicar sus conclusiones. Asimismo, debemos entender a la prueba por vestigios a la que necesita como primer elemento que el indicio esté probado y que la inferencia esté basada en los tres elementos antes referidos.

En ese sentido, para identificar el valor de la prueba denominada en una etapa procesal anterior a su valoración como tal "evidencia digital", resulta importante señalar que la misma sufrirá diversos estudios por parte de personal pericial quienes son los profesionales responsables mediante la aplicación de diversas técnicas "pericias" con el fin de obtener un informe pericial informático o llamado también "Análisis Digital Forense", debiendo esta respetar los procedimientos periciales así como las garantías constitucionales y procesales en pro de la legalidad y el debido proceso.

Es a partir del referido "peritaje" realizado a la "evidencia digital" adquiere la categoría de "prueba" una vez esta se encuentra valorada en la etapa de juicio conforme al Código Procesal Penal del 2004, siendo que mientras dicha pericia no haya sido valorada por el juez responsable, tendrá la calidad de "elemento de convicción", denominación distinta al concepto de "prueba". Entendemos que la denominación de "evidencia" conlleva a que la misma necesita una certeza científica, pues la misma como tal manipulada por personas no

[4] Código Procesal Penal 2004 - artículo 158° numeral 1 y 3,

especializadas en el tema, conllevaría a una evidencia perdida, pues no se habrían respetado las garantías procesales y/o constitucionales importante para una correcta sanción penal, lo que en la etapa de juicio no sería valorada como "prueba".

Sumándose a ello, la necesidad de que la ciencia ayude a la búsqueda de la verdad conlleva de manera indispensable las técnicas utilizadas por personal pericial, siendo necesario el diferenciar el "Análisis e investigación del Cibercrimen" y el Análisis de Informática Forense" como tal , teniendo una mejor explicación la siguiente figura citada:

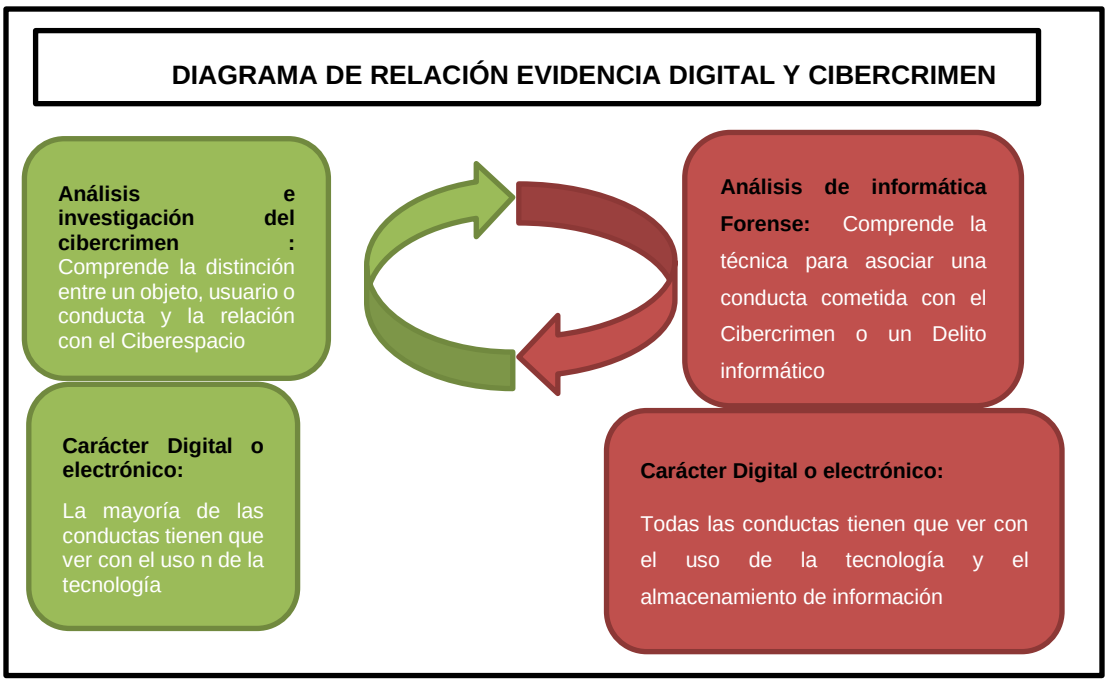


Figura N° 02: Tomado del artículo Aproximación del Cibercrimen en Colombia (primera parte), adaptado a la adopción de mejores prácticas para realizar el tratamiento y aseguramiento de la evidencia digital. https://www.researchgate.net/publication/341541797_APROXIMACION_METODOLOGICA_DEL_CIBERCRIMEN_EN_COLOMBIA_PRIMERA_PARTE

1.4.2.1. Procedimiento de integridad de la evidencia digital

Es así , que el Ministerio Público el 11 de agosto del año 2020 a través de la Resolución de la Gerencia General 365-2020-MP-FN-GG, aprueba la "**Guía de Análisis Digital Forense del Ministerio Público"**, la misma que abarca el tratamiento de la "Evidencia digital" y su procedimiento para mantener su integridad, la cual resulta indispensable comprender ello conforme a las (04) metodologías que este manual aplica, esto es: a) Identificación, b)Recolección, c)Adquisición y d) Preservación.

1.4.2.1.1 Respecto de la identificación

La misma consiste en dos procesos, física y lógica, siendo la primera la representación de datos dentro de un dispositivo tangible y la segunda a la representación virtual de datos de un dispositivo. Asimismo, dicho proceso de identificación implica varias características como :

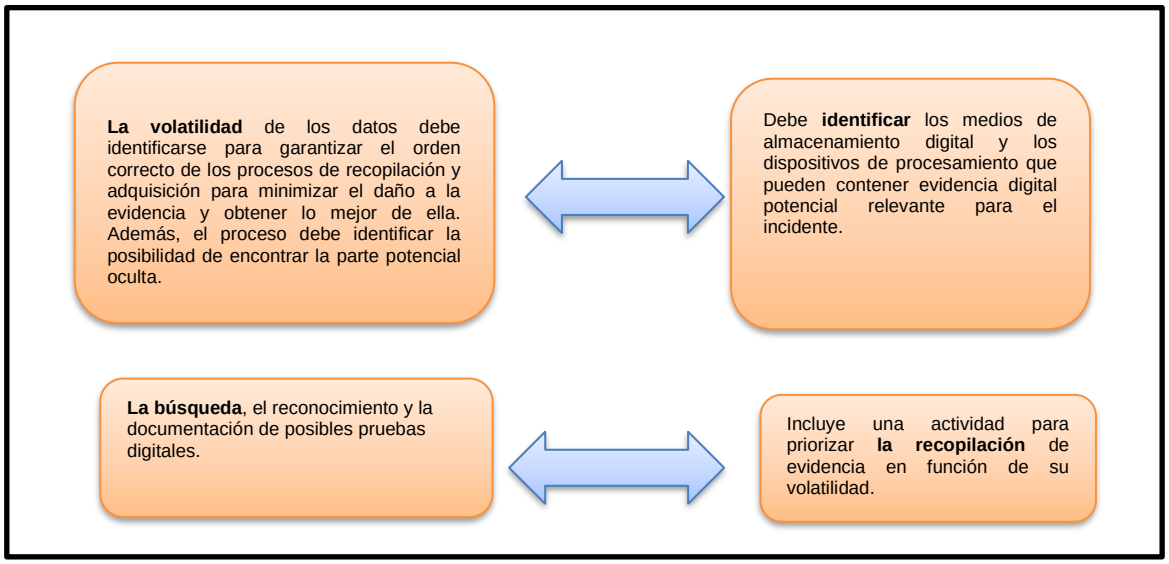


Figura 3: Realizado conforme "Guía de Análisis Digital Forense del Ministerio Público"

1.4.2.1.2 Respecto de la recolección

Una vez que dicha evidencia digital en sus aspectos física o lógica ha sido identificada, resulta necesario determinar si la misma será llevada a laboratorio forense o en su defecto el análisis digital se realiza in situ.

Dicha recopilación, consiste en el manejo que pueda tener , pues el contenido de dicha evidencia digital pueda estar en uno o dos estados, es decir cuando el sistema esta encendido o cuando el sistema esta apagado. Es a partir de ello, lo que determinara el tipo de uso de herramientas necesarias dependiendo del estado del dispositivo materia de análisis. Asimismo, la recolección de la evidencia conlleva a un procedimiento externo llamado “cadena de custodia”, lo que genera la confianza de que la evidencia no será modificada, cambiada e inclusive destruida, pues la persona que suscribe es la responsable ya que se encuentra bajo su custodia. Esto implica que el lacrado realizado a la evidencia es realizado por el Fiscal y el llenado del formato de cadena correspondiente, a fin de darle un valor legal, y posterior a ello su remisión a la Gerencia de Peritajes o Policía Forense, según corresponda el método de investigación dispuesto.

A ello, como lo mencionado, debemos tener claro las consideraciones para la recolección de la evidencia:

En sentido del equipo electrónico encendido:

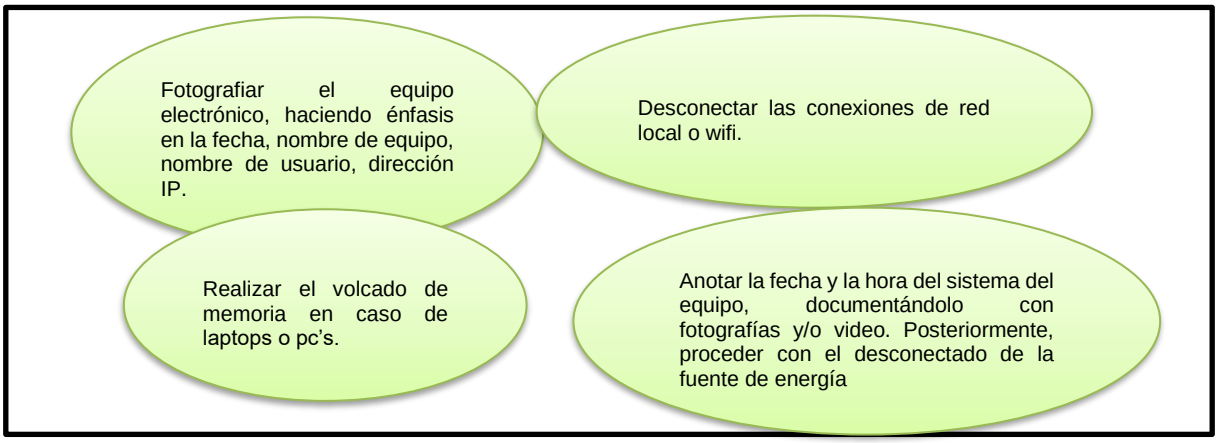


Figura 4: Conforme "Guía de Análisis Digital Forense del Ministerio Público.

En sentido del equipo electrónico apagado :

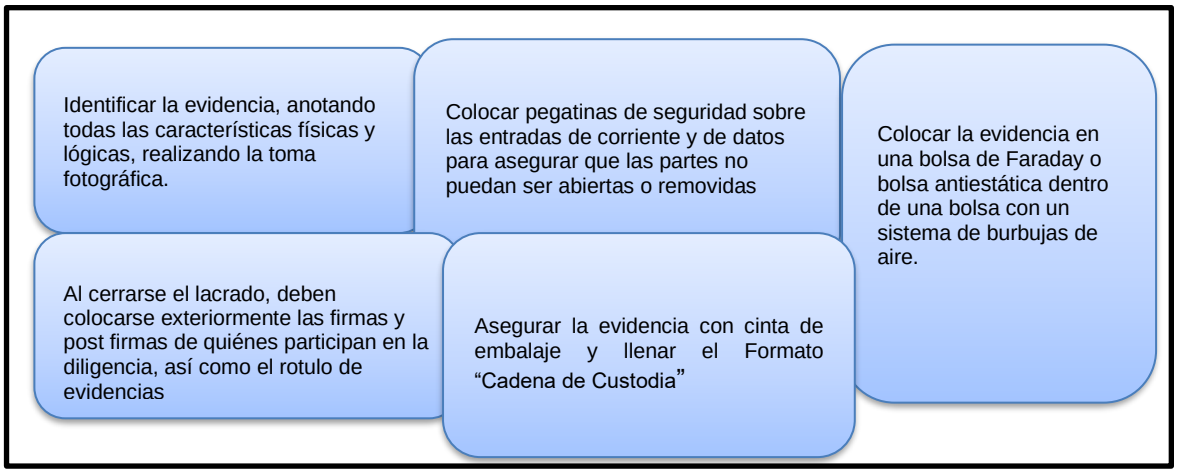


Figura 5: Conforme "Guía de Análisis Digital Forense del Ministerio Público"

1.4.2.1.3 Respecto de la Adquisición

Siguiendo las metodologías referidas, comprende entender el procedimiento de adquisición, esto conlleva a producir una copia de la evidencia digital o imágenes forense, es decir, el resultado produce una copia de la evidencia digital para su posterior análisis,

debiendo la misma estar asegurada y autenticada a través del código HASH5, que brindara un aseguramiento de la fuente original y que posterior a la copia que se realiza deba ser el mismo código. Posterior a ello, la documentación de los equipos y herramientas utilizadas como tal .

1.4.2.1.4 Respecto de la Preservación

Culminando la metodología referidas , su resultado implica la preservación de la evidencia digital, es decir la protección del dispositivo que conlleva a los datos digitales que contenga, debiendo esta mantenerse durante todo el proceso hasta su culminación.

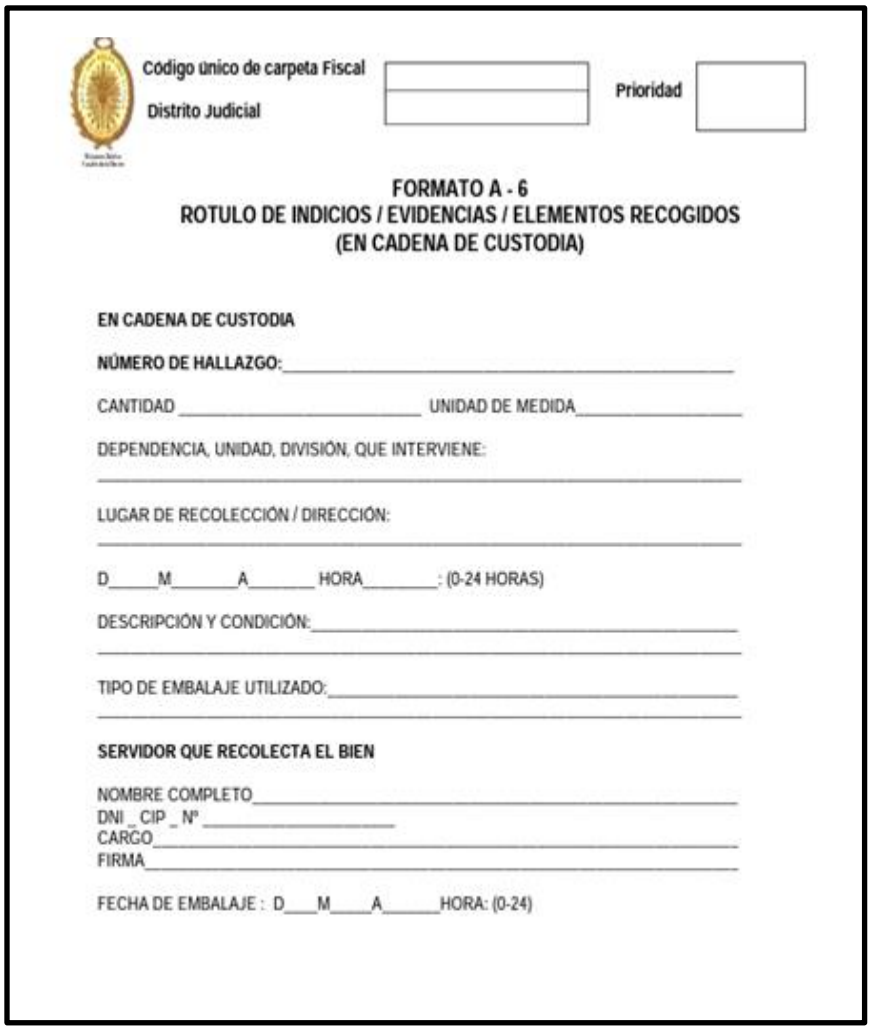
1.4.3. Etapas de la Cadena de custodia

Como lo señalamos, la correcta realización de la cadena de custodia conlleva un porcentaje de un resultado idóneo que se aplique a la evidencia digital, pues conlleva a su protección e intangibilidad de la misma como tal. Es así, que dicho procedimiento comienza con el llenado de datos respectivo en los formatos A-6 y A-7.

Esto es, en el formato A-6 , corresponde a la consignación de los datos más importantes, como el número de hallazgo, unidad de medida , cantidad de muestras , entidad que interviene, lugar de recolección, fecha, hora, descripción de la muestra , el embalaje utilizado para el lacrado y datos de servidor o funcionario que realiza el lacrado. Posterior a ello, corresponde

[5] Se trata de una función algorítmica de resumen seguro de un documento, volumen o dispositivo de almacenamiento cuyo valor es único. La probabilidad de que dos documentos distintos posean el mismo código HASH es prácticamente nula, es como el ADN de un archivo o volumen. https://www.eicyc.es/que_es_el_codigo_hash/ -Escuela Internacional de Criminología y Criminalística.

el llenado del formato A-7 , que corresponde a la cadena de personas que han tenido en custodia el bien, debiendo consignarse , fecha, hora, nombre, DNI , funcionario que autoriza la custodia y firma respectiva, y de ser necesario la precisión de alguna observación que tenga el sobre lacrado. Esto es, la última persona que suscribe dicho formato es la responsable de la custodia de la evidencia. Es así como, para una mejor ilustración se adjuntan los formatos referidos



Código único de carpeta Fiscal

Distrito Judicial

Prioridad

FORMATO A - 6
ROTULO DE INDICIOS / EVIDENCIAS / ELEMENTOS RECOGIDOS (EN CADENA DE CUSTODIA)

EN CADENA DE CUSTODIA

NÚMERO DE HALLAZGO:_____

CANTIDAD _____ UNIDAD DE MEDIDA_____

DEPENDENCIA, UNIDAD, DIVISIÓN, QUE INTERVIENE:
_____

LUGAR DE RECOLECCIÓN / DIRECCIÓN:
_____

D_____M_____A_____ HORA_____: (0-24 HORAS)

DESCRIPCIÓN Y CONDICIÓN:_____
_____

TIPO DE EMBALAJE UTILIZADO:_____
_____

SERVIDOR QUE RECOLECTA EL BIEN

NOMBRE COMPLETO_____
DNI _ CIP _ Nº _____
CARGO_____
FIRMA_____

FECHA DE EMBALAJE : D___M____A_____HORA: (0-24)

Figura n°6: Rotulo de Evidencias del Ministerio Público

Código único de carpeta Fiscal

Distrito Judicial

Prioridad

FORMATO A - 7
CADENA DE CUSTODIA (*)

FECHA D /M /A	HORA	NOMBRE COMPLETO DE QUIEN EMBALA BIENES INCAUTADOS	NOMBRE COMPLETO DEL TRO QUE TRANSPORTA BIENES INCAUTADOS	DNI \ CPI	CARGO / INSTITUCIÓN	FIRMA

REGISTRO DE CONTINUIDAD DE CUSTODIA DE ELEMENTOS MATERIALES, EVIDENCIAS Y BIENES INCAUTADOS (*)

FECH A D/M / A	HORA	NOMBRE COMPLETO DE QUIEN RECIBE BIENES INCAUTADOS	DNI \ CPI	CARGO / INSTITUCIÓN	CÓDIGO DE RECEPCIÓN	PROPÓSITO DEL TRASLADO	AUTORIDAD QUE AUTORIZA TRASLADO O DESTINO FINAL	FIRMA	OBSERVACIONES

IMPORTANTE :ESTE FORMATO DE CUSTODIA DEBE PERMANECER CON EL BIEN INCAUTADO

Versión 1 - Junio 2006

Figura n°7: Formato A-7 -Cadena de custodia.

A ello, a manera de una mejor ilustración, la siguiente imagen corresponde a (01) CPU, el cual se encuentra lacrado , con su formato A6, conforme a lo siguiente:

Figura N°8: Ejemplo de lacrado de (01) CPU y su rotulado con formato A6.

Seguidamente, la referida evidencia antes mostrada con su formato A-7

Figura N°9: Ejemplo de lacrado de (01) CPU y su rotulado con formato A6 y cadena de custodia A7.

En ese sentido, es de suma importancia comprender cuales son las etapas de su aplicación :

Figura 10: Conforme “Guía de Análisis Digital Forense del Ministerio Público”

Se debe entender a nivel de extracción o recolección, el procedimiento por el cual se obtiene preserva y conserva los indicios digitales físico o lógicos para su posterior traslado y análisis. Seguidamente, en relación con la preservación ,busca la protección mediante el lacrado y posterior a ello su formato de cadena de custodia, lo que brindara la seguridad de la evidencia para su traslado y posterior análisis.

Así, también el "Manual para el Recojo de Evidencia Digital", aprobado por el Ministerio del Interior a través de Resolución Ministerial N° 848-2019-IN, resulta ser una guía de actuación de procedimientos para los miembros de la Policía Nacional del Perú, con la finalidad de recabar y preservar en forma técnica y profesional el recojo de dispositivos de almacenamiento de datos y/o registros en la escena del crimen que estén relacionados con la comisión de un hecho delictivo, evitando su contaminación, supresión y/o alteración, ello en cumplimiento de lo establecido en el Decreto Legislativo N° 1267, que aprueba la Ley de la Policía Nacional del Perú, el cual en su artículo 2, numerales 8 y 9, señala que las funciones de la Policía Nacional del Perú, respecto al recojo y análisis de evidencia consiste en; *"…8) Obtener custodiar, asegurar, trasladar, y procesar indicios, evidencias y elementos probatorios, relacionados con la prevención e investigación del delito, poniéndolos oportunamente a disposición de la autoridad competente; 9) Practicar y emitir peritajes oficiales de criminalística para efecto de procesos judiciales y otros derivados de la función policial…"*, dichas funciones, enmarcadas dentro del ámbito de investigación, legitima a la Policía Nacional del Perú y le permite desarrollar su actuación dentro del marco de la Ley. A ello, el Decreto Legislativo 957, Código Procesal Penal, en su artículo 67, establece expresamente que la Policía Nacional del Perú tiene como función *"…reunir y asegurar los elementos de prueba que puedan servir para la aplicación de la Ley Penal…",* así mismo, en el artículo 68° establece sus atribuciones "*…d)Recoger y conservar los objetos e instrumentos relacionados con el delito, así como todo elemento material que pueda servir en la investigación…"*, por lo tanto, a nivel procesal, la actuación de la Policía Nacional del Perú se encuentra enmarcada dentro del ordenamiento jurídico. Sin embargo, la recolección de este tipo de evidencia digitales conlleva a un

procedimiento distinto al de una evidencia común, pues su característica principal recae en su intangibilidad y por ende enerva la necesidad de que su obtención se realice mediante un procedimiento de obtención especial a fin de que establezca la metodología de recolección y su preservación en el tiempo, procedimiento normativo que no existe en el Perú, pues solo existen manuales por parte de la Policía Nacional del Perú y el Ministerio Público.

En ese sentido, resulta necesario establecer un procedimiento normativo único , donde se establezca que personal profesional es el idóneo para la obtención de la evidencia digital y sus posteriores procedimientos, teniendo como premisa principal el correcto tratamiento, obtención, preservación de la evidencia digital en delitos de cibercrimen, la definición de "Evidencia Digital" y en qué casos resulta aplicable la normativa.

1.4.4. Tratamiento y Análisis de la Evidencia Digital

A ello, en la fase del tratamiento , encontramos la actuación del Perito de Análisis Digital Forense, el cual postulamos como el experto que tendrá a cargo de realizar el análisis a la evidencia digital ya sea en el laboratorio o en el campo de obtención. Seguidamente , resulta importante tener claro que la técnica aplicada por el perito es en base al objeto pericial que el fiscal requiere conforme a su metodología de investigación que aplique y aporte a su tesis fiscal. Entre lo principal para las metodologías de identificación y recolección de la evidencia digital se deben encontrar; nombre, fecha de inicio y fin, nombres y tipos de archivos, números de teléfonos, usuarios del sistema, correos electrónicos , páginas webs, valores numéricos y otros datos, que permitan enfocar el sentido de la pericia a realizar.

Sin perjuicio de lo antes mencionado, el rol principal del tratamiento e integridad de la evidencia digital busca que todo lo actuado sea realizado a la "evidencia digital primigenia", pues con ello se tiene la certeza de la integridad de la evidencia digital, esto es su valor probatorio, no conlleve a futuras solicitudes de nulidades por parte de las defensas técnicas, pues como ya lo mencionamos anteriormente este tipo de evidencias tiene un grado fácil de sufrir alteraciones y en los perores de los casos su eliminación.

Por lo que, en la fase tratamiento se encuentra la metodología elegida por el perito la cual debe otorgar resultados concordantes con el objeto pericial ordenado por el fiscal.

1.4.5. La actuación del fiscal en la recolección de la evidencia digital

- ***A nivel de diligencia urgentes e inaplazables***

El actor principal que brinda legalidad lo tiene el fiscal, y la recolección de la evidencia conlleva que el representante de la sociedad disponga y realice la diligencias necesarias de conformidad con lo dispuesto en el artículo 330.2 del Código Procesal Penal, para la obtención de la evidencia que requiera para sustentar su tesis fiscal, donde los participantes son necesariamente el fiscal, abogado defensa y peritos expertos. Sin embargo, no se encuentra establecido una normativa que detalle el procedimiento de obtención de evidencia digitales en casos de cibercrimen, que conlleven a crear la confiabilidad del procedimiento realizado con un estándar de calidad de buenas prácticas.

- ***A nivel de incautación que deviene del allanamiento***

En casos de la incautación, nos encontramos con lo establecido en el artículo 317 del Código Procesal Penal, esto es que los efectos provenientes de la infracción penal o los instrumentos con que se hubiere ejecutado, así como los objetos del delito permitidos por la Ley, siempre que exista peligro por la demora , pueden ser incautados durante las primeras diligencias y en el curso de la Investigación Preparatoria, ya sea por la Policía o el Ministerio Público. A ello, el fiscal deberá requerir inmediatamente al juez de la Investigación Preparatoria la expedición de una resolución confirmatoria, la cual se emitirá, sin tramite alguno, en el plazo de dos días de conformidad con el artículo 316 del referido código. En el mismo sentido, no se encuentra establecido una normativa que detalle el procedimiento de obtención de evidencia digitales en casos de cibercrimen, a nivel de incautación.

1.4.6. Casos Nacionales

Para poder comprender la magnitud de la afectación de estas conductas digitales delictivas, debemos conocerlo en la práctica, esto es casos reales que hayan sucedido a nivel nacional, teniendo para ello los siguientes ejemplos :

- "**El Cartel del Fraude"**[6] consiste en un caso de un fraude informático por S/. 354,310.15 soles, mediante la transferencias ilegales vía internet en Áncash. Esto se logró a partir de lo resuelto por el Décimo Primer Juzgado de la Corte Superior de Justicia de Lima, quien autorizó el allanamiento de cinco inmuebles de los

6 https://andina.pe/agencia/noticia-desarticulan-banda-acusada-fraude-informatico-mas-s-350000-782863.aspx

implicados donde se incautaron celulares, equipos de cómputo, así como dispositivos electrónicos vinculados a la investigación, en la cual los ciberdelincuentes lograron vulnerar cuentas bancarias de la INVESTMENT PROJECT SAC mediante el "phishing", la cual consistió que el usuario entregue su información bancaria sin sospechar que la página web que se lo solicita es falsa. Es así, que de ello se realizaron tres transacciones online a la cuenta de la Institución CEGNE de Jesús EIRL. mediante la falsificación de documentos la cual dividió el dinero en montos de hasta 3,000 soles para nuevas transferencias vía internet hacia 32 cuentas bancarias de terceros en el cual los dueños de las cuentas bancarias recibieron comisiones de entre 50 y 70 soles por la creación de la cuenta bancaria, la entrega de la tarjeta y la clave para el retiro del dinero, lo que fueron captados por redes sociales como Facebook, Instagram y otros . A ello, indico la policía (DIVINDAT) en su oportunidad: "Los propietarios no conocían la identidad real de las personas que les ofrecieron el dinero. Se tuvo que trabajar (en su identificación) desde cero con los seudónimos", rastreándose las redes sociales y se emplearon herramientas digitales para identificar a los involucrados.

- "**Los Ciberdelincuentes de Ate"**[7] habrían realizado 22 transacciones luego de recibir la transferencia ilegal de parte del municipio de San Borja. Los ciberdelincuentes habrían realizado 22 transacciones luego de recibir la transferencia ilegal de parte del municipio, tras la denuncia, se bloquearon las

7 https://andina.pe/agencia/noticia-detienen-ciberdelincuentes-habrian-robado-s-5-millones-a-municipalidad-833098.aspx

cuentas receptoras para evitar pérdidas económicas. Sin embargo, se estimó que 593 mil soles fueron retirados luego de las transacciones ilegales.

- **Hackeo de sistema RENIEC por ciberdelincuentes se roban casi un millón de soles**[8]. : El caso consiste en que ciberdelincuentes , habiendo hackeado el sistema de RENIEC, habría tenido acceso a los datos personales de las personas beneficiadas con el bono universal de S/. 760 soles. Dicho ataque era realizado en coordinación vía internet , los cuales fueron detectados por dos expertos en ciberseguridad. A ello, indican que de dentro de la evidencia encontrada, se encuentran mensajes de cobros realizados por los beneficiado sin haber sido cobrados por los mismos beneficiarios.

En los casos referidos, se advierte las conductas dolosas, utilización de hardware y software respectivamente para la vulneración de sistemas, por la cual se ejecutaron los delitos digitales.

Asimismo, debemos tener en cuenta que estos delitos abarcan daños patrimoniales de suma importancia, así como la información confidencial (cuentas bancarias, correos electrónicos u otros). Es así, como resulta necesario identificar el procedimiento a seguir para la obtención de la evidencia digital que generen convicción y pueda motivar debidamente la resolución que corresponda por parte del operador de

[8] https://ancashaldia.com/bono-universal-ciberdelincuentes-se-roban-casi-un-millon-de-soles-tras-hackear-sistema-reniec/

justicia (juez) y para ello generar jurisprudencia en el ordenamiento jurídico, respecto a este tema poco tratado.

1.5. Marco Teórico Doctrinario

1.5.1. Diferencia Delitos informáticos y Cibercrimen

El profesor (Casanova, 2006) realiza una diferencia entre los conceptos de "Delitos Informáticos" y el Cibercrimen", en el cual define al primero como los elementos informáticos para la ejecución de delitos y al segundo como la posterior generación de conductas delictivas en el que interviene la comunicación, abierta, cerrada o de uso restringido.

Siendo entonces el uso irrestricto y doloso del "internet" como elemento esencial para la comisión delictiva digital. Sumado a ello, (Davara, 2002), señala respecto a las dificultades en el cibercrimen surgen a partir de la intangibilidad de la información y bien jurídico a proteger, teniendo en cuenta el desvanecimiento de las teorías jurídicas tradicionales y sumado que en el cibercrimen el "anonimato" protege al delincuente informático, suma una barrera para recolectar las pruebas de los hechos delictivos de carácter universal del delito informático; las mismas que se encuentran en la física, lógica, y del ámbito jurídico de seguimiento, procesamiento y enjuiciamiento en estos hechos delictivos.

En otras palabras, el cibercrimen, consiste en las conductas llevadas a cabo, en un territorio virtual y/o digital, donde el sujeto pasivo se encuentra en una constante vulneración, pues este tipo de delitos como ya se ha referido, es de difícil seguimiento,

pues la ubicación del ciberdelincuente se encuentra como tal en un mundo digital, el cual no es de fácil acceso, (Deep Web u otros), sumado a que las herramientas tecnológicas buscan la dirección de la IP del dispositivo pero no delimita al sujeto activo (usuario) como tal, lo que genera una impunidad jurídica. Es en esa medida que el sujeto pasivo deberá establecer medidas de seguridad para la protección de sus bienes jurídico.

1.6. Marco Teórico Normativo Nacional

Nuestro ordenamiento jurídico actualmente plantea para la erradicación de este tipo de conductas digitales delictivas los siguientes dispositivos legales :

- Ley N°30096, Ley de delitos informáticos, del 21 de octubre de 2013, modificada por la Ley N°30171, de fecha 17 de febrero de 2014. *El referido cuerpo legal tiene por objeto prevenir y sancionar las conductas ilícitas que afecten los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas con la utilización de tecnologías de la información o de la comunicación , con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.*
- Ley N°30171- Ley que modifica la Ley de Delitos Informáticos en los artículos 2,3,4,5,7,8 y 10.
- Resolución de la Fiscalía de la Nación N° 1503-2020-MP-FN, de fecha 30 de diciembre de 2020: *Cuerpo normativo mediante la cual se crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima.*
- La Guía de Análisis Digital Forense del Ministerio Público, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG, del 11 de agosto de 2020.

- El "Manual para el Recojo de Evidencia Digital", aprobado por el Ministerio del Interior a través de Resolución Ministerial N° 848-2019-IN.

1.7. Marco Normativo Internacional

1.7.1. Convenio de Budapest

El "Convenio sobre la Ciberdelincuencia", llamado "Convenio de Budapest" adoptado el 23 de noviembre del 2001 en la ciudad de Budapest y ratificado en nuestro ordenamiento jurídico a través de Decreto Supremo N° 010-209-RE de fecha 09 de marzo del 2019 con entrada en vigencia el 01 de diciembre del 2019, consiste en un tratado internacional que nace para cubrir las necesidades de los países miembros del Consejo de Europa con el fin de hacer frente a los delitos informáticos a través de mecanismos de homologación de normas, estandarización de procesos penales y cooperación internacional.

En ese sentido, es de tener en cuenta que las tecnologías de vanguardia utilizadas en el día a día en nuestra región son las que brindan países como China, EE.UU y países de Europa como Alemania, Rusia y otros, tecnologías que hace unos 10 a 15 años eran impensable, siendo en pleno año 2022 en la cual se utilizan smarthphone , tablets ,laptop, relojes smart y entre otros, nos permiten tener acceso a aplicativos conectados a cuentas bancarias personales, laborales, correo electrónico, así como realizar pago de servicios, compras electrónicas, redes sociales entre otro, lo que implica información muy valiosa para la ejecución de diversas conductas digitales delictivas.

Es en sentido, el artículo 14 del referido convenio establece el ámbito de aplicación a la conducta criminal referida, la misma que deberá encontrarse en un entorno

de comisión donde se tenga como resultado la importancia de la utilización de medios digitales; es decir, se toma en cuenta la utilización de sistemas y datos informáticos, el objeto mismo sobre el que se produce el delito y el instrumento para la comisión delictiva como soporte de información.

Es ahí, donde aparece la importancia del conocimiento del procedimiento idóneo para la obtención de la evidencia digital, pues es el elemento probatorio que permitirá concretizar la responsabilidad jurídica del ciberdelincuente (sujeto activo) .

1.7.2. Norma Internacional ISO/IEC 27037-2012

Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" - *"Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales"*

La referida norma internacional, es una norma ISO que consiste en el procedimiento de la actuación pericial en el escenario de la recolección, identificación, adquisición y preservación de la evidencia digital[9] pero no aporta respecto al procedimiento del análisis puesto que la metodología forense es decisión profesional propia de cada perito, la cual no se encuentra normalizada en el Perú por el INDECOPI, ente encargado de realizar las normas técnicas nacionales, siendo un marco normativo

[9] https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

de relevancia jurídica pues establecería un estándar de buenas prácticas para la obtención de la evidencia digital.

Es en ese sentido, nuestro ordenamiento jurídico no ha procedido a la adecuación de esta norma ISO en los procedimientos para la obtención de la evidencia digital en el ámbito nacional, dejando un vacío en el ámbito jurídico respecto de un procedimiento de suma importancia en la medida que el Cibercrimen se actualiza en nuestra sociedad conforme al estilo de vida de nuestra sociedad.

Es así que esta norma internacional ISO plantea el procedimiento formal para la obtención de la evidencia digital y los separa en tres principios: a) Relevancia , b) Confidencialidad y la c) Suficiencia ,principios necesarios para la obtención de la evidencia digital.

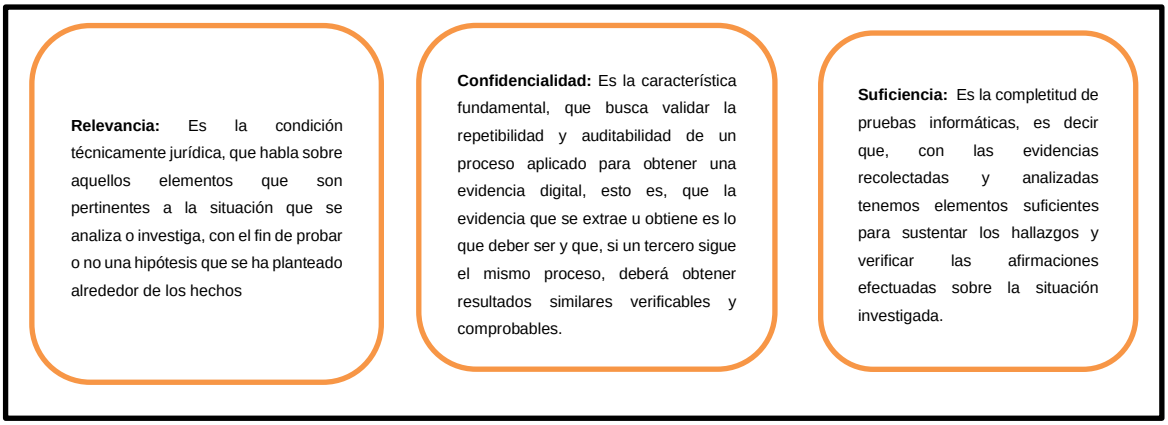


Figura n°11: Elaborado conforme: https://insecurityit.blogspot.com/2013/09/reflexiones-sobre-la-norma-isoiec.html

A ello, contempla a los individuos denominados como la (Digital Evidence First Responder (DEFRs) o especialista en evidencia digital de primera intervención y (Digital

Evidence Specialist (DESs) o especialista en evidencia digital, los cuales constituyen a los especialistas en respuestas a los incidentes y a los directores de laboratorios forenses. La identificación del personal responsable asegura la correcta gestión de la evidencia digital se realice ante prácticas de estándar internacional con el objetivo de que la investigación sea realizada de una manera unificada en el ámbito internacional, preservando la integridad y autenticidad de la evidencia digital.

La referida norma internacional desde nuestra percepción busca la confiabilidad y/o integridad de la evidencia digital en casos de cibercrimen, ello a partir del estándar de calidad internacional para la obtención de la evidencia digital, norma internacional que debe tener su "norma técnica nacional" por parte del INDECOPI para que ella pueda ser aplicada en nuestro ordenamiento jurídico y genere confianza tanto en la parte de la defensa técnica como al fiscal ante el Juez respectivo.

1.7.3. República de Argentina

Lo aplicado por la República de Argentina mediante UFECI - Unidad Fiscal Especializada en Ciberdelincuencia- DIGCRI Dirección General de Cooperación Regional e Internacional, mediante el instrumento Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero del año 2020, consisten en recomendaciones sistematizadas se centran exclusivamente en la preservación y obtención de evidencia electrónica almacenada por los proveedores de servicios, y no en la obtención en tiempo real de comunicaciones.

1.7.4. República de Chile

La referida república contempla la recolección de la evidencia digital a través de la Ley N° 21.459-Delitos Informáticos y recolección de la evidencia digital de fecha 20 de junio

2022[10], la cual mediante el artículo 12, *indica: Cuando la investigación de los delitos contemplados en los artículos 1°, 2°,3°, 4°, 5° y 7° de esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los preceptos precedentemente señalados, el juez de garantía, a petición del Ministerio Público, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.*

Como es de advertirse, en la referida ley internacional recientemente establece al representante de la sociedad (fiscalía) como el que dirige y actúe en la recolección de la evidencia de ámbito digital, la misma que debe estar sujeta bajo los supuesto delitos de la referida norma penal.

1.7.5. República Federal de México

Ante la premisa de investigación, México contempla a través del Poder Judicial de la Federación del Consejo de la Judicatura Federal, "*Lineamientos para la obtención y tratamiento de los recursos informáticos y /o evidencias digitales",* teniendo como finalidad establecer recomendaciones para la obtención y tratamiento de recursos informáticos y/o evidencia digital que ayuden en las investigaciones. Señalando el referido documento como

[10] https://www.pensamientopenal.com.ar/legislacion/90172-chile-ley-ndeg-21459-delitos-informaticos-y-recoleccion-evidencia-digital

inicio que para la recolección de dicha evidencia digital deban constituirse al menos dos personas autorizadas por la Dirección General de Tecnologías de la Información, debiendo previamente haberse identificado los recursos informáticos, el personal, el cual deberá indicar el lugar, hora, fecha, nombre y órgano jurisdiccional o área administrativa, así como la interacción posterior y su resguardo en el lugar. Aunado a ello, establece como el perfil requerido un profesional con conocimientos debe ser capaz de extraer y recuperar datos, evidencias electrónicas, análisis de información, manejo de herramientas y software forense, redacción de informes, estructuras y protocolos y otros, lo que se acerca a un personal de perito propiamente dicho.

Aunado a ello, cuenta con el "Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales ,aprobado mediante el "Acuerdo General del Pleno del Consejo de la Judicatura Federal" de fecha 17 de junio del 2016, que en concreto establece métodos y procedimientos que aseguren la detección, recolección, manejo, autentificación, análisis, procesamiento y resguardo de los recursos informáticos y/o evidencias digitales obtenidos de las computadoras, redes informáticas, discos duros, memorias de almacenamiento masivo de información (USB), discos compactos, tabletas, teléfonos alámbricos y móviles, sistemas de correo electrónico, mensajería sincrónica o instantánea asincrónica, intercambio de archivos en línea, redes sociales, y en general de cualquier dispositivo de comunicación, almacenamiento y transmisión de datos, con la finalidad de integrar al marco constitucional y normativo las investigaciones y procedimientos que realizan en su respectivo ámbito de competencia las Secretarías Ejecutivas de Vigilancia, Información y Evaluación, y la de Disciplina, así como la Dirección General de Tecnologías de la

Información, todas del Consejo de la Judicatura Federal y, por su parte, la Visitaduría Judicial y la Contraloría del Poder Judicial de la Federación.

Como es de apreciarse, el establecer el procedimiento idóneo, así como el personal, genera que la obtención de la evidencia digital se encuentre bajo la tutela de un marco normativo establecido lo que genera confianza y buenas prácticas en la recolección y/o obtención de la evidencia digital.

1.8. Organismos internacionales relevantes contra el "Cibercrimen"

A raíz del nacimiento del convenio del Budapest contra el Cibercrimen, países de Europa decidieron crear organismos institucionales con fin de realizar el seguimiento de estas conductas digitales delictivas, con aras de realizar trabajos de prevención y en los mejores casos su erradicación, es así como nacen los siguientes organismos internacionales:

- **Centro europeo de ciberdelincuencia (EUROPOL)** [11]

La Europol nació en el Centro Europeo de Ciberdelincuencia (EC3) en el año 2013, con el fin de fortalecer la respuesta policial a la ciberdelincuencia en la Unión Europea y para proteger a las personas , empresas y gobiernos europeos , siendo su creación una contribución significativa a la lucha contra el ciberdelito; brindando ciberseguridad, pues ha estado involucrado en decenas de operaciones de alto perfil y cientos de despliegues de apoyo operativo sobre el terreno que resultaron en cientos de arrestos, y ha analizado cientos de miles de archivos, la gran mayoría de los cuales han demostrado ser maliciosos.

[11] https://www.europol.europa.eu/ec3

- **EINSA** [12]

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) la cual se encarga de la política cibernética en la Unión Europea para la búsqueda de la confiabilidad de los productos, servicios y procesos de Tecnologías de la información y la Comunicación (TIC), esto mediante la utilización de esquemas de certificación de ciberseguridad mediante la cooperación con los Estados miembros y los organismos de la Unión Europea, siendo su pilar principal Europa, a fin de que se encuentre listo para los desafíos cibernéticos que se presenten.

1.9. Instituciones nacionales relevantes contra el "Cibercrimen"

La importancia de la "evidencia digital" consiste en un instrumento bastante desconocido en el ámbito judicial y en general por los profesionales del Derecho, generando contradicciones, lagunas o vacíos etc, su desconocimiento genera sentencias, no motivadas debidamente o incluso el llegar plantear sentencias que no son acorde a la realidad de los hechos, es ahí donde el cibercrimen llega a ganar a nuestro sistema de justicia, pues los administradores como tal necesitan la capacitación constante para la mejor resolución de los casos. Es en ese sentido, que en nuestro ordenamiento jurídico contempla a dos entidades especializadas que ayudan a la recolección de la evidencia digital , siendo desde la Policía Nacional del Perú a la DIVINDAT -División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú" y del Ministerio Público a través de la Unidad Fiscal Especializada en Ciberdelincuencia.

[12] https://www.enisa.europa.eu/

1.9.1. La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT)[13]

El cibercrimen como tal, conlleva a conductas digitales delictivas que se originan ante los crecientes avances de las tecnologías, así como de ciberdelincuentes que llevan a otro nivel su conducta delictiva, que, si bien no afecta físicamente, afecta frecuentemente en el ámbito íntimo y patrimonial. En ese sentido, esta unidad policial especializada, conlleva a entender que, si existen "ciberdelincuentes", existen "ciberpolicías" que buscan constantemente erradicar a los sujetos activos (ciberdelincuentes) los cuales utilizan diversas modalidades delictivas del Cibercrimen como las siguientes:

- **Skimming**: Entiéndase a la copia de la banda de la tarjeta para luego a transferir la información confidencial a otra tarjeta en blanco.
- **Pharming**: Mecanismo utilizado para llegar a las cuentas bancarias de las víctimas.
- **Phishing:** Buscan acceder a información personal mediante el envío de correos electrónicos falsos, es decir la pesca digital.
- **Cryptojacking:** Consiste en el uso de manera subrepticia de la potencia de los ordenadores para generar criptomoneda.

A ello, resulta importante conocer las cifras de denuncias de esos delitos en nuestro país, pues es de vital importancia que modalidad o modalidades son las utilizadas por los sujetos activos, así como los requerimientos del Ministerio Público realizados a la referida unidad especializada policial por lo que tenemos lo siguiente:

Tabla n° 1

[13] https://www.mininter.gob.pe/content/ciberpolic%C3%AD-contra-delitos-inform%C3%A1ticos

Denuncias de Delitos Informáticos investigados por la DIVINDAT del año 2013 al 2020										
DELITO	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**	**%**
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	0.4
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	
Suplantación de identidad	**10**	**101**	**114**	**134**	**132**	**227**	**247**	**572**	**1537**	**12.6 %**
Suplantación de identidad	9	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños , niñas y adolescentes con fines sexuales por medios tecnológicos	**9**	**9**			**29**	**94**	**49**	**100**	**290**	**2.4 %**
Contra la indemnidad sexual de menores										
Proposiciones a niños , niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra Datos y sistemas informáticos	**38**	**62**	**47**	**47**	**104**	**126**	**159**	**177**	**760**	**6.2 %**
Acceso Ilícito	11	42	1	1	49	84	129	151	468	
Acceso Ilícito a una base de datos										
Atentado a la integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la Intimidad y el secreto de las comunicaciones						**3**	**2**	**8**	**13**	**01%**
Interceptación de datos								2	2	
Interceptación de datos personales								1	1	
Tráfico llegal de datos						3	2	5	10	
Fraude In formatico	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2 %**
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0 %**

Nota: Cuadro realizado en el Informe N°04-Ciberdelincuencia en el Perú: Pauta para una investigación especializada el cual fue adaptado del informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020 y de información remitida por el Coronel Orlando Mendieta, jefe de DIVINDAT, a la OFAEC de fecha 20 de enero de 2021.

Siendo así, se advierte un gran crecimiento de casos referentes a cibercrimen, los cuales conforme el cuadro precedente durante la etapa del Covid-19 (2020), el mundo comenzó a depender más de la tecnología, también conllevo a que la delincuencia sea en el entorno digital.

1.9.2. La Unidad Fiscal Especializada en Ciberdelincuencia con competencia nacional.

Al respecto, nuestro ordenamiento jurídico con el transcurso del tiempo va en un constante avance para la reducción y /o erradicación de dichas conductas digitales

delictivas y eso se refleja con la última Unidad Especializada en Ciberdelincuencia por parte del Ministerio Público, dicha unidad tiene por objeto principal el efectuar la orientación técnico-jurídica en las investigaciones de los delitos cometidos por medios tecnológicos, que comienza desde la identificación y preservación de la evidencia digital. Aunado a ello, resulta importante comprender cuales son las formas de afectación de las víctimas de dichas conductas digitales delictivas, pues también resulta en un elemento necesario a la hora de plantear las estrategias de ciberseguridad a los usuarios, estrategia que el fiscal pueda establecer. Es así como, la Unidad Fiscal Especializada en Ciberdelincuencia en base a la información brindada por la DIVINDAT, ha establecido las formas de afectación de bienes jurídicos más realizados:

Tabla n°2

Formas de Afectación a las víctimas de delitos informáticos
De manera económica
Existe Afectación Psicológica y moral en el tema de acoso sexual y suplantación de identidad informática .
Afectación a la intimidad , a la libertad personal. Necesidad de establecer otros medios de protección; las victimas por el uso de sus te cuentas de redes sociales pierden el uso de estas, y tienen que crear otros perfiles.
Frustración, sentimiento de injusticia al no identificarse a los autores
A la libertad e indemnidad sexual

Nota: Cuadro realizado conforme a señalado en el Informe N°04-Ciberdelincuencia en el Perú: Pauta para una inves especializada

.

Sumándose a ello, el poder tener en concreto una estadística en un rango determinado de años las denuncias por dichos delitos informáticos a nivel nacional hasta el año 2020, surge la siguiente tabla:

Tabla n° 03

Denuncias por delitos informáticos registradas en Fiscalías Penales Comunes y Fiscalías Mix octubre del 2013 a julio del 2020.

Delito Subgenérico	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**	**%**

Lima	67	325	550	708	1495	2366	3717	1116	10 340	47.68%
Lima Norte	3	24	24	99	174	357	717	220	1618	7.46%
Arequipa	1	18	47	155	255	291	506	115	1388	6.40 %
Lima Este	3	17	26	53	147	251	603	183	1283	5.92%
La Libertad	3	20	35	36	94	213	487	232	1120	5.16%
Lambayeque	1	11	31	82	119	182	326	124	876	4.04%
Callao	3	15	16	52	57	130	332	101	696	3.21%
Lima Sur	1	4	9	27	52	120	355	119	687	3.17%
Cusco	4	33	42	41	79	81	*176*	81	537	2.48%
Ica		3	10	22	24	91	195	57	402	1.85%
Piura	3	10	33	15	34	68	134	40	337	1.55%
Loreto	1	7	15	24	48	93	100	32	320	1.48%
Moquegua	1	2	1	5	19	46	141	47	262	1.21%
Santa		3	3	6	36	20	90	27	185	0.85%
Huánuco		3	2	3	30	25	61	36	160	0.74%
Junín		5	7	5	16	44	52	27	156	0.72%
Ucayali		4	6	9	18	42	44	15	139	0.64%
San Martin		3	4	6	30	18	51	20	130	0.64%
Amazonas	2	1	2	6	30	18	51	20	130	0.60%
Cajamarca	1	3	2	4	5	21	59	31	126	0.58%
Tacna		6		5	4	20	50	15	91	0.42%
Sullana		3	12	9	12	15	25	15	91	0.42%
Huaura		4	6	8	11	20	32	10	91	0.42%
Ancash		2	4	5	12	20	35	8	86	0.40%
Lima Noroeste			2	6	3	15	31	5	48	0.33%
Puno	1		3	3	12	8	15	6	48	0.22%
Apurímac		3	1	1	2	18	13	4	42	0.19%
Madre de Dios		2	3		3	1	23		32	0.19%
Tumbes		4	3	2	5	6	8	1	29	0.13%
Huancavelica	1	1	2	3		4	17	1	29	0.15%
Cañete		1	1	1	1	1	15	3	23	0.11%
Selva Central			3		1	1	5	8	18	0.08%
Pasco	1				2	4	4	1	12	0.08%
Total	**99**	**540**	**907**	**1410**	**2841**	**4648**	**8504**	**2738**	**21 687**	**100.00%**

Nota: Cuadro realizado en el Informe N°04-Ciberdelincuencia en el Perú: Pauta para una investigación especializada Adaptado de reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.

Por lo que, como es de apreciarse, estos delitos digitales van en un aumento constante y van generando carga procesal, resultando de importancia el elemento de todo caso digital, esto es la "evidencia digital", la cual varia conforme al delito cometido.

1.10. Marco Teórico normativo referente a la Prueba.

Nuestro ordenamiento jurídico plantea diversas definiciones acerca del concepto de "Prueba", pero no precisa diversas interrogantes, es decir ¿Que entendemos como prueba? ¿Cuáles son las características de la prueba? Al respecto el profesor (Castro, 2015) refiere una definición de "prueba" como:

"La actividad de las partes procesales, que buscan la acreditación necesaria de actividades de demostración para obtener convicción ante el juez sobre los hechos por ellas afirmados, intervenida por el órgano jurisdiccional bajo la vigencia de los principios de contradicción, igualdad y de las garantías".

Sumado a ello, debemos tener en cuenta sobre el "derecho a probar", conforme a lo señalado por el Tribunal Constitucional:

EXP. N° 03997-2013-PHC/TC, LIMA *NORTE* "*El derecho a probar es uno de los componentes elementales del derecho a la tutela procesal efectiva, pues, como ya lo ha señalado este Tribunal en la sentencia recaída en el Expediente N° 010-2002-AI, constituye un elemento implícito de tal derecho…".***

Como se puede observar, en referencia a la prueba y al derecho a probar, es necesaria la interacción de elementos objetivos con el fin de buscar la verdad. Entonces, enfocando al tema materia de investigación: *¿Como delimitamos la evidencia digital en los casos de cibercrimen?* Son muchos los aspectos de los cuales buscamos una mejor definición en base a las opiniones jurídicas de diversos autores, así como la definición de las misma en dispositivos normativos, así como nos planteamos la interrogante de ¿ Que

entendemos como evidencia digital? En ese sentido, podemos entender como evidencia digital lo señalado por (Hernandez, 2014)

> "*(..) a cualquier información obtenida a partir de un dispositivo electrónico, o medio digital, que sirve para adquirir convencimiento de la certeza de un hecho".*

1.11. Definiciones básicas

A continuación, procederé a realizar la definición de palabras claves en la presente investigación, lo cual permitirá tener una mejor noción y asociarlas con las circunstancias presentadas y por señalar en la presente investigación.

- **Cibercrimen**: (Casabona, 2006) : *Consiste en cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o internet y en el que el ordenador, teléfono o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito.*
- **Prueba Indiciaria:** (Seva, 1996)**:** *Se dirige a demostrar la certeza de unos hechos (indicios) que no son constitutivos de delito objeto de acusación, pero de los que a través de la lógica y de las reglas de la experiencia pueden inferirse los hechos delictivos y la participación del acusado; que ha de motivarse en función de un nexo causal y coherente entre los hechos probados -indicios- y el que se trate de probar -delito.*
- **Delitos informáticos:** (Urdaneta, 2002) *Consiste en aquellas conductas ilícitas sancionadas por el ordenamiento jurídico, donde se hace uso indebido de las computadoras como medio o instrumento para la comisión de un delito, también a aquellas otras conductas que van dirigidas en contra de las computadoras convirtiendo a éstas en su fin u objetivo.*

- **Peritaje:** (A.Herrera, Administración de la Empresa Constructora , 2013) *Consiste en el estudio y examen que realiza un profesional especializado sobre un problema encomendado para luego entregar su informe o dictamen con rango pericial con sujeción a lo dispuesto por la ley"*
- **Evidencia digital**: *Consiste en cualquier información que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". Entendiéndose que el único fin de la evidencia es saber con la mayor exactitud posible los hechos facticos, encontrándonos como ejemplos de evidencias: a) Un disco duro, Pendrive, etc, b) Restos de instalación, c) Archivos temporales, d) Un proceso en ejecución, e) Un fichero en disco, f) El Uptime de un sistema, g) Una cookie en un disco duro, h) Un log en un fichero, i) El último acceso a un fichero.* (Guidelines for Management of It Evidence , 2003)
- **Análisis Digital Forense**: *Se define como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas en un proceso judicial. López (2007),*
- **Cadena de Custodia:** (Darahuge, 2016), *Consiste en el procedimiento controlado que se aplica a los indicios materiales (prueba indiciaria) relacionados con un hecho delictivo o no, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene como fin asegurar la inocuidad y esterilidad técnica en el manejo de los mismos, evitando alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva por orden judicial.*

- **Prueba Pericial:** *Elemento probatorio con una gran porcentaje de certeza, pues se utilizan métodos científicos e informáticos, los cuales otorgan un gran valor de probanza,* (A.Herrera, Administración de la Empresa Constructora, 2013).
- **Hacker:** *Sujetos que acceden al sistema informático sin autorización, con el fin de buscar información para ellos mismos o por "pedido" de terceros, constituyendo en una dificultad no poder entrar a un sistema o a un sitio que se proponga.*
- **Cracker:** *Sujetos que de manera dolosa inutiliza los sistemas de protección de aplicaciones informáticas mediante programas elaborados para tal fin con la intención de provocar daño.*
- **Phreaker:** *Sujetos que utiliza técnicas de fraude en telefonía ya sea esta digital o analógica.*
- **Virucker:** *Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan, pero no dañan, y los malignos que destruyen información o impiden trabajar.*
- **Sniffers:** *Sujetos con la finalidad de obtener determinados conocimientos, entendiéndose a la práctica de examinar todos los paquetes informáticos que pasan por unja red, de modo que abren y captan las informaciones necesarias (contraseñas) para la realización de futuras actividades.*
- **Pirata informático:** *Sujeto que reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor.*

- **Hash :** *Algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.*

Respecto del bien jurídico, tipificación objetiva, subjetiva y autoría en el cibercrimen (Regulación española)

La regulación del código penal español plantea la tipificación al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo sistemas informáticos u otros derivados. Sin embargo, a partir de la decisión Marco 2005/22/JAI de fecha 24 de febrero del 2005[14], referente a los ataques contra los sistemas de información del código penal (Ley Orgánica 5/2010, de fecha 22 de junio que modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal [15]) realizó una intervención para crear la regulación de los delitos informáticos al Derecho de la Unión Europea y establecer una definición para la determinación como tal de este delito pues, ello implicaría la utilización de tecnologías mediante herramientas como software y hardware necesarias para establecer y/o determinar el concepto materia de investigación penal. Es así que podemos entender al:

[14] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.boe.es/doue/2005/069/L00067-00071.pdf

[15] Página 7 capitulo XIV chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf

- ***Bien Jurídico:*** *Acarrea al sujeto pasivo a través del patrimonio , conocimiento, la alcanzabilidad del mismo y la protección de los sistemas informáticos, como bienes jurídicos tutelados.* (Terreros, 2014)
- ***Tipicidad objetiva:*** *Consiste en el comportamiento doloso que no integra el tipo penal porque una vez que el sujeto activo se encuentra en el sistema, es necesario que ponga en acto ciertas acciones dolosas identificadas en el tipo penal que buscan el aniquilamiento del objeto material en cuestión. Pues el sujeto activo se encuentra exento de sanción penal, siempre que no vaya a actos que tienen como objeto la producción de daños.*
- ***Tipicidad Subjetiva:*** *Consiste en el daño informático ocasionado a causa de una conducta dolosa siendo por dolo directo como dolo eventual.*
- ***Autoría:*** *Consiste en la autoría mediata como la forma más común de comisión de hechos, debiendo ser personas que tengan conocimientos específicos de la red (internet).*
- ***Sujeto Activo:*** *Los infractores de la ley penal en materia de delitos informáticos no son delincuentes comunes y corrientes, sino que, por el contrario, son personas especializadas en la materia informática.* (MANSON, 2013)

1.12. Formulación del problema

1.12.1. Problema General

- ¿Cuál es el Procedimiento Normativo para la obtención de la evidencia digital en el Cibercrimen?

1.12.2. Problemas Especifico 1

- ¿ Resulta idóneo la actividad policial en la obtención de evidencia digital en el cibercrimen?

1.12.3. Problemas Especifico 2

- ¿ Es idónea la norma que regula la obtención de evidencia digital en el cibercrimen ?

1.13. Objetivos

1.13.1. Objetivos General

- Determinar el procedimiento normativo para la obtención de la evidencia digital en el cibercrimen

1.13.2. Objetivos Específicos 1

- Determinar la idoneidad de la actividad policial en la obtención de evidencia digital en el cibercrimen

1.13.3. Objetivo Especifico 2

- Determinar la idoneidad de la norma que regula la obtención de evidencia digital en el cibercrimen.

1.14. Hipótesis

En el Perú no existe un procedimiento normativo y/o norma técnica nacional para la obtención de la evidencia digital, más solo existen los instrumentos "manuales" de evidencia digital del Ministerio Público y Policía Nacional, ambos aprobados mediante resoluciones ministeriales, los cuales consisten en manuales con criterios diferentes para la obtención del elemento probatorio "evidencia digital". Sumado a ello, dichos instrumentos no regulan un procedimiento normativo unificado que sea de carácter obligatorio para la obtención de la evidencia digital en delitos de cibercrimen, así como el personal idóneo,

respectivo. En ese sentido, resulta necesario establecer y/o la creación de un instrumento normativo que unifique criterios respecto a la obtención y preservación de la evidencia digital en casos de cibercrimen en el Perú.

1.15. Justificación

La presente investigación desarrolla un tema necesario en la ámbito penal peruano en referencia a la evidencia digital como resultado de conductas digitales delictivas (huellas digitales), estando a que es un tema poco tratado en nuestro ordenamiento jurídico. En ese sentido, para contrarrestar al Cibercrimen en el año 2013, la Ley N°30096-Ley de Delitos Informáticos comienza a regular dichas conductas digitales delictivas y consecuentemente el 01 de diciembre del 2019 nuestro ordenamiento jurídico ratifica el convenio de Budapest adoptado el 23 de noviembre del 2001, esto es 18 años de demora en la ratificación de un convenio importante para la erradicación de este tipo de conductas que día a día va actualizándose conforme al avance de la tecnología en nuestro país, así como en el mundo.

Sin embargo, no se cuenta con procedimiento normativo respecto de la obtención de la evidencia digital, siendo la justificación regular dicho procedimiento, a fin de brindar soluciones para la determinación del procedimiento de obtención idóneo, de buenas prácticas, así como el personal respectivo.

CAPÍTULO II: METODOLOGÍA

2.1 Tipo de Investigación

2.1.1 De acuerdo con su finalidad

El tipo de estudio que se desarrolla en el presente trabajo de investigación es básico, pues implica introducir conocimiento y teoría (SARLO, 2006), teniendo la característica de provisional, lo que permitirá corregir o desarrollar un modelo de investigación que resulta necesario para institucionalizar la investigación jurídica.

2.1.2 De acuerdo a su enfoque

La presente investigación se ha optado por realizar de manera "cualitativa", ello mediante entrevistas a profesionales , el cual ha sido validado por (02) expertos en la materia, siendo ellos peritos informáticos del área de análisis digital forense de la Gerencia de Peritajes del Ministerio Público , el personal experto idóneo en el tema de la evidencia digital.

2.1.3 De acuerdo a su diseño

La presente investigación optara conforme al actual Estado de Emergencia Sanitaria, la no experimental, siendo notables las dificultades sanitaria que emplea el covid-19, que en base a sierra es el más frecuente en las investigaciones pues emplea técnicas de recolección de información basada en la observación directa, en la entrevista y en el análisis de documentos (derecho comparado y doctrina), mostrando el objeto de investigación sin intervención.

2.1.4 De acuerdo a su alcance

Finalmente, he de indicar que según el alcance de la presente investigación será de manera descriptiva, pues se buscará el responder ciertas variables para la complementación de una teoría jurídica, (LUCIO, 2017)

2.2 Unidad de Estudio

2.2.1 Unidad de estudio A :

Análisis documental nacional e internacional referente al objetivo general y especifico de estudio materia de investigación.

2.2.2 Unidad de estudio B

Abogados penalistas del Ministerio Público y Peritos informáticos especializados en el análisis digital forense de la Gerencia de Peritajes del Ministerio Público que responderán respecto al objetivo general y especifico de estudio materia de investigación.

2.3 Población

La población de estudio es un conjunto de casos, definido, limitado y accesible, que formará el referente para la elección de la muestra, y que cumple con una serie de criterios predeterminados (Arias-Gómez, Villasís-Keever, & Miranda Novales, 2016)

La población de la presente investigación se divide en 2 grupos :

Población A : Consiste en profesionales entre los cuales se encuentran abogados penalistas y peritos especializados en análisis digital forense (Ingenieros en sistemas) de la Gerencia de Peritajes del Ministerio Público.

Población B: Consiste en el análisis en el ámbito nacional de (02) Manuales, (01) Guía de procedimiento y en el ámbito internacional se encuentra (01) protocolo, (01) Guía , (01) Ley y (01) Norma Internacional ISO, todo referente a la obtención de la evidencia digital.

2.2.2 Muestra

Entendemos como muestra a la esencia de un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población (Sampieri, 2010)

Teniendo en cuenta las variables utilizadas y en base al tipo de investigación y las dificultades que ello conlleva conforme al actual estado de emergencia por el covid-19, será cualitativa y/o documental.

2.2.2.1 Tipo de muestra

El tipo de muestra es no probabilístico, estando a que la elección fue realizada conforme a las características de la investigación y decisión propia del autor de la presente investigación, pues cumplen con responder la hipótesis de la investigación.

- **Tipo de muestra para la población A**: *Entrevistas a (08) profesionales de los (10) con los cuales contaba la presente investigación, entre los cuales se encuentran abogados penalistas y Peritos de análisis digital forense de la Gerencia de Peritajes del Ministerio Público., preguntas la cuales fueron revisadas y aprobadas por 2 expertos en el tema quienes tienen la función vital de revisar las preguntas según su experiencia profesional, debiendo indicar que el experto 1 es el encargado del área de análisis digital forense de la Gerencia de Peritajes del Ministerio Público con competencia a nivel nacional, es decir*

el área que realiza pericias informáticas de delitos comunes y especializados a nivel nacional, experto que agrega un alto valor a la presente investigación, pues conforme a las diversas pericias realizadas a lo largo de su trayectoria ha validado las preguntas que ayudaran a responder el objetivo general y los objetivos específicos materia de investigación, además de que han sido parte del equipo de peritos que participó en la elaboración de la Guía de Análisis Digital Forense del Ministerio Público. Por lo que, estando al tipo de investigación , el tipo de muestreo no es probabilístico estando a que no resulta necesario la evaluación de estadísticas.

- **Tipo de muestra para la población B:** *el análisis documental (doctrina y legislación comparada), respecto al tema materia de investigación. Por lo que, estando al tipo de investigación, el tipo de muestreo no es probabilístico estando a que no resulta necesario la evaluación de estadísticas.*

2.2.2.2 Muestras seleccionadas

Tabla N° 4

Muestra seleccionada de la Población A-Entrevistas

N°	Nombre	Profesional	Cargo	Extracción de datos
1	**Sharom Cáceres Medina**	Abogada	Abogada en el Ministerio Público	Responden al objeto materia de investigación y estando a su participación en diligencias urgentes e inaplazables de forma in situ, así como su participación en allanamientos e incautaciones en diversas investigaciones donde se
2	**Nelida Choque Cruz**	Abogada	Abogada en el Ministerio Público	
3	**Martin Christian Cárdenas Castillo**	Abogado	Abogado de la Tercera Fiscalía Superior Nacional Especializada en Delitos de Lavado de Activos	

4	**Jhomira Selene Morau Zuasnabar**	Abogado	Abogada- Asistente en Función Fiscal de la Tercera Fiscalía Superior Nacional Especializada en Delitos de Lavado de Activos	obtienen evidencias comunes y digitales (Lacrado de PC, USB, Celulares y otros)
5	**Karin Elizabeth Cuchache Mendez**	Abogada	Abogada en el Ministerio Público	
6	**Helmut Nixon Meza**	Ingeniero en Sistemas	Perito Líder del área de Análisis Digital Forense de la Gerencia de Peritajes el Ministerio Público	Aportaron respuestas conforme al objeto general materia de investigación, conforme a su profesión como ingenieros en sistema especializados en análisis digital forense y su participación en la realización de la Guía de Análisis Digital Forense del Ministerio Público.
7	**Arturo Lazarte Vilcamango**	Ingeniero en Sistemas	Perito del área de Análisis Digital Forense de la Gerencia de Peritajes el Ministerio Público	
8	**Tania Gonzales Mego**	Ingeniero en Sistemas	Perito del área de Análisis Digital Forense de la Gerencia de Peritajes el Ministerio Público	

Nota: Elaboración propia.

Tabla: 5

Muestra seleccionada de la población B-Análisis Documental

País	Documento	Extracción de datos
Perú	La Guía de Análisis Digital Forense del Ministerio Público, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG, del 11 de agosto de 2020.	Establece lineamientos y procedimientos para el desarrollo de las actividades periciales a fin de contribuir al cumplimiento de las funciones del área de Análisis Digital Forense de la Oficina de Peritajes.
	"Manual para el Recojo de Evidencia Digital", aprobado por el Ministerio del Interior a través de Resolución Ministerial N° 848-2019-IN.	Establece procedimientos para el adecuado recojo de medios de almacenamiento digital en la escena del crimen, garantizando su seguridad e integridad, con la finalidad de proteger la evidencia digital con valor probatorio para una investigación. (…)

	Manual de Evidencia Digital -Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi	Guía de procedimiento para las actuaciones de personal policial, técnicos y fiscales , cuando en una escena del crimen se encuentran dispositivos de almacenamiento informático.
Argentina	Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero del año 2020- UFECI - Unidad Fiscal Especializada en Ciberdelincuencia-DIGCRI Dirección General de Cooperación Regional e Internacional	Pautas de recomendaciones para la preservación y obtención de la evidencia electrónica almacenada por los proveedores de servicios y no en la obtención en tiempo real de comunicaciones.
Chile	Ley N° 21.459-Delitos Informáticos y recolección de la evidencia digital de fecha 20 de junio 2022	Cuando la investigación de los delitos contemplados en los artículos 1°, 2°,3°, 4°, 5° y 7° de esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los preceptos precedentemente señalados, el juez de garantía, a petición del Ministerio Público, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.
México	Poder Judicial de la Federación del Consejo de la Judicatura Federal, "Lineamientos para la obtención y tratamiento de los recursos informáticos y /o evidencias digitales" "Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales ,aprobado mediante el "Acuerdo General del Pleno del Consejo de la Judicatura Federal" de fecha 17 de junio del 2016	Recomendaciones para la obtención de la evidencia digital y tratamiento de recursos informáticos y/o evidencia digital.
Organismos Internacional de Estandarización	Norma Internacional ISO/IEC 27037-2012 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and	Consiste en pautas para el manejo de la evidencia digital entre lo que se encuentra la sistematización de la identificación, recolección,

	preservation of digital evidence" - "Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales"	adquisición y preservación de la misma, ,m procesos deben diseñarse para mantener la integridad de la evidencia y con una metodología aceptable para contribuir a su admisibilidad en procesos legales. Según esta norma la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital.

Nota: Elaboración propia.

2.3 Técnicas e instrumentos de recolección y análisis de datos

La técnicas utilizadas para la recolección de datos fueron mediante análisis documental, con el cual se busca la validez, siguiendo con la doctrina que nos aporta la confiablidad de la información en base al planteamiento de teorías, pues esta conlleva a información de calidad. Sumando a ello, se encuentra las entrevistas a expertos que aportan información relevante para la presente investigación. Teniendo en cuenta en referencia al formulario de preguntas, ello conforme a lo señalado por el Portal Crece Negocios (K, 2015), *"... Es un método para recolectar información donde precedentemente se interroga de manera verbal o escrita a un grupo de individuos con el propósito de obtener una determinada información necesaria para la investigación".*

Sumado a ello, en referencia a las técnica cualitativas, encontramos el método Delphi y los métodos de opinión. (Sancho, 2001) en el cual podemos emplear:

- Realizar entrevistas
- Recoger las respuestas
- Obtención de resultados

Procedimiento el cual esta investigación abarca, pues a raíz de las respuestas obtenidas de los expertos y el análisis documental antes señalado lograremos demostrar nuestra hipótesis. Sumado a ello, es de indicar que se han podido identificar problemáticas que no son materia de investigación pero que merecen ser materia de otro trabajo de investigación como un aporte pendiente al ordenamiento jurídico.

2.4 Criterios Utilizados

A continuación, los criterios de selección utilizados serán los artículos buscados Google Académico *"un buscador de Google enfocado y especializado en búsqueda de un contenido más científico-académico",* la misma que comprendió la verificación de la información en "línea", así como su descarga en archivo PDF, la búsqueda de casos relevantes, los cuales contiene valiosa información referente al tema de los antecedentes, así como la documentación para el análisis documental de ámbito nacional e internacional , estando a las características del tema investigado.

Asimismo, se encuentra el buscador SciELO, que consiste *"en una biblioteca electrónica, donde se puede compartir información y conocimiento orientado al desarrollo de la comunicación científica; en particular, de las revistas que tienen las colecciones nacionales e internacionales".*

También se utilizó Dialnet, el cual *"es un portal que comprende y proporciona un acceso a documentos que han sido publicados en España, publicados en idioma español y otra lengua".* Así como la normativa del Convenio de Budapest, como elemento jurídico internacional junto con la normativa nacional ya señalada en párrafos anteriores.

Finalmente, la información de libre acceso brindada por la Oficina de Análisis Estratégico contra la Criminalidad del Ministerio Público, mediante su informe de Análisis N°04-Ciberdelincuencia en el Perú: *Pautas para una Investigación Fiscal Especializada en referencia a la recientemente creada Unidad Fiscal Especializada en Ciberdelincuencia*, conforme la resolución de la Fiscalía de la Nación N° 1503-2020-MP-FN de fecha 30 de diciembre del 2020, en el cual se observa el trabajo realizado por la DIVINDAT, en conjunto con el Ministerio Público, mediante diferentes criterios.

2.5 Procedimiento de recolección de datos

Las recolección de datos se basa en las respuesta obtenidas mediante las entrevistas realizadas a profesionales y expertos, los cuales fueron obtenidos a través de la guía de preguntas aprobado por los expertos , el cual fue remitida a los profesionales en la obtención de los resultados que ayuden a responder la problemática jurídica de la presente investigación, debiendo precisar que conforme al tema tratado y en base a las entrevistas, las mismas fueron recabadas a través de correo electrónico Gmail , WhatsApp, Google Meet y de forma física.

Tabla N° 6

Documentos analizados para los antecedentes- Fuentes de Extracción

Fuente	Búsqueda	Depurados	Seleccionados
Google Académico	10	6	4
Scielo	4	2	2
Dialnet	10	8	2
Total	24	16	8

Nota: Se muestra en cantidades y porcentajes de documentos que fueron considerados respecto a la fuente de donde provienen.

Tabla N° 7

Muestra seleccionadas de la población A - Fuentes de Extracción

Fuente	Recolectados	Depurados	Seleccionados	Motivo de depuración
Entrevistas	10	2	8	El desconocimiento de los que es un Hardware y Software , así como del análisis de las respuesta , las mismas no brindar un aporte a la investigación.
Total	10	2	8	

Nota: Creación propia

Tabla N° 8

Muestra seleccionadas de la población B - Fuentes de Extracción

Fuente	Búsqueda	Depurados	Seleccionados	Motivo de depuración
Google Académico	15	7	8	No se encontraban acorde al objeto materia de investigación
Total	15	7	8	

Nota: Creación propia

Finalmente, se procedió a trabajar con los seleccionados y a depurar los que no guardan relación con el objeto general y objeto especifico 1 y 2 materia de investigación.

2.6 Procedimientos de tratamientos y análisis de datos.

Al respecto, se indica que la metodología utilizada cualitativa, esto es el determinar el procedimiento normativo idóneo para la obtención de la evidencia digital en delitos de cibercrimen, partiendo de ello el tener una noción del concepto como tal, el personal idóneo. Sumado a ello, como se indicó, mediante la aplicación de entrevistas y análisis documental aplicando el derecho comparado.

2.7 Aspecto Éticos

Al respecto, debo indicar que los criterios utilizados en la presente investigación son la ética profesional, honestidad, integridad, disciplina que el suscrito cuenta para la realización de la presente investigación. Sumado a ello, el respecto que el suscrito realiza a las conclusiones optadas en las investigaciones previas respetando los derechos de autor y la aplicación correcta del manual APA en el presente trabajo de investigación lo que también implico un respeto a las indicaciones del asesor como punto de partida y a lo señalado sobre la investigación por parte de los expertos en el tema como fueron los peritos , quienes contribuyeron al resultado de la presente investigación.

CAPÍTULO III: RESULTADOS

Antes de comenzar con los resultados, es preciso señalar lo dicho por SCHNEIER:

"*Si Ud. piensa que la tecnología puede resolver sus problemas de seguridad, entonces Ud. no entiende los problemas de seguridad y tampoco entiende la tecnología"*

Conforme a la metodología de investigación, así como los instrumentos utilizados, se procede a presentar los resultados obtenidos los cuales brindan respuestas al objetivo general y los específicos, los cuales se han categorizado sobre el análisis documental referente al ámbito jurídico nacional, internacional.

Respecto al Objetivo General ¿Cuál es el Procedimiento Normativo para la obtención de la evidencia digital en el Cibercrimen?

Para responder el referido objetivo general se realizaron las siguientes preguntas:

- ¿Conoce usted algún reglamento y/o directiva que regule la obtención de la evidencia digital en delitos de cibercrimen?
- ¿En el Perú existe algún procedimiento normativo que regule la obtención de la evidencia digital para delitos de cibercrimen ?

Tabla n°9

Resultados respecto de la muestra A sobre objetivo general -Entrevistas

Entrevistado	Respuesta
Sharom Cáceres Medina	La letrada indica que no conoce una normativa que regule la obtención de la evidencia digital, así como desconoce un procedimiento normativo referente a ello.
Nelida Choque Cruz	La letrada indica que no conoce una normativa que regule la obtención de la evidencia digital, así como no tiene idea de la existencia de un procedimiento normativo referente a ello.
Martin Christian Cárdenas Castillo	El letrado señala que actualmente conoce la Resolución Ministerial N° 848-2019-IN que el Ministerio del Interior público a fin de aprobar el Manual para el recojo de la evidencia digital. Sin embargo, no puede precisar respecto si en el Perú existe algún procedimiento normativo.
Jhomira Selene Morau Zuasnabar	La letrada indica que no conoce una normativa que regule la obtención de la evidencia digital, así como desconoce un procedimiento normativo referente a ello.
Karin Elizabeth Cuchache Mendez	La letrada indica que no conoce una normativa que regule la obtención de la evidencia digital, así como indica que, si conoce un procedimiento normativo, pero no recuerda la normativa.
Helmut Nixon Meza	El experto indica que no conoce reglamento y/o directiva . Sin embargo, señala sobre los procedimiento que regulan la obtención de la evidencia digital el Manual de evidencia digital del Ministerio de Justicia y Derechos Humanos y la Guía de Análisis Digital Forense del Ministerio Público
Arturo Lazarte Vilcamango	El experto indica que respecto al reglamento y/o directiva el manual de evidencia digital del Ministerio Público, así como respecto al procedimiento El manual de evidencia digital del Ministerio Público

Tania Gonzales Mego	La experta indica respecto al reglamento y/o directiva conoce la Ley N° 30171 Ley que modifica la Ley N° 30096, Ley de Delitos Informáticos, Directiva N.º 03-19-2015-DIRGEN-PNP/EMG-DIRASOPE-B, Normas y procedimientos policiales para proteger la escena del delito y garantizar la cadena de custodia, aprobada mediante RD. N°751- 2015-DIRGEN-EMG-PNP y la Resolución Legislativa N° 30913, del 12 de febrero de 2019; y, ratificado a través del Decreto Supremo N° 010-2019-RE, del 9 de marzo de 2019. "Convenio sobre la Ciberdelincuencia". Sobre el procedimiento normativo que regule la evidencia digital para delitos de cibercrimen no conoce alguna normativa al respecto.

NOTA: Elaboración propia

Tabla n°10

Resultados respecto de la muestra B sobe objetivo general -Análisis Documental

Ámbito	Documento	Resultado
Perú	La Guía de Análisis Digital Forense del Ministerio Público, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG, del 11 de agosto de 2020.	La presente guía acapara lineamientos y/o procedimientos para el análisis digital forense, esto es después la obtención de la evidencia digital, es decir el trabajo en la evidencia obtenida.
	"Manual para el Recojo de Evidencia Digital", aprobado por el Ministerio del Interior a través de Resolución Ministerial N° 848-2019-IN.	Dicho documento establece el procedimiento para el recojo de la evidencia digital por personal policial en la escena del crimen. Esto conlleva a no solo evidencias digitales sino todo tipo de evidencias. la Policía Nacional del Perú, resulta ser un organismo de apoyo en la lucha contra el cibercrimen, pero no resulta el personal idóneo para este tipo de delitos digitales que maneja conocimiento de estándar digital como tal , global y de constante avance. Es en estas situaciones que contempla la problemática jurídica en la obtención de la evidencia digital, pues si bien la DIVINDAT, como división especializada en estos delitos apoya al Ministerio Público, resulta necesaria la implementación de un procedimiento normativo estándar que contemple el procedimiento acorde a las situaciones delictivas digitales generadas a partir de los ciberdelincuentes. Es

		en esa medida, que dicho manual no contempla los supuestos necesarios en estos delitos digitales complejos que sea realizado por personal idóneo, especializado con la logística necesaria que conlleve a un resultado integro que comprometa la situación jurídica del ciberdelincuente y establezca su responsabilidad mediante un elemento probatorio debidamente trabajado y respetando lineamientos estandarizados, lineamientos que no existe en el Perú, lo que no garantiza a nivel procesal la aplicación de un debido procedimiento acorde a la conducta delictiva y ello genere una imputabilidad al sujeto activo (ciberdelincuente).
	Manual de Evidencia Digital -Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi	El proyecto el cual establece una guía de procedimientos para que el personal policial, técnico y fiscal para la obtención de dispositivos informáticos. Esto es, establece el procedimiento la obtención de evidencia que pueda encontrarse en algún hardware, pero no en algún software, el cual si necesita un procedimiento con más especialidad como la ubicación de servidores, direcciones VPN u otros, el cual debe ser realizado por personal experto como ingenieros en sistemas pero de la revisión en el ámbito nacional resulta como el más completo para la obtención de la evidencia digital en casos de cibercrimen, pero no tiene rango normativo como si cuenta la república de chile, quien nos lleva la delantera.
Argentina	Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero del año 2020-UFECI - Unidad Fiscal Especializada en Ciberdelincuencia-DIGCRI Dirección General de Cooperación Regional e Internacional	La referida guía establece el procedimiento para la obtención de evidencia electrónica almacenada por los proveedores de servicio (datos de usuario, historial de conexiones , contenido de mensajes), así como las comunicaciones en tiempo real. Es decir, se enfoca más al ámbito del Software como tal.
Chile	Ley N° 21.459-Delitos Informáticos y recolección de la	La presente norma en su artículo 12 establece el procedimiento a realizar cuando se encuentre en situaciones de sospecha de la realización de delitos informáticos, señala que es el Ministerio Público el ente

	evidencia digital de fecha 20 de junio 2022	autorizado para realizar las diligencias urgentes e inaplazables y que podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, así como el establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos.
México	Poder Judicial de la Federación del Consejo de la Judicatura Federal, "Lineamientos para la obtención y tratamiento de los recursos informáticos y /o evidencias digitales" "Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales ,aprobado mediante el "Acuerdo General del Pleno del Consejo de la Judicatura Federal" de fecha 17 de junio del 2016	Dichos documentos, tiene por finalidad establecer recomendaciones para la obtención y tratamiento de la evidencia digital, debiendo constituirse 02 personas de la Dirección General de Tecnologías de la Información , a fin de que realicen dicha obtención. A ello, el "Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales ,aprobado mediante el "Acuerdo General del Pleno del Consejo de la Judicatura Federal" de fecha 17 de junio del 2016, que en concreto establece métodos y procedimientos que aseguren la detección, recolección, manejo, autentificación, análisis, procesamiento y resguardo de los recursos informáticos y/o evidencias digitales obtenidos de las computadoras, redes informáticas, discos duros, memorias de almacenamiento masivo de información (USB), discos compactos, tabletas, teléfonos alámbricos y móviles, sistemas de correo electrónico, mensajería sincrónica o instantánea asincrónica, intercambio de archivos en línea, redes sociales, y en general de cualquier dispositivo de comunicación, almacenamiento y transmisión de datos, con la finalidad de integrar al marco constitucional y normativo las investigaciones y procedimientos que realizan en su respectivo ámbito de competencia las Secretarías Ejecutivas de Vigilancia, Información y Evaluación, y la de Disciplina, así como la Dirección General de Tecnologías de la Información, todas del Consejo de la Judicatura Federal y, por su parte, la Visitaduría Judicial y la Contraloría del Poder Judicial de la Federación.
Organismos	Norma Internacional ISO/IEC 27037-2012	Esta normativa internacional por excelencia establece las principios necesarios para la obtención de la

Internacional de Estandarización	"Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" - "Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales"	evidencia digital, esto es la relevancia, confiabilidad y suficiencia. Dichos principios establecen un estándar de calidad que debe respetar el procedimiento para la la obtención de la evidencia digital . La referida norma internacional busca la confiabilidad y/o integridad de la evidencia digital en casos de cibercrimen, ello a partir del estándar para la obtención de la evidencia digital, norma internacional que debe tener su "norma técnica nacional" por parte del INDECOPI para que ella pueda ser aplicada en nuestro ordenamiento jurídico y genere confianza tanto en la parte de la defensa técnica como al fiscal ante el Juez respectivo.

NOTA: Elaboración propia

Respecto al Objetivo específico 1: Determinar la idoneidad de la actividad policial en la obtención de la evidencia digital en el cibercrimen.

Para responder el referido objetivo se realizaron las siguientes preguntas:

- ¿Cree usted que la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT) es la unidad idónea para la obtención de la evidencia digital para delitos de cibercrimen?
- ¿Cree usted que la Policía Nacional del Perú , se encuentra capacitada para realizar el procedimiento de obtención de evidencia digital en delitos de cibercrimen ?
- ¿Cree usted que la Policía Nacional del Perú, cuenta con la logística de recursos humanos y tecnológicos para la obtención de la evidencia digital en delitos de cibercrimen?

Tabla N°11

Resultado respecto de la muestra A sobre objetivo específico 1 -Entrevistas

Entrevistado	Respuesta
Sharom Cáceres Medina	La letrada indica que la DIVINDAT no es la unidad idónea para la obtención de la evidencia digital en casos de cibercrimen . Asimismo, señala que la policía no se encuentra capacitada pues la misma institución no cuenta con la logística necesaria para realizar dicho trabajo especializado.
Nelida Choque Cruz	La letrada indica que la DIVINDAT si es la unidad idónea para la obtención de la evidencia digital en casos de cibercrimen . Asimismo, señala que la policía si se encuentra capacitada, pero señala que dicha institución no cuenta con la logística necesaria para realizar dicho trabajo especializado.
Martin Christian Cárdenas Castillo	El letrado señala que las investigaciones y con apoyo de esta división sería la única , puesto que no hay otra que pueda realizar las diligencias especiales ante los delitos informáticos. Asimismo, señala que la PNP no se encuentra capacitada para realizar el procedimiento de obtención de evidencia digital , pues carece de recursos humanos y logísticos para un efectivo resultado.
Jhomira Selene Morau Zuasnabar	La letrada señala que puede mejora con capacitación continua del personal a cargo de dicha área implementando mayor tecnología, así mismo respecto a la capacidad de la PNP para la obtención de la evidencia digital, señala que no se encuentra capacitada. Finalmente señala sobre la logística de la PNP, al ser un área recién abordada no se encuentra bien equipado respecto de los recursos tecnológicos y humanos para realizar una labor de tal magnitud y complejidad.
Karin Elizabeth Cuchache Mendez	La letrada señala que la PNP es idónea para la obtención de la evidencia digital , se encuentra capacitada y cuenta con los recursos tecnológicos y humanos requeridos para una actividad compleja de gran magnitud.
Helmut Nixon Meza	El experto señala que personal policial de la DIVINDAT no es el personal idóneo para la obtención de la evidencia por poca experiencia en el campo de

	tecnologías de la información. Asimismo, no respondió acerca de la capacidad de la policía para la obtención de la evidencia digital y sobre la logística que cuenta la PNP indica que existen muchas dificultades por ser un campo relativamente nuevo en el país , y la poca experiencia del personal que hace que a veces no se obtenga lo que realmente se necesita.
Arturo Lazarte Vilcamango	El experto señala el Ministerio Público como la Policía Nacional, teniendo los suficientes recursos, brindaría una mejor atención para la obtención de la evidencia, teniendo en cuenta que se debe actuar rápido por la volatibilidad de la misma evidencia.
Tania Gonzales Mego	La experta señala sobre la idoneidad de la DIVINDAT en tanto tenga profesionales capacitados para la labor de peritaje informático, claro que puede realizar un buen procedimiento en el tratamiento de la evidencia digital. Asimismo, sobre la capacidad de la PNP, en tanto tenga profesionales capacitados para la labor de peritaje informático, es posible que puede realizar un buen procedimiento en el tratamiento de la evidencia digital. Finalmente, sobre la logística de la PNP no tiene conocimiento.

Tabla N°12

Resultado respecto de la muestra B sobre objetivo específico 1 -Análisis Documental

Ámbito	Documento	Resultado
Perú	La Guía de Análisis Digital Forense del Ministerio Público, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG, del 11 de agosto de 2020.	Del análisis documental, la referida guía no indica respecto a la idoneidad de la actividad policial en la obtención de la evidencia digital en casos de cibercrimen, pues esta guía abarca el conocimiento en etapa de análisis digital forense por parte de personal de Peritos de la Gerencia de Peritajes del Ministerio Público.
	"Manual para el Recojo de Evidencia Digital", aprobado por el Ministerio del Interior a través de Resolución Ministerial N° 848-2019-IN.	Del análisis documental establece el procedimiento para el recojo de la evidencia digital por personal policial en la escena del crimen como un organismo de apoyo en la lucha contra el cibercrimen, pero no indica si el personal idóneo para la obtención de evidencia digital.
	Manual de Evidencia Digital -Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi	Del análisis documental, dicho manual contempla un proyecto de apoyo para la obtención de la evidencia digital en el ámbito de hardware, no indica sobre la idoneidad de la Policía Nacional en estos casos. Esta guía no realiza una selección del personal idóneo, no es su objetivo, pues solo indica el procedimiento que debe realizar, el cual puede ser realizado por cualquier persona con conocimientos de informática forense.
Argentina	Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero del año 2020-UFECI - Unidad Fiscal Especializada en Ciberdelincuencia-DIGCRI Dirección General de Cooperación Regional e Internacional	Del análisis documental, la referida guía no contempla a la policía como el profesional encargado de la obtención de la evidencia digital, pues abarca la obtención de evidencia electrónica almacenada por los proveedores de servicio (datos de usuario, historial de conexiones , contenido de mensajes), así como las comunicaciones en tiempo real. Es decir, se enfoca más a la entrega de información en el ámbito del Software.
Chile	Ley N° 21.459-Delitos Informáticos y recolección de la	Del análisis documental, la presente norma en su artículo 12 el Ministerio Publico como director de la investigación podrá ordenar a

	evidencia digital de fecha 20 de junio 2022	funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados en la referida Ley.
México	Poder Judicial de la Federación del Consejo de la Judicatura Federal, "Lineamientos para la obtención y tratamiento de los recursos informáticos y /o evidencias digitales" "Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales ,aprobado mediante el "Acuerdo General del Pleno del Consejo de la Judicatura Federal" de fecha 17 de junio del 2016	Del análisis documental, el referido documento en el capítulo VI, Perfil de Personal Autorizado, indica que el profesional debe ser una persona con los conocimientos de informática forense suficientes a fin de ayudar en las diligencias que se requieran sobre la evidencia a analizar, debe tener el conocimiento de realizar el trabajo de la obtención acorde y respetando el marco normativo a un estándar constitucional.
Organismos Internacional de Estandarización	Norma Internacional ISO/IEC 27037-2012 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" - "Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales"	Del análisis documental, dicha norma contempla a los individuos denominados como la (Digital Evidence First Responder (DEFRs) o especialista en evidencia digital de primera intervención y (Digital Evidence Specialist (DESs) o especialista en evidencia digital, los cuales constituyen a los especialistas en respuestas a los incidentes y a los directores de laboratorios forenses, señalando así que la identificación del personal responsable asegura la correcta gestión de la evidencia digital se realice ante prácticas de estándar internacional con el objetivo de que la investigación sea realizada de una manera unificada en el ámbito internacional, preservando la integridad y autenticidad de la evidencia digital.

Respecto del Objetivo específico 2: Determinar la idoneidad de la norma que regula la obtención de evidencia digital en el cibercrimen

Para responder el referido objetivo general se realizaron las siguientes preguntas:

- ¿Cree usted que resulta suficiente para la obtención de la evidencia digital en el Perú, la Guía de Análisis Digital Forense del Ministerio Público?
- ¿Cree usted que resulta suficiente para la obtención de la evidencia digital en el Perú, el Manual para el Recojo de Evidencia Digital" de la Policía Nacional?
- ¿Cree usted que resulta necesaria la creación de un procedimiento normativo especifico que permita establecer el procedimiento de obtención de la evidencia digital, así como el personal idóneo para su obtención en delitos de cibercrimen?

Tabla N°13

Resultado respecto de la muestra A sobre objetivo específico 2 -Entrevistas

Entrevistado	Respuesta
Sharom Cáceres Medina	La letrada señala que la guía de análisis digital forense y el manual para el recojo de la evidencia digital de la Policía Nacional no resultan suficientes para la obtención de la evidencia digital .Sin embargo, señala que resulta necesario la creación de un procedimiento normativo especifico que permita la obtención de evidencia digital y determine el personal idóneo respectivo.
Nelida Choque Cruz	La letrada señala que la guía de análisis digital forense y el manual para el recojo de la evidencia digital de la Policía Nacional no resultan suficientes para la obtención de la evidencia digital .Sin embargo, señala que resulta necesario la creación de un procedimiento normativo especifico que permita la obtención de evidencia digital y determine el personal idóneo respectivo.
Martin Christian Cárdenas Castillo	El letrado señada que la guía de análisis digital forense y el manual para el recojo de la evidencia digital de la Policía Nacional no resultan suficientes para la obtención de la evidencia digital .Sin embargo, señala que resulta necesario la creación de un procedimiento normativo especifico que permita la obtención de evidencia digital y determine el personal idóneo respectivo.
Jhomira Selene Morau Zuasnabar	La letrada no puede señalar la idoneidad de la guía de análisis digital forense y el manual para el recojo de la evidencia digital de la Policía Nacional por desconocimiento de los referidos manuales. Sin embargo, concuerda que resulta necesario la creación de un procedimiento normativo especifico, así como el personal idóneo para su obtención pues ello mejoraría a gran escala el nivel de atención para cada caso.
Karin Elizabeth Cuchache Mendez	La letrada respecto de la guía de análisis digital forense y el manual para el recojo de la evidencia

	digital de la Policía Nacional si resultan suficientes, pero pueden mejorar con una ampliación de dichos documentos. A ello, concuerda que resulta necesario la creación de un procedimiento normativo especifico, así como el personal idóneo para su obtención.
Helmut Nixon Meza	El experto señala sobre la idoneidad de la guía de análisis digital forense y el manual para el recojo de la evidencia digital de la Policía Nacional, no resultan suficientes, por el contrario, resulta necesario un procedimiento normativo. A ello, señala sobre la creación de un procedimiento normativo especifico, así como el personal idóneo para su obtención, los peritos del Ministerio Publico, con experiencia laboral mayor a 10 años en todos los campos que abarca las Tecnologías de la Información, son el personal idóneo. A su vez, a fin de garantizar un buen proceso de obtención de evidencia digital se debe tener en cuenta que se debe contar con equipos o llaves forenses en cantidad suficiente para no tener evidencia en espera de extracción, el contar con equipo de gran performance (servidores) con gran capacidad de almacenamiento y procesamiento a fin de que las indexaciones y generación de reportes sean obtenidos en menor tiempo y contar con personal especializado con experiencia comprobada a fin de que ningún caso solicitado por las despachos fiscales, tengan demora por sobre carga laboral de la Oficina de Peritajes.
Arturo Lazarte Vilcamango	El experto señala sobre la idoneidad de la guía de análisis digital forense y el manual para el recojo de la evidencia digital de la Policía Nacional partir del año 2021 las Fiscalías Especializadas en Ciberdelincuencia han estado orientando en la parte técnico-jurídico a las fiscalías a nivel nacional, así como investigando delitos informáticos, esto es un proceso que está madurando cada vez más, permitiendo que se pueda obtener una adecuada evidencia digital para que los fiscales puedan seguir con sus investigaciones. Al no tener fronteras los delitos informáticos, es necesario la cooperación internacional para preservar la evidencia y esto aún es un gran desafío en nuestro país que está en un proceso

	de madurez , así como cree que dotando de mayores recursos reuniría las condiciones necesarias u óptimas para brindar una mejor atención. Actualmente la sobredemanda y falta de apoyo logístico se hace insuficiente en la Policía Nacional del Perú. Finalmente , respecto de la necesidad de la creación de un procedimiento normativo especifico, así como el personal idóneo para su obtención, el desconocimiento para un adecuado recojo de evidencia digital, personal calificado insuficiente para la atención a nivel nacional genera dificultades para la obtención de evidencia digital. El Perú con la adhesión al Convenio de Budapest le ha abierto las oportunidades de tener mayor personal capacitado para la obtención de la evidencia digital y que puedan tener una mejor investigación en los delitos informáticos. Es necesario que se siga capacitando a más personal para realizar un mejor recojo de evidencias digitales. Es muy importante en el manejo adecuado de la evidencia digital para esta manera puedan tener una correcta investigación en estos tipos de delitos.
Tania Gonzales Mego	La experta señala sobre la idoneidad de la guía de análisis digital forense, dicha guía, establece los lineamientos y procedimientos para el desarrollo de las actividades periciales a fin de contribuir al cumplimiento de las funciones del área de Análisis Digital Forense, la cual se encuentra en actualización de una nueva versión para su mejora y en referencia al manual para el recojo de la evidencia digital de la Policía Nacional, considera que es suficiente pues recoge procedimientos y buenas prácticas de la norma La Norma ISO/IEC 27037:2012. Finalmente, sobre la necesidad de la creación de un procedimiento normativo especifico que permita establecer el procedimiento de obtención de la evidencia digital, así como el personal idóneo, señala que es necesario tener un procedimiento normativo especifico que permita establecer el proceso de obtención de la evidencia digital, ya que la valía legal y técnica de las evidencias en la mayoría de las ocasiones depende del proceso realizado en la recopilación y preservación de las

mismas y este sea una guía de procedimiento para todo personal encargado de recojo de Evidencia Digitales.

Tabla N°14

Resultado respecto de la muestra B sobre objetivo específico 2 -Análisis Documental

Ámbito	Documento	Resultado
Perú	La Guía de Análisis Digital Forense del Ministerio Público, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG, del 11 de agosto de 2020. "Manual para el Recojo de Evidencia Digital", aprobado por el Ministerio del Interior a través de Resolución Ministerial N° 848-2019-IN.	Del análisis documental, tanto la Guía de Análisis Digital Forense del Ministerio Público y el Manual para el Recojo de Evidencia Digital de la Policía Nacional del Perú, encontramos una semejanza en los documentos con los cuales cuenta en el caso de Argentina , la Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero y en el caso de México "Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales" pero nos encontramos en desventaja en la necesidad de un procedimiento normativo como si lo tiene la República de Chile, quien ha establecido dicho procedimiento a través de la Ley N° 21.459-Delitos Informáticos y recolección de la evidencia digital de fecha 20 de junio 2022. Es de apreciarse, que nuestro ordenamiento jurídico se encuentra en la necesidad del procedimiento normativo acorde con estándares internacionales adecuados que regule la correcta obtención de la evidencia digital en casos de cibercrimen tanto de hardware como de software. A ello, resulta de importancia que parte de dicho procedimiento normativo respete los lineamientos de calidad establecidos en la Norma ISO/IEC 27037-2012, como instrumento internacional base para la obtención de la evidencia digital y sus demás procedimientos que impliquen el correcto tratamiento de la evidencia digital y se complemente con el proyecto Manual de Evidencia Digital -Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi, que si bien tiene de referencia la norma ISO referida, dicho proyecto no constituye una norma técnica nacional que regularice la Norma ISO/IEC 27037-2012.
Argentina	Manual de Evidencia Digital -Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero del año 2020- UFECI - Unidad Fiscal Especializada en Ciberdelincuencia- DIGCRI Dirección General de Cooperación Regional e Internacional	
Chile	Ley N° 21.459-Delitos Informáticos y recolección de la evidencia digital de fecha 20 de junio 2022	
México	Poder Judicial de la Federación del Consejo	

	de la Judicatura Federal, "Lineamientos para la obtención y tratamiento de los recursos informáticos y /o evidencias digitales" "Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales ,aprobado mediante el "Acuerdo General del Pleno del Consejo de la Judicatura Federal" de fecha 17 de junio del 2016	Respecto al personal idóneo, se ha obtenido que el personal acorde son los peritos de la Gerencia del Ministerio Público como el personal especializado para la obtención de la evidencia digital en casos de cibercrimen.
Organismos Internacional de Estandarización	Norma Internacional ISO/IEC 27037-2012 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" - "Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales"	

CAPÍTULO IV: DISCUSIÓN

4.1 Limitaciones

Antes de ingresar al debate entre los resultados con los objetivos de esta investigación, es preciso hacer mención sobre las limitaciones presentadas a lo largo de este trabajo, el cual tuvo diversas dificultades conforme a las siguientes líneas.

En primer lugar, este trabajo se construyó durante la crisis sanitaria debido a la pandemia mundial del Coronavirus (COVID-19), la cual fue declarada como emergencia sanitaria y el gobierno peruano optó por establecer, en todo el país, el estado de emergencia nacional, para restringir el libre tránsito y la movilización de las personas en el territorio peruano, y establecer medidas de aislamiento social obligatorias y cuarentena, todo ello con la finalidad de no aumentar los contagios y evitar pérdidas humanas de forma incontrolable. Esto restringió la movilización social y se paralizaron todas las actividades empresariales, administrativas, sociales y demás; con excepción de los servicios básicos (alimentación y servicios esenciales).

En ese sentido, la presente investigación tuvo que aplicarse algunos aspectos para poder ajustarse a la coyuntura social actual, y lograr obtener información con las herramientas disponibles que, en su gran mayoría tuvieron que ser artículos y documentos digitales, conjuntamente estudiados con libros y guías de doctrina de derecho, y con el indispensable Código Penal Peruano , siendo la documentación como tal el instrumento más utilizado.

4.2 Interpretación comparativa de resultados

Al respecto, resulta necesario realizar el análisis sobre las entrevistas realizadas y el análisis documental en la presente investigación con el fin de determinar qué diferencias o semejanzas encontramos y si los resultados obtenidos coadyuvan a resolver los objetivos materia de investigación.

Tabla n° 15

Discusión del Objetivo General

Determinar el procedimiento normativo para la obtención de la evidencia digital en el cibercrimen

Conforme Muestra A	**Conforme Muestra B**
Se advierte un desconocimiento del procedimiento normativo para la obtención de la evidencia digital respecto de los abogados entrevistados y en referencia a los peritos tienen como referencia y/o señalan los instrumentos de Manual de evidencia digital del Ministerio de Justicia y Derechos Humanos y la Guía de Análisis Digital Forense, pero no toman en cuenta el Manual de Evidencia Digital -Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi, el cual contempla diversos lineamientos, protocolos así como Acuerdos Plenarios de nuestro ordenamiento jurídico.	Se propone la creación de una norma técnica nacional con base en la Norma Internacional ISO/IEC 27037-2012 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" - "Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales" , como el instrumento de excelencia para la creación de un procedimiento normativo nacional el cual debe servir como la mejor propuesta para la regulación mediante una norma técnica que se encuentra pendiente de elaboración por el INDECOPI como el ente encargado

Desde la perspectiva de investigación, creemos que dicho "Manual" es la más idóneo para la obtención de la evidencia digital en casos de cibercrimen, pero resulta necesaria del complemento de normas de calidad , es decir de la norma internacional ISO, como la norma internacional que establece la calidad estándar a nivel internacional.	de la normalización de dicha norma ISO así como ya lo hizo con la norma técnica Peruana NTP-ISO/IEC 27035-2013 que regula sobre la tecnología de la información-Técnicas de Seguridad-Gestión de Incidentes de seguridad de la información . A ello, también se encuentra el Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales de la República de México ,aprobado mediante el "Acuerdo General del Pleno del Consejo de la Judicatura Federal" de fecha 17 de junio del 2016, instrumentos de regulación internacional que permiten establecer directrices bajo un ámbito de carácter normativo de buenas prácticas el cual debe ser adecuado al ordenamiento jurídico peruano con el fin de obtener el procedimiento normativo nacional que cumpla estándares de buenas prácticas forenses para la obtención de la evidencia digital y ello genere la confiabilidad en el proceso penal peruano, cuando se trate de este tipo de evidencias digitales en los delitos de cibercrimen. Es decir, resulta necesaria la creación de una Norma Técnica Peruana que regule lo señalado en la Norma ISO/IEC 27037-2012, como la norma de calidad que

	establezca buenas prácticas para la obtención de la evidencia digital en casos de cibercrimen.

Nota: Elaboración Propia

Tabla n°16

Discusión del Objetivo Especifico 1

Determinar la idoneidad de la actividad policial para la obtención de la evidencia digital en el cibercrimen.

Conforme muestra A-Entrevistados	**Conforme muestra B- Análisis Documental**
De la respuestas obtenidas por parte de los abogados reconoce a la Policía Nacional del Perú como una unidad idónea y capacitada en un 40 %. Sin embargo , con relación a los peritos consideran que personal policial tiene las capacidades suficientes pero la falta de recursos humanos y logística restringe el actuar de la Policía e inclusive del propio personal de la Gerencia de Peritajes del Ministerio Público. d)¿Conoce usted cual es la importancia del código Hash y Cadena de custodia contra los	Se considera conforme a la Ley Orgánica de la Policía Nacional del Perú, como el órgano de apoyo más no el director de la investigación, facultad que, si la tiene el representante del Ministerio Público, quien según su estrategia de investigación podrá optar el trabajar con la DIVINDAT-PNP o en su defecto con la Gerencia de Peritajes del Ministerio Público. Desde la normativa internacional, no encontramos a la Policía como el personal idóneo para la recolección de la evidencia digital, pues según lo verificado, dicha facultad la tiene el representante del Ministerio

delitos de cibercrimen?: En relación con ello, existe un acuerdo plenario en que resulta el procedimiento de aseguramiento de la evidencia digital por excelencia.	Público. En el sentido de la normativa de la cadena de custodia deberá tenerse en cuenta el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados. Aprobado por Resolución Nº 729-2006-MP-FN del 15.junio.2006 y sobre el código hash la Guía de Análisis Digital Forense del Ministerio Público, como instrumento especializado de aseguramiento de evidencia.

Nota: Elaboración Propia

Tabla n°17

Discusión Objetivo Especifico 2

Determinar la idoneidad de la norma que regula la obtención de evidencia digital en el cibercrimen

Conforme muestra A-Entrevistas	Conforme muestra B-Análisis Documental
De las respuestas obtenidas por parte de los peritos se establece que tanto la Guía de Análisis Digital Forense del Ministerio Público y el Manual para el Recojo de	Tanto la Guía de Análisis Digital Forense del Ministerio Público y el Manual para el Recojo de Evidencia Digital de la Policía Nacional del Perú, encontramos una

Evidencia Digital de la Policía Nacional del Perú, no resultan documentos suficientes para la obtención de la evidencia digital, pues el desconocimiento para un adecuado recojo de evidencia digital, personal calificado insuficiente para la atención a nivel nacional genera dificultades para la obtención de evidencia digital. En el caso de las abogadas consultadas indican que dichos documentos no son suficientes. Respecto de la necesidad de la creación de un procedimiento normativo especifico que permita establecer el procedimiento de obtención de la evidencia digital, así como el personal idóneo para su obtención en delitos de cibercrimen, se observa que si resultan necesario la creación de un procedimiento normativo especifico, tal como el Perú cuenta con el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados. Dicho semejanza en los documentos con los cuales cuenta en el caso de Argentina , la Guía de Buenas Prácticas para obtener evidencia electrónica en el extranjero y en el caso de México "Protocolo de Actuación para la Obtención y Tratamiento de Recursos Informáticos y/o Evidencias Digitales" pero nos encontramos en desventaja en la necesidad de un procedimiento normativo como si lo tiene la República de Chile, quien ha establecido dicho procedimiento a través de la Ley N° 21.459-Delitos Informáticos y recolección de la evidencia digital de fecha 20 de junio 2022. Es de apreciarse, que nuestro ordenamiento jurídico se encuentra en la necesidad del procedimiento normativo acorde con estándares internacionales adecuados que regule la correcta obtención de la evidencia digital en casos de cibercrimen. Como se señaló anteriormente, resulta de importancia que parte de dicho

procedimiento permitiría mediante las buenas prácticas por parte del personal capacitado un trabajo de calidad y con la confiabilidad de que la obtención de la evidencia digital fue realizada respetando un marco de estándar normativo adecuado al ordenamiento jurídico nacional.	procedimiento normativo respete los lineamientos de calidad establecidos en la Norma ISO/IEC 27037-2012, como instrumento internacional base para la obtención de la evidencia digital y sus demás procedimientos que impliquen el correcto tratamiento de la evidencia digital y se complemente con el proyecto Manual de Evidencia Digital -Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi, que si bien tiene de referencia la norma ISO referida, dicho proyecto no constituye una norma técnica nacional que regularice la Norma ISO/IEC 27037-2012. Respecto al personal idóneo, se ha obtenido que el personal acorde son los peritos de la Gerencia del Ministerio Público como el personal especializado para la obtención de la evidencia digital en casos de cibercrimen.

Nota: Elaboración Propia

CAPÍTULO V: CONCLUSIONES

Como se puede advertir, la "evidencia digital" constituye una parte importante en los casos de delitos de cibercrimen, pues como se ha podido advertir, su intangibilidad genera que dicha evidencia conlleve a que sea tratada de manera especial, estando a que los delitos donde se puede obtener también lo son, y esto como lo señalamos ocurre a través del mundo digital. Es importante señalar que la evidencia digital es un elemento probatorio de gran importancia pues acarrea que a partir de ella se puede establecer la responsabilidad penal al sujeto activo. En ese sentido, del resultado de la presente investigación, se concluye lo siguiente:

a) En el Perú, no contamos con un procedimiento normativo referente a la obtención de la evidencia digital, más solo se cuenta con manuales de la Policía Nacional del Perú, el manual de Análisis Digital Forense de la Gerencia de Peritajes del Ministerio Público y proyecto Manual de Evidencia Digital - Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi, los cuales plantean diferentes metodologías referente a la obtención de la evidencia digital.
b) Resulta necesario tener un procedimiento normativo especifico referente a la obtención de la evidencia digital en casos de cibercrimen.
c) El personal policial de la DIVINDAT-PNP, se encuentra como un órgano de apoyo para el Ministerio Público y su Manual para el recojo de evidencia digital, no cuenta con la integración de la norma internacional ISO/IEC 27037-2012, "Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales".
d) El manual de análisis digital forense de la Gerencia de Peritajes del Ministerio Público no cuenta con la integración de la norma internacional ISO/IEC 27037-2012, "Tecnologías de la información —

Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales".

e) El Manual de Evidencia Digital -Proyecto de Apoyo al Sector Justicia de autoría del Dr. Alan Martín Nessi, cuenta con la integración de la norma internacional ISO/IEC 27037-2012, "Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales" pero resulta necesaria la norma técnica nacional que trabaje los procedimientos de la obtención de la evidencia digital con estándares de nivel internacional.

f) El personal policial no resulta ser el personal idóneo para la obtención de la evidencia digital, salvo que estos se encuentren capacitados respecto a procedimiento de sistemas informáticos como si lo están los profesionales de ingeniería en sistemas (peritos de la) .

g) Señalamos aspectos de relevancia que cuenta la evidencia digital:

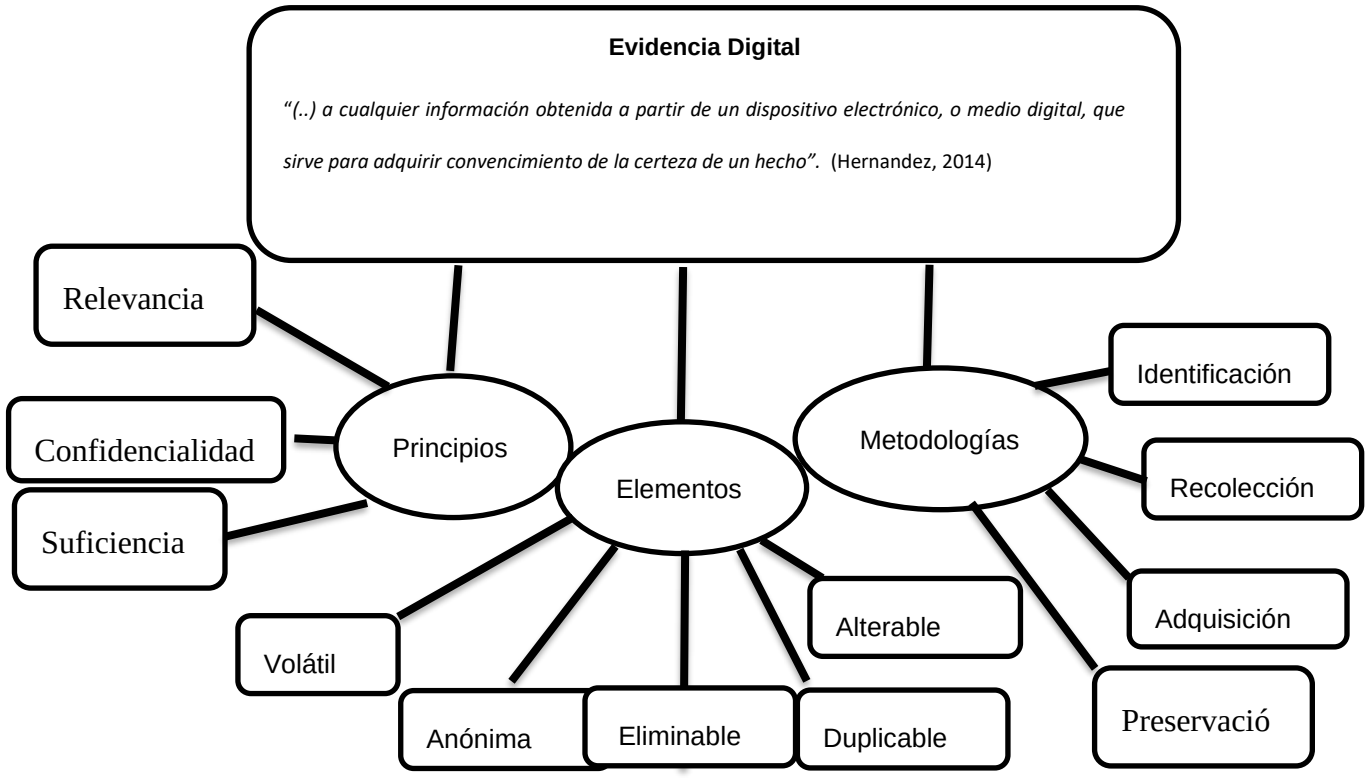


Figura 12: Elaboración propia

CAPÍTULO VI: RECOMENDACIONES

Resulta importante que el Perú se encuentre siempre en la vanguardia en lo que respecta a normas de nuestro ordenamiento jurídico, pues implica que nuestra sociedad y operadores de justicia siempre tendrán las herramientas jurídicas necesarias en el momento que se presentan hechos complejos. Es así, que el procedimiento normativo especifico respecto a la obtención de la evidencia digital en casos de cibercrimen deberá establecer una definición a lo que respecta a la evidencia digital, características, metodologías y/o procedimiento de obtención, conservación y el personal idóneo . Asimismo, este documento normativo deberá contemplar lo que señala el Convenio de Budapest, Ley N°30096 y su modificatoria, Manual de recojo de la evidencia digital de la Policía Nacional del Perú, Manual de Análisis Digital Forense de la Gerencia de Peritajes del Ministerio Público y normas internacionales, entre la que se encuentra Norma ISO/IEC 27037-2012, "Tecnologías de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y conservación de pruebas digitales", ya que deberá contemplar todo lo avanzando en lo que respecta a este tema poco tratado, debiendo establecer estándares de calidad de buenas prácticas.

Por lo que , la recomendaciones que planteamos son:

- Los peritos del área de análisis digital forense de la Gerencia de Peritajes del Ministerio Público, resultan ser el personal idóneo por excelencia en la obtención de la evidencia digital, estando a que son ingenieros en sistemas y trabajan no solo informes periciales respecto de delitos sobre

cibercrimen sino que trabajan a nivel nacional delitos comunes y especializados como delitos de corrupción de funcionarios, crimen organizado, lavado de activos u otros.

- Mayor presupuesto a la Gerencia de Peritaje del Ministerio Público, como la institución idónea con el objetivo de contratar herramientas de obtención de la evidencia digital, profesional especializados y la creación de laboratorios forense.
- Descentralización de la oficina de la Gerencia de Peritaje del Ministerio , con la finalidad de que todo el país cuente con los profesionales capacitados para la obtención de la evidencia digital en casos de cibercrimen.
- Capacitación constante al personal de peritos mediante talleres, cursos, seminarios u otros al personal pericial, respecto a la obtención de la evidencia digital en casos de cibercrimen.

REFERENCIAS

A.Herrera. (2013). *Administración de la Empresa Constructora.* Lulu.com.

A.Herrera. (2013). *Administración de la Empresa Constructora .* Lulu .

Arias-Gómez, J., Villasís-Keever, M. Á., & Miranda Novales, M. G. (2016). El protocolo de investigación III: la población de estudio. En J. Arias-Gómez, M. Á. Villasís-Keever, & M. G. Miranda Novales. Ciudad de Mexico : Revista Alergia Mexico .

BALLESTEROS, M. C. (2014). *CIBERCRIMEN : PARTICULARIDADES EN SU LEGISLACIÓN Y ENJUICIAMIENTO .* Anuario Jurídico y Económico Escurialense.

CADILLO, E. S. (2018). *TRATAMIENTO DE LA PRUEBA DIGITAL OFRECIDA POR LAS PARTES EN EL PROCESO PENAL DEL MINISTERIO PUBLICO DE VENTANILLA CALLAO-2017.* PERU .

Casabona, C. R. (2006). *De los Delitos Informaticos al Cibercrimen .* Granada : Comares P1-42 .

Casanova, C. R. (2006). *DE LOS DELITOS INFORMATICOS AL CIBERCRIMEN : AUNA APROXIMACIÓN CONCEPTUAL Y POLITIICO -CRIMINAL. .* GRANADA : EDITORIAL COMARES .

Castro, C. S. (2015). *Derecho Porcesal Penal Lecciones.* Lima: INPECCP.

Darahuge, A. y. (2016). *La Cadena de Custodia.* Obtenido de http:// www.iadisportal.org/digital-library/lacadena-d-custodia-inform%C3%Altico-forense

Davara, M. A. (2002). *Fact Book del Comercio Electronico .* Arazandi.

Escobedo, M. A. (2018). *LA ADMISIBILIDAD Y EL VALOR PROBATORIO DE LA EVIDENCIA DIGITAL EN EL SISTEMA JURIDICO PERUANO 2018. .*

Francés, M. L. (2011). *La privacidad en el espacio virtual (riesgos y cauces de protección .* Cuadernos de la Catedra de Seguridad Saamantina .

Guidelines for Management of It Evidence . (2003). *Guidelines for Management of It Evidence .*

Hernandez, J. A. (2014). *Anuario Juridico y Economico Escuialense-Cibercrimen :Particularidades en su investaigación y enjuiciamiento. .* Madrid : Universidad Complutense de Madrid .

LIBARDO, P. B. (2020). *MODELO DE GESTION DE ANALISIS FORENSE DE HECHOS DELICTIVOS INFORMATICOS EN EL MARCO DEL SISTEMA DE JUSTICIA PERUANO.* LIMA.

LINARES, M. (s.f.). *La cibercriminalidad 2.0 Falacias y realidades" ,pp 58-59 .*

MANSON, M. (2013). Legislación sobre delitos informáticos.

Maya, R. P. (junio de 2017). El cibercrimen y sus defectos en la teoria de la tipicidad: de una realidad fisica a una realidad virtual. Universidad EAFIT .

MAYA, R. P. (2017). *EL CIBERCRIMEN Y SUS EFECTOS EN LA TEORIA DE LA IPICIDAD: DE UNA REALIDAD FISICA A UNA REALIDAD VIRTUAL .* COLOMBIA .

Neira, M. M. (s.f.). *Delito Informatico y cadena de cusatodia .*

RUIZ, E. O. (2019). *CONTEXTO DE LA EVIDENCIA DIGITAL EN COLOMBIA: BUENAS PRATICAS Y APLICACIÓN DE METODDOLOGIAS .* COLOMBIA .

Sampieri, R. H. (2010). *Metodologia de la Investigación -Quinta Edición .* Mexico DF : McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Schroder, H. Z. (2017). *Las normas técnicas en el Perú: marco teórico y legal.* Lima : Foro jurídico (Lima), N° 16.

Seva, A. P. (1996). *La prueba en el Proceso Penal .* Pamplona: Aranzadi.

SICHACA, A. P. (2019). *REQUISITOS JURIDICOS PARA LA VALIDEZ DE A PRUEBA DIGITAL .* COLOMBIA .

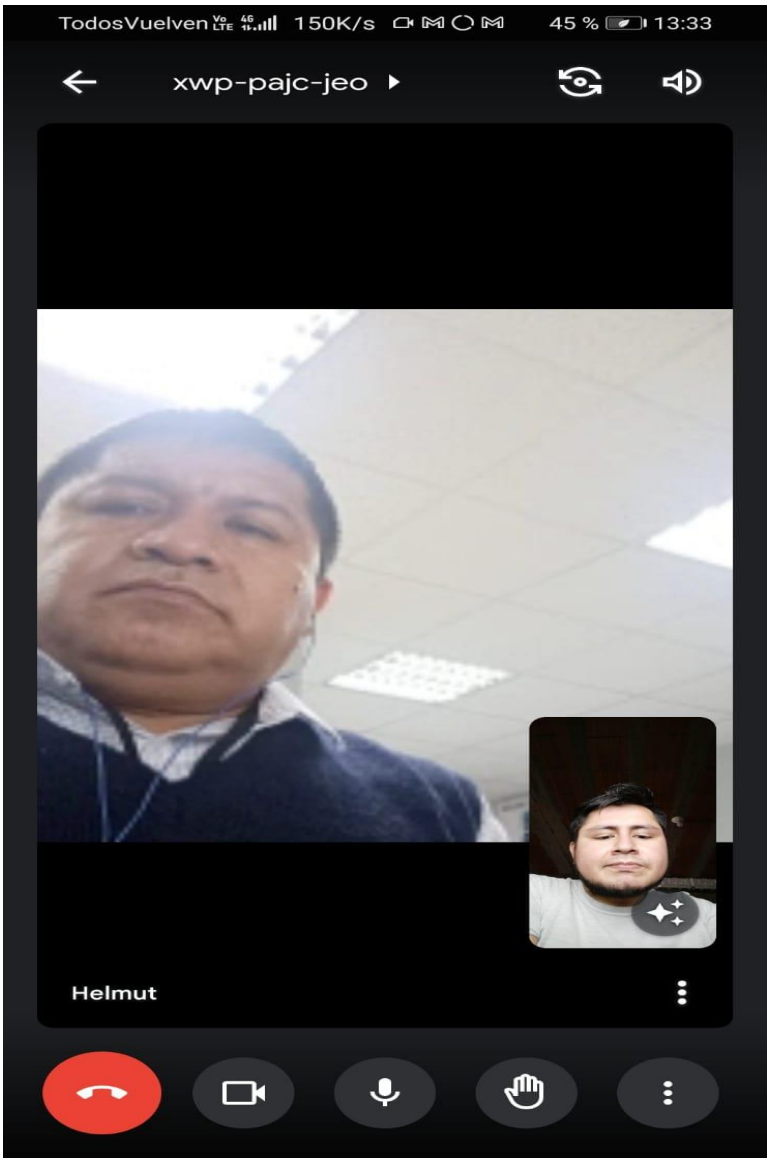
Terreros, F. V. (2014). *DELITOS INFORMATICOS-CIBERCRIMEN .* Revista ius et veritas.

Urdaneta, E. (2002). *Información Juridica .* Maracaibo: Uribe .

ANEXOS

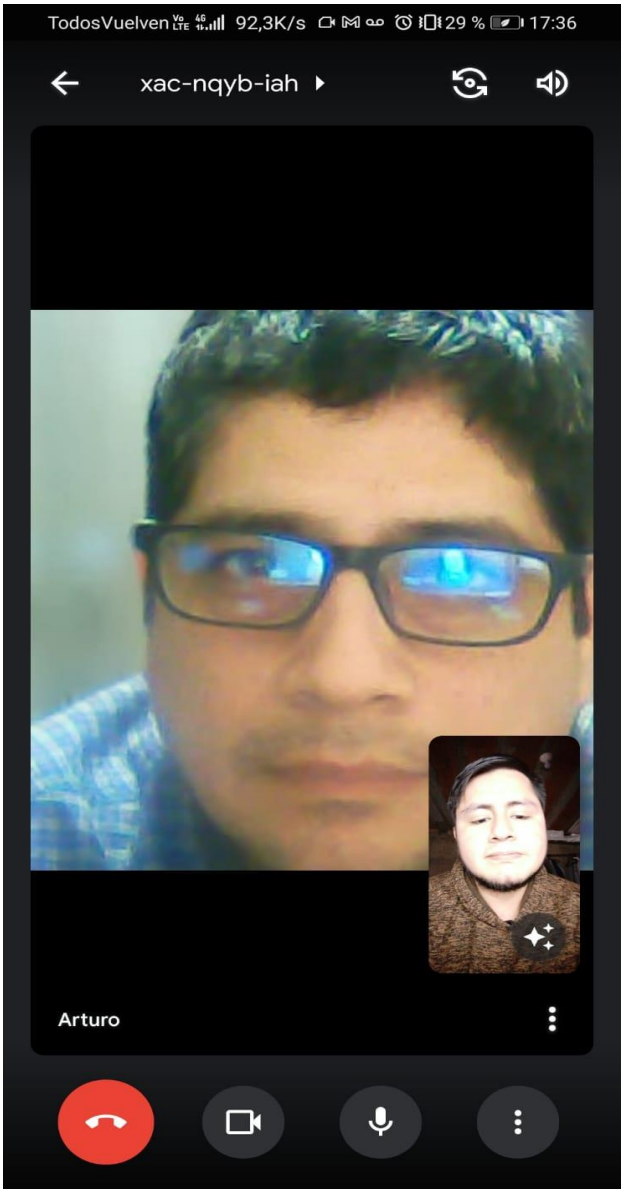
ANEXO 1

Captura de pantalla de entrevista a Experto -Helmut Nixon Rodríguez Meza-Perito de la Gerencia de Peritajes del Ministerio Público



ANEXO 2

Captura de pantalla de entrevista a Experto -Arturo Lazarte Vilcamango -Perito de la Gerencia de Peritajes del Ministerio Público



ANEXO 3

MATRIZ PARA EVALUACIÓN DE EXPERTOS

Título de la investigación:	LA EVIDENCIA DIGITAL EN EL CIBERCRIMEN –PERÚ 2022
Línea de investigación:	Cualitativa
Apellidos y nombres del experto:	Arturo Lazarte Vilcamango
El instrumento de medición pertenece a la variable:	1,2,3

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Ítems	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición? (*)	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto:

(*) Aplica solo para investigaciones cuantitativas

ANEXO 4

MATRIZ PARA EVALUACION DE EXPERTOS

Titulo de la investigación:	LA EVIDENCIA DIGITAL EN EL CIBERCRIMEN –PERÚ 2022
Línea de investigación:	Cualitativa
Apellidos y nombres del experto:	Helmut Nixon Rodríguez Meza
El instrumento de medición pertenece a la variable:	1,2,3

Mediante la matriz de evaluación de expertos, Ud. tiene la facultad de evaluar cada una de las preguntas marcando con una "x" en las columnas de SÍ o NO. Asimismo, le exhortamos en la corrección de los ítems, indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre la variable en estudio.

Items	Preguntas	Aprecia		Observaciones
		SÍ	NO	
1	¿El instrumento de medición presenta el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas tienen un sentido coherente y no están sesgadas?	X		
7	¿Cada una de las preguntas del instrumento de medición se relaciona con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Son entendibles las alternativas de respuesta del instrumento de medición? (*)	X		
10	¿El instrumento de medición será accesible a la población sujeto de estudio?	X		
11	¿El instrumento de medición es claro, preciso y sencillo de responder para, de esta manera, obtener los datos requeridos?	X		

Sugerencias:

Firma del experto

(*) Aplica solo para investigaciones cuantitativas

ANEXO 5

Enlace drive donde se encuentra las entrevistas escritas escaneadas para su visualización de considerarlo.

https://drive.google.com/drive/folders/1Tb6RW8omEyUsxfmlDz-z18X-vsGtd1R0?usp=sharing

MATRIZ DE CONSISTENCIA Y CRONOGRAMA

TÍTULO	PROBLEMA	OBJETIVOS	HIPOTESIS	MARCO TEORICO	METODOLOGIA
LA EVIDENCIA DIGITAL EN EL CIBERCRIMEN-PERU 2022	**¿Cuál es el Procedimiento Normativo de la obtención de la evidencia digital en el Cibercrimen?**	**GENERAL:** Determinar el procedimiento normativo de la obtención de la evidencia digital en el cibercrimen **Problemas Especifico 1** ¿ Resulta idóneo la actividad policial en la obtención de evidencia digital en el cibercrimen? **Problemas Especifico 2** ¿ Es idónea la norma que regula la obtención de evidencia digital en el cibercrimen ? **Objetivo General** Determinar el procedimiento normativo de la obtención de la evidencia digital en el cibercrimen **Objetivo específico 1** Determinar la idoneidad de la actividad policial en la obtención de prueba digital en el cibercrimen. **Objetivo Especifico 2** Determinar la idoneidad de la norma que regula la obtención de evidencia digital en el cibercrimen	**Hipótesis General** En el Perú no existe un procedimiento normativo para la obtención de la evidencia digital, más solo existen los instrumentos "manuales" de evidencia digital del Ministerio Público y Policía Nacional, ambos aprobados mediante resoluciones ministeriales, los cuales consisten en manuales con criterios diferentes para la obtención del elemento probatorio "evidencia digital". Sumado a ello, dichos instrumentos no generan un procedimiento normativo unificado que sea de carácter obligatorio para la obtención de la evidencia digital en delitos de cibercrimen, así como el personal idóneo, respectivo. En ese sentido, resulta necesario establecer y/o la creación de un instrumento normativo que unifique criterios respecto a la obtención y preservación de la evidencia digital en casos de cibercrimen en el Perú. Justificación La presente investigación desarrolla un tema necesario en la ámbito penal peruano en referencia a la evidencia digital como resultado de conductas digitales delictivas (huellas digitales), estando a que es un tema poco tratado en nuestro ordenamiento jurídico. En ese sentido, para contrarrestar al Cibercrimen en el año 2013, la Ley N°30096-Ley de Delitos Informáticos comienza a regular dichas conductas digitales delictivas y consecuentemente el 01 de diciembre del 2019 nuestro ordenamiento jurídico ratifica el convenio de Budapest adoptado el 23 de noviembre del 2001, esto es 18 años de demora en la ratificación de un convenio importante para la erradicación de este tipo de conductas que día a día va actualizándose conforme al avance de la tecnología en nuestro país, así como en el mundo. Sin embargo, no se cuenta con procedimiento normativo respecto de la obtención de la evidencia digital, siendo la justificación regular dicho procedimiento, a fin de brindar soluciones para la determinación del procedimiento de obtención idóneo, así como el personal respectivo.	**Marco teórico** Artículos especializados, doctrina nacional e internacional.	**Tipo de investigación: Cualitativa**