



UNIVERSIDAD CÉSAR VALLEJO

**ESCUELA DE POSGRADO
PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO
PENAL Y PROCESAL PENAL**

**La obtención de la prueba digital en los delitos informáticos
en el distrito fiscal de Lima Norte, 2021**

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

AUTOR:

Silva Huaman, Gustavo Adolfo (orcid.org/0000-0003-4133-0818)

ASESOR:

Dr. Miranda Aburto, Elder Jaime (orcid.org/0000-0003-1632-4547)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y formas del
Fenómeno criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la Democracia, liderazgo y ciudadanía

LIMA – PERÚ

2022

Dedicatoria

A Dios, que nos brinda cada oportunidad en la vida. A Soli y Amanda que son la motivación para la culminación del presente trabajo

Agradecimiento

Ustedes que me enseñaron lo correcto y el valor de cada esfuerzo realizado, quienes estuvieron siempre a mi lado y me impulsaron a seguir esta noble carrera. Siempre han sido mis mejores guías de vida. Hoy que culmino mis estudios, les dedico a ustedes este logro amados padres, como una meta conquistada. Gracias

Índice de contenido

| | |
|--|------|
| Carátula | i |
| Dedicatoria | ii |
| Agradecimiento | iii |
| Índice de contenido | iv |
| Índice de tablas | vi |
| Resumen | vii |
| Abstract | viii |
| I. INTRODUCCIÓN | 1 |
| II. MARCO TEÓRICO | 4 |
| III. METODOLOGÍA | 14 |
| 3.1 Tipo y diseño de investigación | 14 |
| 3.2 Categorías, Subcategorías y matriz de categorización | 14 |
| 3.3 Escenario de estudio | 15 |
| 3.4 Participantes | 15 |
| 3.5 Técnicas e instrumentos de recolección de datos | 16 |
| 3.6 Procedimiento | 17 |
| 3.7 Rigor científico | 17 |
| 3.8 Método de análisis de datos | 18 |
| 3.9 Aspectos éticos | 18 |
| IV. RESULTADOS Y DISCUSIÓN | 19 |
| 4.1 Resultados | 19 |
| 4.2 Discusión | 24 |
| V. CONCLUSIONES | 26 |
| VI. RECOMENDACIONES | 28 |
| REFERENCIAS | 29 |
| ANEXOS | 34 |

Índice de tablas

| | |
|---|----|
| Anexo 1 Tabla 1. Matriz de Categorización | 35 |
| Anexo 2 Tabla 2. Matriz de Operacionalización | 36 |
| Anexo 3 Tabla 3. Caracterización de participantes | 37 |
| Anexo 4 Tabla 4. Validez de contenido de los instrumentos de recolección de datos | 39 |

Resumen

La presente tesis tuvo como objeto de estudio identificar los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021.

La presente investigación tuvo un enfoque cualitativo, con diseño fenomenológico, teniendo como instrumento de evaluación la guía de entrevistas conformada por catorce preguntas semiestructuradas, vinculadas con los objetivos general y específicos. Los participantes fueron personal Fiscal y Jueces del Distrito Fiscal de Lima Norte, siendo que la muestra estuvo conformada por siete participantes, tres jueces penales y cuatro fiscales penales.

Esta investigación concluye que luego de haberse identificado la problemática para la obtención de la prueba digital, se considera necesario que se pueda efectuar una Guía para la Obtención, recolección, conservación y actuación de la prueba Digital aplicable a los operadores de justicia, a fin de uniformizar los criterios y facilitar el conocimiento de la investigación a los operadores de justicia.

Palabras clave: Prueba digital, delitos informáticos, procedimientos, actuación probatoria en juicio.

Abstract

The purpose of this thesis was to identify the challenges faced by justice operators in obtaining digital evidence in computer crimes in the Fiscal District of North Lima in 2021.

The present research had a qualitative approach, with phenomenological design, having as an evaluation instrument the interview guide made up of fourteen semi-structured questions, linked to the general and specific objectives. The participants were Prosecutor and Judges of the Fiscal District of North Lima, being that the sample was made up of seven participants, three criminal judges and four criminal prosecutors.

This research concludes that after having identified the problem for obtaining digital evidence, it is considered necessary that a Guide can be made for the Obtaining, collection, conservation and performance of the Digital evidence applicable to justice operators, in order to standardize the criteria and facilitate the knowledge of the investigation to justice operators.

Keywords: *Digital evidence, computer crimes, procedures, evidentiary action in court*

I. INTRODUCCIÓN

En el ámbito internacional, el delito tecnológico representa un gran desafío para las instituciones encargadas de hacer cumplir las leyes, partiendo por descifrar la capacidad de los delincuentes para perpetrar fraudes, plagios de identidad, y lavado de dinero a gran escala, entre otros muchos delitos, sin limitación alguna de fronteras, espacio ni tiempo. Al respecto, la *Convención de Budapest*, se postuló como instrumento de referencia para más de 130 países alrededor del mundo, incluyendo a miembros del Consejo de Europa, con el objetivo de combatir la ciberdelincuencia, por medio de la armonización de legislaciones y así proteger a las actuales sociedades -tan vulnerables- ante crímenes en el ciberespacio (Rodríguez, 2013).

En ese mismo orden, países como Canadá han implementado políticas contra el auge de dichas organizaciones delictivas transnacionales, entre las cuales destaca el acceso a la base de datos de proveedores de telecomunicaciones tanto a nivel nacional como en el extranjero, lo cual ha sido objeto de constates objeciones por ir en contra de los derechos a la privacidad personal, establecido por organismos como la ONU. Pese a ello, esta iniciativa se perfila como un avance importante en materia de investigaciones criminales, principalmente en el ámbito de la obtención de pruebas, tomando en consideración el tiempo que puede tomar la obtención de autorizaciones judiciales para contar con el acceso a dicha información y poder combatir la cibercriminalidad (Acurio, 2016)

El Perú no escapa a la problemática antes expuesta, ya que la impunidad reinante en materia de sanciones contra los delitos tecnológicos otorga de manera flagrante a los ciberdelincuentes mayor campo de acción para delinquir, en detrimento de ello, se perjudica a una sociedad cada vez más amenazada por estafas y fraudes electrónicos, generando amplias posibilidades de ser identificado y plagiado mediante estas nuevas modalidades delictivas. Esto se debe según Madalengoitia (2019), a un alto nivel de incertidumbre jurisdiccional, así como la falta de conocimientos por parte de entidades judiciales y estatales, siendo imperativo en este aspecto que legisladores del Estado y profesionales en materia de Derechos (jueces, fiscales y abogados) junto con organismos policiales,

implementen un marco legal contra delitos tecnológicos que promueva seguridad y libertad digital.

En cuanto al contexto local, los delitos informáticos en el Distrito Fiscal de Lima Norte han registrado un incremento considerable en los últimos años, a consecuencia del avance de las tecnologías lo que implicó que también la delincuencia empleara nuevos métodos para obtener ganancias al margen de la ley y en perjuicio de terceras personas, resultando ahí, de gran relevancia la obtención de la prueba digital a fin de poder investigar y a la postre obtener una sentencia condenatoria para los delincuentes. Los orígenes de dicha actividad delictiva derivan de la globalización, la cual se define como un sistema dinámico y estructurado caracterizado principalmente por su interdependencia e interconexión a nivel global (Flores, 2016).

Respecto al contexto social, el presente trabajo, se ubica en la globalización y digitalización de una sociedad, la cual, fue impulsada en mayor medida por la pandemia del COVID19, al uso constante de internet, debido al encierro y el otorgamiento de diferentes bonos por parte del estado, situación que fue aprovechada por los delincuentes para crear nuevas formas de obtener dinero de forma ilegal en el ciberespacio; resultando necesario profundizar respecto de la obtención de la prueba digital en los Delitos Informáticos durante el año 2021 en el Distrito Fiscal de Lima Norte a fin de poder llevar a cabo investigaciones con resultados exitosos, dado que la misma servirá como prueba determinante en las investigaciones. Asimismo, el aporte jurídico será que con el análisis realizado en la presente investigación, se efectuará un protocolo para la obtención, recolección y preservación de la prueba digital en los Delitos Informáticos contra el Patrimonio en el Distrito Fiscal de Lima Norte, a fin que sea usado por los operadores de justicia, y sea un marco de referencia a fin de evitar cuestionamientos y exclusiones de la prueba digital en juicio.

De igual forma se establecieron los problemas de investigación, siendo el Problema General: ¿Cuáles son los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021?, y como Problemas Específicos: 1.- ¿Cuáles son los procedimientos para la obtención a nivel preliminar de la prueba digital en

los delitos informáticos en Lima Norte en el año 2021? 2.- ¿Cuáles son los problemas de la actuación probatoria en juicio de la prueba digital en los delitos informáticos en Lima Norte en el año 2021? 3.- ¿Cuáles son los mecanismos y los instrumentos nacionales y de cooperación internacional para la obtención de la prueba digital en los delitos informáticos en Lima Norte en el año 2021?

Como parte del desarrollo de este estudio, se expuso la justificación teórica que radica en el análisis documental de diversas fuentes científicas así como legislativas tanto nacionales como internacionales vinculadas estrechamente con las categorías Prueba Digital y Delitos Informáticos y de esta forma brindar propuestas basadas en una sistematización de registro de cuentas, facilitando así la labor de los operadores de justicia; por lo cual este estudio servirá como base teórica para próximos estudios relacionados al tema. De igual forma se presenta la Justificación metodológica, debido a que este estudio emplea un método con enfoque cualitativo y diseño descriptivo, lo cual permitirá abordar de forma concatenada los argumentos y análisis que se deriven de la misma, y a partir de allí lograr los objetivos y responder las preguntas relacionadas con Delitos informáticos y la Prueba digital, siguiendo un carácter científico. De igual forma, posee Justificación práctica, ya que la realización de este estudio permitirá a través de una sistematización de datos, la identificación de posibles autores del delito y los tipos de métodos empleados, evitar duplicidad de investigaciones y deducir los tiempos de procesos de investigación, mediante la sistematización de datos.

Finalmente, este estudio estableció como Objetivo General: Identificar los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021, y como Objetivos Específicos se plantea: 1.- Determinar los procedimientos para la obtención a nivel preliminar de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. 2.- Determinar y establecer los problemas de la actuación probatoria en juicio de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. 3.- Identificar y establecer los mecanismos y los instrumentos nacionales y de cooperación internacional para la obtención de la prueba digital en los delitos informáticos en Lima Norte en el año 2021.

II. MARCO TEÓRICO

En esta sección se presentaron los antecedentes de investigación, relacionados con las categorías postuladas en este estudio. En cuanto al contexto internacional, se consideró la investigación de Ochoa (2021), quien empleó un método analítico comparando las definiciones del ciberdelito respecto a las leyes establecidas en Latinoamérica. Concluyó que a pesar de que existe una normativa que regula el cibercrimen dentro del Estado ecuatoriano, aun no es suficiente para la mitigación de este tipo de delitos. El aporte de este estudio destaca en la aplicación de políticas adecuadas en favor de proteger la información digital de los usuarios.

De igual forma, Vadell et al (2021), emplearon el método inductivo y de análisis. Y se concluyó que se debe especificar en las normas penales, criterios concretos para aplicar estos procedimientos de una manera flexible, evitando arbitrariedades. Como aporte este estudio favorece al análisis de los procesos de valoración de la prueba digital, y así se podrán realizar de forma objetiva las conclusiones.

Por su parte, Gómez (2021) empleó el método analítico. Concluyó que la normativa nacional rige plenamente sobre los principios de legalidad, de allí que el Estado no puede acordar otras normas tecnológicas restrictivas no contempladas en la ley. Este estudio permite visualizar el alcance de la jurisprudencia y el impacto de las TICs en el contexto judicial el cual debe ser regulado dentro de las leyes.

También, Acosta et al. (2020), emplearon un método mixto (cualitativo-cuantitativo), empleando como técnica el estudio exploratorio y análisis de teorías y Leyes, así se pudo evidenciar la importancia de conocer los tipos de delitos informáticos para establecer las debilidades de las organizaciones. Concluyeron que el delito informático más frecuente, es el *espionaje informático*, así como también los *sabotajes informáticos*, siendo la raíz de ello el desconocimiento y la falta de atención por parte de los usuarios. Su aporte se basa en destacar el rol primordial de los expertos en *seguridad cibernética* para salvaguardar información confidencial de los usuarios, ante la cantidad de ciberdelincuentes presentes en la web.

Asimismo, Ospina y Sanabria (2020) realizaron su estudio de enfoque cualitativo, teórico, documental y descriptivo. Concluyeron que el Estado

Colombiano presenta diversas amenazas cibernéticas, muchas de ellas causadas en la pandemia Covid-19, periodo en el que se incrementaron los delitos informáticos hacia otras organizaciones y personas.

De igual forma, Hernández (2019) aplicó en su investigación el método descriptivo documental. Según su análisis documental y legal se evidenció que la población no cuenta con la educación necesaria para establecer cuáles actos cibernéticos son considerados como delitos. Concluyó que es necesario de parte del gobierno realizar campañas en donde los habitantes adquieran conocimientos sobre los perjuicios y los beneficios del mundo digital. Esta investigación resaltó, la importancia de la educación digital y la responsabilidad directa del Estado para frenar los delitos cometidos a través de internet.

Finalmente, dentro del contexto internacional, Devia (2017), uso el método descriptivo. Evidenció que las directrices y políticas implementadas en el campo real (*persona a persona*), se han vuelto inadecuadas e insuficientes para combatir los delitos electrónicos. En ese sentido, concluyó la importancia de unir esfuerzos entre estados la sociedad y los expertos, para así crear nuevas estrategias e imponer una ley, especialmente en materia de Derecho penal, que sea exitosa y adecuada en el mundo virtual. Su aporte para este estudio se sustenta en la imperante necesidad de nuevas legislaciones que, alineadas con políticas internacionales, garanticen la protección de datos de los ciudadanos y entidades públicas y privadas.

A nivel nacional, Izquierdo (2021) empleó el método inductivo, analítico, sintético y hermenéutico, y el análisis documental fue basado en los informes de delitos informáticos desde el año 2018 al 2020. Concluyó que los cibercrimes económicos, por su complejidad, mermaron la eficacia de los procesos fiscales, por lo que es imperativo contar con una Fiscalía y cuerpo policial especializados y dotados con recursos tecnológicos de avanzada. Como aporte, los distintos métodos de análisis de datos antes mencionados servirán como referente para esta investigación.

También Vinelli (2021) efectuó un método analítico, y abordó los delitos informáticos y suplantación de identidad. Para ello realizó una revisión y análisis de la Ley 30096 Ley de Delitos Informáticos, modificada por la Ley 30171. Concluyó

que los problemas más relevantes son las actividades delictivas de sustracción de dinero y estafa a través de dichas plataformas bancarias, lo que ha generado innumerables dificultades para el ciudadano común y la banca. Este estudio aportó una visual del impacto de los ciberdelitos en el ámbito socioeconómico destacando la importancia de accionar nuevos instrumentos legales para combatirlos eficazmente.

Adicionalmente, Leyva (2021), realizó un estudio dogmático doctrinario. Concluyó que se debe profundizar en el estudio dogmático y renovar las leyes según realidad actual para garantizar mayor protección a los ciudadanos y por otra parte sancionar a los culpables de delitos informáticos. Como aporte este estudio permitió establecer perspectivas constitucionales para modernizar los procesos penales en función de mitigar o erradicar el ciberdelito.

Posteriormente Pastor (2020) empleó el método analítico y de observación. Se concluyó que existe la necesidad de modernización en los sectores especializados de la Fiscalía para lograr mejores análisis forenses de los delitos. Por ello, el autor desarrolló el modelo FORESYS, el cual permite identificar el modo de ejecución del ilícito, las herramientas empleadas y el perfil de quien los empleó. El aporte de esta investigación exalta la importancia de actualizar los recursos en función de atender las denuncias de delitos informáticos considerando el uso fundamental de tecnología avanzada.

En ese orden, Mori (2019), usó como tipo de investigación el descriptivo-explicativo, logrando así comprobar las hipótesis y objetivos establecidos en su estudio. Se concluyó que el amparo de la privacidad en las infracciones informáticas es uno de los principales elementos que influye en los desaciertos de las entidades señaladas, también se evidenció su impericia y falta de especialización en materia de delitos informáticos. Esto aportó evidencia sobre la falta de competitividad de los operadores de justicia que intervienen en la indagación y juzgamiento de las contravenciones perpetradas en internet.

De igual forma, Blossiers (2018) utilizó el método dogmático y diseño documental, basado en el análisis e interpretación doctrinario. Se evidenció que los llamados *hackers*, han logrado violentar estos sistemas de seguridad, haciendo uso ilegal de su conocimiento informático. Concluyó que los delitos informáticos

impactan severamente a los bancos en lo económico, social y jurídico. El aporte al presente estudio se basa en la evidente falta de sistemas tecnológicos de seguridad ante los fraudes bancarios lo cual origina desconfianza en los sistemas bancarios por parte de clientes y usuarios.

Finalmente, Pardo (2018) utilizó un enfoque cualitativo y nivel descriptivo explicativo. Evidenció así que existen deficiencias en cuanto al tratamiento jurídico-penal de los *delitos informáticos*. Concluyó que la Ley no está totalmente actualizada a las nuevas modalidades cibernéticas, en tal sentido, recomendó que el Congreso peruano inicie las acciones para la adhesión del Perú al convenio de Budapest. Como aporte, se evidenció que los delitos informáticos contra el patrimonio en su modalidad de estafa no contienen una sanción efectiva dentro del código, demostrando un alto nivel de incertidumbre e impunidad jurisdiccional.

A continuación se desarrollaron las definiciones correspondientes a los enfoques y categorías de estudio, para ello se iniciará con la conceptualización de la primera categoría Prueba digital, que conforme a lo señalado por Nikkel (2020) es una subdisciplina emergente del análisis forense que alcanza a las tecnologías, por tanto sirve al igual que otras evidencias, como instrumento probatorio de la verdad sobre aquellos acontecimientos que son objeto de investigación criminalística, con la distinción del carácter digital de la información, brindando sostenibilidad de lo que se denuncia. De manera que, según el autor se respalda la veracidad de la prueba digital como instrumento para comprobar los hechos, entre tanto, posee sus particularidades lo cual le distingue entre las evidencias tradicionales.

Mendoza (2022), señala que la Prueba digital es aquella evidencia cuya técnica de obtención fue a través de dispositivos tecnológicos, por ende se presenta bajo el formato de imágenes, videos o audios, los cuales por su naturaleza, se hayan almacenados en equipos, teléfonos móviles u otros similares, sin que ello impida, estar considerada dentro de la definición de *prueba documental*, del artículo 185 del Código Procesal Penal, el cual determinó que, para efectos de un proceso penal, es considerada como *prueba documental*.

Por su parte, Bujosa, Bustamante y Toro (2021), indicaron que la prueba digital es toda data que es obtenida por medios digitales o electrónico, la cual, tiene

como finalidad evidenciar un hecho relevante enfocado en una orden jurisdiccional. Se considera según lo anterior, otra particularidad de la prueba digital es su forma de obtención lo cual es clave para su valoración como tal, ya que, al estar la evidencia almacenada en un dispositivo, su extracción debe ser realizada de manera transparente.

Asimismo, Gooding (2019) describió la Prueba digital como aquellos soportes tecnológicos los cuales permiten conocer, archivar y/o reproducir hechos relevantes para la investigación, en forma de videos, audios, imágenes y datos propios o de terceros, etc., facilitando a las fuerzas del orden público, valorar la prueba presentada en función del delito imputado y así llevar a cabo una investigación efectiva, habiendo cumplido previamente con los requisitos y exigencias legales para que dicha evidencia sea introducida en el proceso como prueba y visualizada -sin alteraciones- por las partes y el tribunal.

Tal definición coincide con la connotación del factor tecnológico, el cual por sus tipologías hace que la prueba digital sea considerada compleja, sin embargo, esto no resta validez, una vez cumplido sus parámetros de obtención (Ledesma, 2016). Por otro lado, Prueba digital es entendida como aquella evidencia cuya técnica de obtención fue a través de dispositivos tecnológicos, por ende, se presenta bajo el formato de imágenes, videos o audios, los cuales, por su naturaleza, se hayan almacenados en equipos, teléfonos móviles u otros similares, sin que ello impida, estar considerada dentro de la definición de *prueba documental*, del artículo 185 del Código Procesal Penal (Mendoza, 2022).

Estando a lo señalado por los autores mencionados, se concluye que la Prueba Digital es aquella información obtenida a través de un medio electrónico o dispositivo digital mediante diversos formatos como imágenes, videos, audios, información de correos electrónicos, redes sociales u otros similares, la cual servirá como piedra angular para las investigaciones por la presunta comisión de Delitos Informáticos.

Seguidamente, se sustentaron los enfoques teóricos de la categoría Prueba Digital. Al respecto, se expuso la Teoría de la prueba informática, la cual establece, según Martínez (2019), el rompimiento de las concepciones de evidencias penales tradicionales, dando paso al tratamiento de pruebas usando soportes tecnológicos.

En tal sentido, pretende precisar los conocimientos técnicos que demanda este nuevo paradigma de parte de los involucrados en el campo del Derecho informático, donde la prueba digital es el elemento clave, alcanzando así una justicia más eficaz, adaptada a un contexto sociocultural digitalizado (Galvis y Bustamante, 2019). De lo señalado por dichos autores, se puede concluir que se destaca que la prueba digital es la piedra angular sobre la cual se sustenta el proceso judicial, por lo que su calificación y tipificación deben ser las más precisas para que los resultados reflejen el cumplimiento legal nacional e internacional.

De igual forma, se propone la Teoría de la Toma de decisión, según Beltrán et al (2018), mencionaron que la derrota de una de las partes y la victoria de la otra está en manos de un juez, quien debe considerar de forma concreta la aplicación de la Ley, teniendo en cuenta los hechos argumentados según las pruebas presentadas para establecer la decisión final que concluye el proceso. También, Blanco (2018) sostuvo que la toma de decisiones conlleva a un proceso racional el cual está sujeto a la cantidad y calidad de información, la capacidad del procesamiento de esta y los criterios, cogniciones o sustentos propios de quien decide. Tomsett et al (2020) indicaron que elementos como datos masivos, la falta de veracidad y las demoras en la validación de información, podrán generar escenarios de incertidumbre. En ese sentido, estando a lo señalado por los autores anotados, se concluye que la teoría señalada permitirá comprender la trascendencia de las sentencias en los casos vinculados a delitos informáticos, destacando principalmente, el rol de la prueba digital, ya que sobre esta se sustentarán los hechos, por ende, la toma de decisiones podría verse afectada.

Finalmente, el Enfoque de Justicia algorítmica, expuso que una manera de afrontar los cambios en los entornos de justicia penal es a través en el uso de herramientas tecnológicas, tomado como base las características particulares del proceso penal, para así diseñar sistemas interactivos adecuados, con los cuales se llegue a la toma de decisiones más acertada (Castro y Rodríguez, 2018). En línea con ello, Završnik (2021) sostuvo que tales automatizaciones deben sostenerse sobre el principio de la igualdad y el derecho a un juicio justo dentro de los procedimientos judiciales. Asimismo, Eubanks (2018), señaló que se debe garantizar que la persona condenada cuente con la posibilidad de cuestionar la

metodología aplicada, desde los datos introducidos en el algoritmo, hasta el diseño general del sistema de toma de decisiones. Concluyéndose de lo expuesto precedentemente, que este enfoque plantea soluciones para combatir los delitos informáticos, empleando los avances que provee la tecnología, con el objetivo de mitigar de forma eficiente dicha problemática social-global.

Se expuso a continuación las definiciones correspondientes a primera sub categoría: Procedimientos para la obtención de prueba digital, consiste según Vadell et al. (2021) en el cumplimiento normalizado de exigencias técnicas y legales para garantizar la integridad de prueba digital, al respecto, se puede mencionar: identificar al remitente, cumplir con la verificación de envío y entrega, almacenarla en condiciones seguras, garantizar su confidencialidad, registrar información del propietario del ordenador y sus elementos técnicos, como certificado electrónico, la utilidad, y su finalidad legal, también, es fundamental que este procedimiento vele por el respeto de los derechos fundamentales de privacidad y el secreto de las comunicaciones. Estando a lo indicado se concluye que la rigurosidad e importancia del cumplimiento procesal de la prueba digital, está enfocado en evitar alterar, o anular su esencia y lograr se mantenga su validez jurídica.

Como segunda subcategoría se estableció la Actuación probatoria en juicio. De acuerdo con Vera (2020), este proceso se rige por, la defensa procesal en su faz instrumental de derecho a probar y controlar la prueba, establecido en art. 8, inciso 2, literal f (Convención Americana de Derechos Humanos), manifestándose: 1) que cada parte cuenta con la oportunidad de plantear los medios de prueba pertinentes a su tesis litigiosa, 2) que estos medios sean adecuadamente admitidos según criterios de razonabilidad intrínseca y extrínseca, 3) que esto último aspecto se traduzca en un acto jurisdiccional decisorio procedente y motivado, 4) que su ejecución esté dentro de los procedimientos legalmente establecidos y, 5) que se otorguen garantías para una efectiva intervención de partes durante su juicio.

Por tanto, de lo expuesto se concluye que la actuación probatoria en juicio de la prueba digital resultará trascendental para una sentencia condenatoria, siempre y cuando se admitan y actúen con las garantías procesales, y que pueda ser sujeto al contradictorio, por lo que el rigor, fundamento y control legal de los

procesos judiciales darán validez a la prueba digital, por tanto, deben ser cumplidos los protocolos establecidos para lograr tal fin.

Ahora, corresponde presentar las definiciones de la denominada segunda categoría Delitos Informáticos, comenzando con Acurio (2016) se determinó que los delitos informáticos son acciones realizadas con intención de delinquir las cuales están vinculadas directamente con el conocimiento y uso de equipos de tecnologías, donde la víctima ha sufrido una pérdida y el victimario ha sustraído un bien de forma impropia. Asimismo, Acosta et al. (2020), expuso que, son todos aquellos actos ilícitos perpetrados a través del uso inapropiado de la tecnología, donde se logra vulnerar la privacidad y confidencialidad de datos e información de un tercero, ya sea personal, económica o laboral, con el fin de dañarlos o extraerlos infringiendo la ley.

También, Bélanger (2017) definió los delitos informáticos como procedimientos delictivos ejecutados por medio de sistemas tecnológicos, que involucran el acceso, interacción y transferencia ilegal de datos, asimismo incluyen la pornografía infantil, plagio de identidad y de derechos de autor. Se concluye de los autores mencionados, que los delitos informáticos son ilícitos efectuados valiéndose de los medios tecnológicos que hacen más difícil su persecución, y por ende se presenta una amplitud de delitos en la virtualidad que se extiende sin limitaciones por lo que representa un daño a la sociedad a escala mundial.

Asimismo, se presentaron los sustentos teóricos y/o enfoques relacionados con las categorías de investigación. Con relación a ello, el enfoque Naturaleza de la conducta, propone según Cisneros y Jiménez (2021) analizaron -a través de diversas doctrinas jurídicas - ¿Cómo un sujeto (activo) se aprovecha de los bienes otro sujeto (pasivo)? De acuerdo con este enfoque, las personas se adaptan y se rigen según principios conductuales que bajo ciertas circunstancias llegan a debilitarse frente al cumplimiento de las normas. A la par de ello, Vargas (2019) sostuvo que el sistema penal debe actuar enmarcado en su poder punitivo para evitar engaños y estafas, ya que esto causa dolo, limitación a la libertad y prejuicios al patrimonio personal, institucional y social. Al respecto, se concluye que el enfoque Naturaleza de la conducta permite identificar las conductas delictivas de

los sujetos, conllevando, tal como plantea los autores al análisis introspectivo de las motivaciones particulares para ejecutar acciones ilegales de cada individuo.

Mientras que la Teoría del Delito, se concibe según Valarezo et al. (2019), como aquella que, dentro del Derecho penal está orientado a garantizar la identidad normativa, la constitutiva y la social, ya que va enlazando al hombre dentro de su contexto social. Asimismo, Rivero (2017) sostuvo que la trascendencia de la teoría del delito en el campo del derecho penal y en particular sobre la Ley penal, ha ido evolucionando, adoptando nuevas tipologías surgidas según la realidad presente, lo cual permite a través de una sucesión de cuestionamientos, analizar la conducta humana. Igualmente, Bacigalupo et al. (2019) expuso que una de las ramas de la Teoría del delito, es la *Teoría jurídica del delito*, la cual permite saber -siguiendo un sistema de normas legales- la existencia de un evento; si éste es ilegal, y, si es condenatorio para el sujeto. Estando a lo señalado, se puede concluir que la Teoría del delito está enfocada básicamente a la conducta humana con su contexto social.

Entre tanto, la Teoría general de la disuasión (GDT) explica, *a través del entendimiento del actuar*, por qué las personas cometen delitos y qué estrategias pueden ayudar a disuadirlos. Salgado (2021), señaló que la disuasión ocurre cuando las personas evitan los delitos debido a los costos o las consecuencias desagradables de esos delitos, evidenciando así que el pensar y el actuar del individuo varía en concordancia con aspectos reflexivos y biopsicosociales que le rodean. De manera que la doctrina jurídica debe diseñar herramientas y recursos tecnológicos disuasivos que, dentro del proceso litigante, permita influir en los perpetradores de delitos informáticos modificando su conducta delictiva por otra más acorde y civilizada (Bhattacharjee y Shrivastava, 2018). Por lo que se concluye que esta teoría permite comprender cómo a través de la psicología se puede influenciar en la manera de pensar y actuar de un individuo, partiendo de un enfoque normativo, lo cual permita dentro del correcto ejercicio del Derecho, hacer cumplir las leyes y sanciones por los daños causados.

En ese orden, fue propuesta como primera subcategoría, Mecanismos e Instrumentos nacionales, el cual no es otro que, la Ley N° 30096: Ley de Delitos Informáticos (21 de octubre del 2013), la cual se perfila -como principal instrumento legal- contra los ciberdelitos en el Perú. Su finalidad es sancionar las conductas

ilícitas que vulneran los sistemas y datos informáticos, así como, otros bienes jurídicos de relevancia penal, mediante la utilización de tecnologías de la información o de la comunicación, para garantizar la lucha eficaz contra la ciberdelincuencia (Robles, 2016). De lo antes descrito, se resalta que la legislación nacional puede brindar los reglamentos y procedimientos jurídicos para combatir el ciberdelito, sin embargo, aún resultan insuficientes para la persecución de dichos delitos, dado que no existen medios tecnológicos suficientemente modernos para determinar las nuevas modalidades de ciberdelitos.

Asimismo, se expuso como segunda subcategoría, Cooperación internacional, siendo el Convenio de Budapest el principal instrumento legal a nivel internacional en la lucha contra los delitos informáticos, el cual entró en vigor el 1° de julio de 2004 y respecto al Perú, se estableció su entrada en el 22 de setiembre del 2019 (Becker, 2020). El objetivo de este acuerdo, según Suárez (2022), es combatir el crimen organizado de alcance transnacional dentro de la visión de *ciberseguridad* entre sus países integrantes, definiendo para ello, procedimientos y sanciones específicas, en la búsqueda de reducción de delitos cometidos en internet.

Al respecto, cabe señalar que el ciberdelito representa un desafío para la justicia internacional por ello es importante unir esfuerzos y armonizar las leyes para combatirlo eficazmente, reduciendo sus efectos con estrategias globales, y que si bien es cierto existen tratados de cooperación suscritos por el Perú con determinados países, es necesario expandirlo a más países, así como agilizar la tramitación cuando necesitemos la cooperación de una entidad con residencia en un país extranjero.

Finalmente se tiene como Aporte epistemológico la búsqueda de nuevas propuestas y sistematización de las categorías de estudio, a partir de una profunda revisión documental, procesal y práctica, para comprender la funcionalidad de las nuevas tecnologías y el uso generalizado que la sociedad hace de ellas. Por lo que resulta necesario un estudio completo de los Delitos tecnológicos y la Prueba digital, desde su obtención hasta su valoración, lo cual permitirá lograr los cambios necesarios en el sistema jurisdiccional, para revertir conflictos señalados en la realidad problemática.

III. METODOLOGÍA

La presente investigación se realizó desde un enfoque cualitativo. Según Guerrero (2016) la investigación cualitativa es aquella que emplea principios teóricos para realizar estudios asociados principalmente al área social, con el fin de hacer más comprensible los hechos.

3.1 Tipo y diseño de investigación

3.1.1. Tipo de investigación: La investigación fue de tipo básica, ya que se busca contribuir con el conocimiento preexistente en la materia de Delitos Informáticos y la valoración de la Prueba Digital, el cual reviste un carácter científico. Al respecto, Escudero y Cortez (2018) señalaron que la investigación básica, es aquella que toma en cuenta fundamentos teóricos para realizar el estudio de la realidad problemática, teniendo como objetivo, descubrir leyes o principios básicos.

3.1.2. Diseño de investigación: El diseño de la presente investigación se orientó en la Teoría fundamentada, ya que ésta permite profundizar en la información de los datos, a partir de los cuales el autor hará emerger una teoría o modelo, esto implica, desarrollar una comprensión del fenómeno observado, por medio del descubrimiento y la inducción (Espriella y Restrepo, 2020).

3.2 Categorías, Subcategorías

Para la realización de este proyecto se empleó las siguientes categorías, siendo en primer orden prueba digital, que tiene dos subcategorías denominadas procedimientos y actuación probatoria en juicio; la segunda categoría desarrollada es delitos informáticos, la cual se subdivide en dos subcategorías, siendo las siguientes: mecanismos e instrumentos nacionales y cooperación internacional.

Tabla 1.

Matriz de Categorización

| Categorías | Autor Base | Subcategorías |
|------------|------------|---------------|
|------------|------------|---------------|

| | | |
|---------------------------|---|--|
| Prueba digital | Es aquella evidencia cuya técnica de obtención fue a través de dispositivos tecnológicos, por ende, se presenta bajo el formato de imágenes, videos o audios, los cuales, por su naturaleza, se hayan almacenados en equipos, teléfonos móviles u otros similares, sin que ello impida, y que su incorporación y actuación probatoria en juicio, debe efectuarse acorde a las reglas de juicio, debiendo ser valorado como prueba documental conforme al artículo 185° del Código Procesal Penal (Mendoza, 2022). | -Procedimientos. - Actuación probatoria en juicio. |
| Delito informático | Son todos aquellos actos ilícitos perpetrados a través del uso inapropiado de la tecnología, donde se logra vulnerar la privacidad y confidencialidad de datos e información de un tercero, ya sea personal, económica o laboral, con el fin de dañarlos o extraerlos infringiendo la ley (Acosta et al. 2020) En el Convenio de Budapest (2001) se señala cuáles son los mecanismos e instrumentos nacionales y de cooperación internacional, tanto para la investigación preliminar como judicial. | -Mecanismos e instrumentos nacionales - Cooperación internacional |

Nota: Elaboración propia.

3.3 Escenario de estudio

El escenario de la investigación se delimitó a la ciudad de Lima, en el Distrito Fiscal de Lima Norte, toda vez que los abogados especialistas en derecho penal que participaron en la investigación radican en dicha ciudad, así como los jueces especializados en lo penal, los mismos que serán entrevistados en temáticas concernientes la prueba digital y delitos informáticos.

3.4 Participantes

Los participantes en la presente investigación fueron 4 Fiscales penales y 3 Jueces Especializados en lo penal que laboran en el Distrito Fiscal de Lima Norte.

Tabla 2. *Caracterización de participantes*

| N° | Informantes | Descripción | Código |
|-----------|------------------------------|--|---------------|
| 1 | Tres jueces en materia penal | Corte Superior de Justicia de Lima Norte | PJ/CSJLN |
| 2 | Cuatro fiscales penales | Ministerio Público – Distrito Fiscal de Lima Norte | MP/DFLN |

Nota: Elaboración propia.

3.5 Técnicas e instrumentos de recolección de datos

Para desarrollar este estudio se empleó el análisis teórico de la doctrina nacional, además se utilizó la entrevista para recoger la información vertida por los magistrados especializados, entre ellos tres Jueces especializados en lo penal y cuatro Fiscales especializados en lo penal. Los instrumentos fueron la ficha de registro de análisis y guía de entrevista, la cual fue diseñada con preguntas abiertas que permitieron al entrevistado brindar información con mayor detalle. Las definiciones conceptuales son las que se indican:

3.5.1 Técnicas

3.5.1.1 Entrevista: es un diálogo que se realiza entre el investigador y el participante con el fin de obtener información relevante sobre los hechos, comportamientos, experiencias y opiniones suscitados en torno al fenómeno en estudio, lo cual permite al investigador desarrollar sus conclusiones satisfactoriamente (Arias, 2020)

3.5.1.2 Análisis teórico: se basa en la identificación de una problemática y sus soluciones a través de una revisión documental, siguiendo por parte del investigador, un modelo sistemático para la correcta selección de archivos durante el proceso de búsqueda, para luego de ello, hacer una interpretación sobre dichos basamentos (López y Fachelli, 2015).

3.5.2 Instrumentos

3.5.2.1 Ficha de registro de análisis: es un instrumento esencial de la investigación cualitativa, caracterizado por contribuir a la transformación de fuentes literarias convirtiéndolos en análisis precisos (datos) para una mejor interpretación de los fenómenos sociales, una vez que se han estudiado las fuentes teóricas del tema (López y Fachelli, 2015).

3.5.2.2 Guía de entrevista: Es un documento físico -manual o computarizado-, que está diseñado para realizar la entrevista con mayor orden y pulcritud, en la cual se presentan las preguntas abiertas o cerradas según sea más conveniente, para obtener información relevante para la investigación (Arias, 2020).

Tabla 3. Validez de contenido de los instrumentos de recolección de datos

| INSTRUMENTO | EXPERTO | GRADO ACADÉMICO | CARGO | ESPECIALIDAD | OPINIÓN |
|--------------------|-----------------------------|---------------------------------------|---|------------------------|-----------------|
| Guía de entrevista | Miranda Aburto Elder | Dr. en derecho Penal | Abogado y docente universitario | Penal y Procesal Penal | Si es aplicable |
| Guía de entrevista | Jose Walter Lopez Fernandez | Mg. en Derecho Penal y Procesal Penal | Fiscal Adjunto Provincial del Distrito Fiscal de LN | Penal y Procesal Penal | Si es aplicable |
| Guía de entrevista | Fiorella Linares Pérez | Mg. en Derecho Penal y Procesal Penal | Juez Especializado del Distrito Judicial de LN | Penal y Procesal Penal | Si es aplicable |

Nota: Elaboración propia.

3.6 Procedimiento

La presente investigación se realizó dentro de lo establecido por la metodología científica cualitativa. En ese sentido, se identificó en el capítulo 1, la realidad problemática, para luego establecer los problemas y objetivos de investigación. Posteriormente se desarrolló el marco teórico referencial donde se citaron diversos autores de investigaciones relacionadas con la Prueba digital y el delito informático, asimismo, se definieron las categorías y subcategorías de estudio y sus fundamentos. Continuando con el marco metodológico, se definió el modelo de investigación y las técnicas a seguir según dicha metodología también se procedió la realización de la entrevista a los participantes siguiendo las pautas de rigor, también se realizó el análisis documental, logrando así obtener la información doctrinaria, cumpliendo con los objetivos propuestos. Finalmente, se detallaron los recursos y presupuestos necesarios para la realización de este estudio, así como el cronograma de ejecución, en el capítulo 4, con lo cual se dio cierre a la investigación.

3.7 Rigor científico

De acuerdo con López et al. (2019), el rigor científico se consideró en el desarrollo de la presente investigación tomando en cuenta que se empleó una estructura secuencial basado en la metodología científica. Asimismo, los instrumentos empleados fueron validados por expertos lo que permitió obtener resultados avalados desde la ciencia.

Alineado con lo anterior, este estudio demostró cumplir con aspectos esenciales tales como: Consistencia lógica, ya que la información recogida fue

objetiva, clara y específica. Credibilidad, considerando que el desarrollo de la misma está fundamentado sobre estudios comprobados y el criterio de expertos en la materia que garantizan la veracidad de la información obtenida, por lo que se puede determinar que cumple con las especificaciones investigativas lo que eleva su calidad y rigor científico.

3.8 Método de análisis de datos

Los datos recogidos con la guía de la entrevista fueron analizados, desde la perspectiva del método comparativo, de esa forma examinar los resultados encontrados con otras posturas y estudios realizados. A su vez se empleó el método analítico para desglosar las categorías y subcategorías expresadas también en los problemas y objetivos de investigación, de esa forma comprobar si a través de las respuestas de los entrevistados se responde a los objetivos por alcanzar. También se empleó el método inductivo a fin de sistematizar las teorías existentes con los hallazgos encontrados acorde al problema de investigación, finalmente se empleó el método hermenéutico para interpretar los datos registrados, y que estos a su vez puedan ser usados, analizados, interpretados por instituciones de carácter jurídico en relación con el tema investigado.

3.9 Aspectos éticos

Se demostró el cumplimiento de los aspectos éticos exigidos por la Universidad César Vallejo, a través la realización ordenada y sistemática del presente trabajo investigativo. De igual forma, todas las fuentes citadas durante el desarrollo del marco teórico de este estudio fueron referenciados siguiendo los estándares establecidos en la 7ma edición de la Asociación Estadounidense de Psicología (APA), respetando en ese sentido, los derechos de autor y la propiedad intelectual. Asimismo, la metodología científica empleada sustentó la credibilidad de la presente investigación, considerando que en ninguna circunstancia fueron manipulados los resultados obtenidos. Finalmente, los antecedentes que se expusieron en la presente investigación obedecen a la información recolectada de fuentes confiables como artículos científicos, revistas indexadas, leyes nacionales e internacionales, lo cual se puede comprobar en las referencias electrónicas que sustentan la investigación, basado en ello se demuestra la confiabilidad y cumplimiento ético de este estudio.

IV. RESULTADOS Y DISCUSIÓN

Para el desarrollo de la presente tesis se entrevistó a Jueces y Fiscales Penales del Distrito Fiscal de Lima Norte, quienes expusieron sus puntos de vista sobre cada una de las interrogantes planteadas, las mismas que estuvieron relacionadas con el objetivo general y con los objetivos específicos que se plantearon. El objetivo general fue identificar los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021. Al respecto, Mendoza (2022), señala que la Prueba digital es aquella evidencia cuya técnica de obtención fue a través de dispositivos tecnológicos, por ende, se presenta bajo el formato de imágenes, videos o audios, los cuales, por su naturaleza, se hayan almacenados en equipos, teléfonos móviles u otros similares, sin que ello impida, estar considerada dentro de la definición de prueba documental, del artículo 185 del Código Procesal Penal. Por otro lado, Gooding (2019) describió la Prueba digital como aquellos soportes tecnológicos los cuales permiten conocer, archivar y/o reproducir hechos relevantes para la investigación, en forma de videos, palabras (audios), imágenes y datos propios o de terceros, etc., facilitando a las fuerzas del orden público, valorar la prueba presentada en función del delito imputado y así llevar a cabo una investigación efectiva, habiendo cumplido previamente con los requisitos y exigencias legales para que dicha evidencia sea introducida en el proceso como prueba y visualizada -sin alteraciones- por las partes y el tribunal.

Al respecto, los entrevistados ante la primera pregunta ¿Considera usted que es necesario la prueba digital durante la investigación preliminar en los delitos informáticos? Manifestaron de forma unánime que si, debido a que dicho medio de prueba resultara necesario para el progreso de la investigación y que en muchos casos es fundamental para el mismo. Por su parte con relación a la segunda pregunta ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Indicaron de forma mayoritaria que es en la realización

de la cadena de custodia y la preservación de la evidencia digital, dado que ello, es el punto de cuestionamiento de la defensa de un investigado.

Respecto a la tercera pregunta ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?. Señalaron en dos posiciones, la mayoría indicó que si existe una diferencia, dado que no es lo mismo efectuar la recolección y cadena de custodia a un elemento común que a un medio electrónico, dado la naturaleza del mismo; sin embargo, otro grupo señaló, que no existe diferencia en la cadena de custodia dado que es la misma para la prueba digital y para la que no es, puesto que ambos están referidos al soporte físico, sino que aunado a ello, en la prueba digital se debe realizar otras acciones con aplicaciones de software o instrumentos que permitan asegurar la evidencia, o que esta no sea alterada.

En relación a la cuarta pregunta, ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? La mayoría a señalado que conocen a la función HASH que sirve para asegurar la evidencia digital y que ésta no puede ser alterada, asimismo han indicado también el software “Centro premiun cellebrite” y UFED, de igual manera un entrevistado menciona la cadena de custodia. En cuanto a la quinta pregunta ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?, la mayoría señaló Guía práctica para requerir información a proveedores internacionales y D.L. N° 1412 – Ley de Gobierno Digital, un segundo grupo hizo referencia a la Ley 30096 Ley de Delitos Informáticos y el Reglamento de la de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados.

Respecto a la sexta pregunta ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?. En este punto la mayoría hizo referencia a la Tutela de Derechos a fin de prevenir la adulterabilidad de la prueba digital, por otro lado, de manera persona, también hicieron referencia al Código Hash y efectuar la inadmisibilidad

de en el ofrecimiento de pruebas. En relación a la séptima pregunta ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué?, la mayoría de entrevistado coincide en señalar que no ha tenido la oportunidad de participar en audiencia donde se cuestione la prueba digital, no obstante ello, una participante indicó que en un caso se cuestionó las capturas de conversaciones mediante el aplicativo WhatsApp toda vez que en la recolección de dicha información no se realizó desde el celular o aparato en el cual obraba la misma, solo se tenía las capturas presentadas por la parte denunciante. El abogado defensor del imputado indicaba que no se tenía certeza si esa información era auténtica por cuanto eran capturas que podrían haber sido manipuladas, teniendo en cuenta la tecnología.

De otro lado, el primer objetivo específico fue determinar los procedimientos para la obtención a nivel preliminar de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. Sobre el particular, Vadell et al. (2021) señala que es el cumplimiento normalizado de exigencias técnicas y legales para garantizar la integridad de prueba digital, al respecto, se puede mencionar: identificar al remitente, cumplir con la verificación de envío y entrega, almacenarla en condiciones seguras, garantizar su confidencialidad, registrar información del propietario del ordenador y sus elementos técnicos, como certificado electrónico, la utilidad, y su finalidad legal, también, es fundamental que este procedimiento vele por el respeto de los derechos fundamentales de privacidad y el secreto de las comunicaciones.

Ahora bien, respecto a este objetivo se planteó la octava pregunta ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. De forma mayoritaria los entrevistados hicieron referencia al tratamiento de la prueba digital desde su obtención, cautelando el medio de prueba a fin de evitar futuros cuestionamientos, para lo cual se hace hincapié en la cadena de custodia, su custodia, con el debido tratamiento al soporte de la evidencia digital, para finalmente se le practique la pericia que corresponda. En el mismo sentido se planteó la novena pregunta ¿Considera Ud, que la normatividad actual es suficiente

para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?. Mayoritariamente los entrevistados indicaron que existe poca regulación o información al respecto, dado su naturaleza o carácter novísimo, y que la realidad está generando casuística que sobre pasa el marco normativo actual, precisando un entrevistado que debería diseñarse protocolos de actuación conjunta de los operadores de justicia; asimismo, otro entrevistado señala que la normatividad sería suficiente, pero que resultaría necesario es el mejoramiento de los equipos periciales para hacer más dinámico y factible la recopilación de pruebas.

Por su parte, el segundo objetivo específico fue determinar y establecer los problemas de la actuación probatoria en juicio de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. Sobre el particular, Vera (2020), señala que la actuación probatoria a nivel judicial se rige por, la defensa procesal en su faz instrumental de derecho a probar y controlar la prueba, establecido en art. 8, inciso 2, literal f (Convención Americana de Derechos Humanos), manifestándose: 1) que cada parte cuenta con la oportunidad de plantear los medios de prueba pertinentes a su tesis litigiosa, 2) que estos medios sean adecuadamente admitidos según criterios de razonabilidad intrínseca y extrínseca, 3) que esto último aspecto se traduzca en un acto jurisdiccional decisorio procedente y motivado, 4) que su ejecución esté dentro de los procedimientos legalmente establecidos y, 5) que se otorguen garantías para una efectiva intervención de partes durante su juicio.

Ante ello se planteó la décima pregunta ¿Cuáles con los cuestionamientos más recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?, en el cual la mayoría de los participantes señaló no haber participado en juicio por este tipo de delitos, indicando una de las entrevistadas que participó en un caso donde se cuestionó el proceso de recojo de evidencia, y que el mismo debería efectuarse de la misma fuente, por lo que se cuestionaba la autenticidad. Así también, ante la décimo primera pregunta ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?, un grupo indico como principal cuestionamiento la obtención y recolección de la evidencia digital y que no ha seguido los procedimientos para su obtención, así como cuestionar la propia

cadena de custodia, así también otro entrevistado hizo referencia a la manipulación de los dispositivos informáticos que podrían alterar la información que almacena y de utilidad para a investigación. Con relación a la décimo segunda pregunta ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?. En este extremo los entrevistados de forma unánime indicaron que, si existe una problemática, refiriendo diversas causas, como son la escasa logística en la falta de programas, licencias de software para la obtención de información o pericias, la demora en la realización de pericias debido a la falta de personal, o que no son idóneos para dicha tarea, y que incluso las pericias arrojan resultados distintos entre sí.

De otra parte, respecto el tercer objetivo específico fue Identificar y establecer los mecanismos y los instrumentos nacionales y de cooperación internacional para la obtención de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. Como instrumento nacional, se tiene a la Ley N° 30096: Ley de Delitos Informáticos (21 de octubre del 2013), la cual se perfila -como principal instrumento legal- contra los ciberdelitos en el Perú. Su finalidad es sancionar las conductas ilícitas que vulneran los sistemas y datos informáticos, así como, otros bienes jurídicos de relevancia penal, mediante la utilización de tecnologías de la información o de la comunicación, para garantizar la lucha eficaz contra la ciberdelincuencia (Robles, 2016).

Con relación a la décimo tercera pregunta ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?. Los entrevistados brindaron respuestas diversas, dos respondieron la Guía práctica para requerir información a proveedores internacionales de internet, dos indicaron el Convenio de Budapest, dos refirieron el NCPP, otro hizo referencia al Manual para el recojo de la evidencia digital y la Ley 29733 – Ley de Protección de datos personales, un entrevistado indicó el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados y Acuerdos Plenarios N° 5-2010/CJ-116 y N° 6-2012/CJ-116 que están referidos al recojo de evidencia y custodia de los mismos, y otro entrevistado indicó que desconocía. Así también se planteó la décimo cuarta pregunta ¿Cuáles son los

instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?. Al respecto cinco entrevistados coincidieron que uno de los instrumentos internacionales es el Convenio de Budapest, y luego agregaron instrumentos diversos, como es la Norma ISO/IEC27037.2012, Protocolo del grupo de trabajo científico en evidencia digital (SWGDE) “Best Practices for Computer Forensics”, la Guía práctica para requerir información a proveedores internacionales de internet y convenios celebrados por nuestro país con otros países sobre ciberdelincuencia, sin precisar a cuales se refieren, mientras dos señalaron desconocer dicha información.

Con relación a las similitudes de los resultados encontrados con trabajos afines, se puede señalar que a nivel nacional existen similitudes con los planteamientos de Pastor (2020), que indicó la necesidad de modernización en los sectores especializados de la Fiscalía para lograr mejores análisis forenses de los delitos a fin de atender las denuncias de delitos informáticos con el uso fundamental de tecnología avanzada; lo cual también se verifica de la presente investigación, donde los entrevistados, tanto Fiscales como Jueces Penales han señalado como parte de la problemática de la obtención de la prueba digital, a la falta de logística tanto a nivel humano como de recursos tecnológicos, lo que dificulta tanto desde su recolección, preservación, actuación y extracción a nivel preliminar de la evidencia digital, así como una demora en los pronunciamientos de los peritos, ya sea de la Policía Nacional del Perú o del Ministerio Público.

Asimismo existe similitud con lo señalado por Mori (2019), que concluyó la existencia de desaciertos de los operadores de justicia, evidenciando falta de especialización y de competitividad de los aludidos cuando intervienen en la indagación y juzgamiento de los delitos informáticos; lo cual también se puede colegir en parte en la presente investigación, dado que existe aún desconocimiento respecto del procedimiento para la obtención de la prueba digital, así como la extracción de su información y preservación de la misma, dado su carácter relativamente nuevo, y poco desarrollo en nuestro país.

De otro lado, se advierten discrepancias con lo señalado por Leyva (2021), quien concluyó en que se debe profundizar en un estudio dogmático y renovar las

leyes según la realidad nacional a fin de establecer perspectivas constitucionales para modernizar los procesos penales en función de mitigar o erradicar el ciberdelito; en tanto, la norma la Ley N° 30096 – Ley de Delitos Informáticos puede aplicarse y tipificar los ilícitos que hasta la fecha se han venido suscitado, y que lo necesita mayor atención es la optimización de la obtención de la prueba digital y de la investigación en si, lo cual es parte del procedimiento para luego traducirse en su actuación probatoria, asegurándose que no adolezca de vulneraciones a Derechos Fundamentales.

Finalmente se encontró diferencias con el trabajo realizado por Izquierdo (2021), quien señaló que los ciberdelitos económicos, por su complejidad, mermaron la eficacia de los procesos fiscales, por lo que es imperativo contar con una Fiscalía y cuerpo policial especializados y dotados con recursos tecnológicos de avanzada; en tanto, consideramos que la deficiencia en las investigaciones fiscales no se deben a la complejidad de los delitos informáticos, sino en el procedimiento para el aseguramiento de la prueba y posterior actuación en juicio, pero que si resulta necesario las unidades especializadas que conozcan dichos delitos.

De igual modo, se encontró diferencias con lo señalado por Vadell et al (2021), quien concluyó que se debe especificar en las normas penales, criterios concretos para aplicar procedimientos de una manera flexible, evitando arbitrariedades; al respecto consideramos que dichos criterios no deben especificarse en las normas penales, sino en Guías o Protocolos que permitan ser una herramientas a los operadores de justicia en las investigaciones por Delitos Informáticos, ello a efectos de poder garantizar que los elementos de prueba que se obtengan no adolezcan de algún vicio, y por tanto no sean excluidos del proceso, y sirvan para arribar a la convicción que el hecho investigado se cometió o no.

V. CONCLUSIONES

Primero.- Se identificó los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021, advirtiéndose que no se cuenta con una norma específica que estandarice la recolección, obtención conservación y análisis de la prueba digital, se presenta una falta de logística en los operadores de justicia, escasez y falta de tecnología en equipos informáticos, software, licencias de programas; así también, se advierte que existe demora en practicarse las pericias a la prueba digital, dado el escaso número de peritos en el Ministerio Público como en la Policía Nacional del Perú, quienes tienen competencia a nivel nacional; de igual modo, no existe una capacitación a los operadores de justicia, Ministerio Público, Policía Nacional del Perú y Poder Judicial, en el procedimiento para recabar la evidencia digital, consistente en su recolección, obtención conservación y análisis, asegurando su originalidad e inalterabilidad del mismo.

Segundo.- Se determinó los procedimientos para la obtención a nivel preliminar de la prueba digital en los delitos informáticos en Lima Norte en el año 2021 que son: a) *Identificación* que consiste en obtener información preliminar sobre hecho del ilícito informático a fin de tener un panorama de cómo proceder y que buscar; b) *Recolección*, consistente en recabar la información de la escena del crimen, la cual incluye los dispositivos digitales, sistemas y servidores digitales, para lo cual se identifica y protege la escena del delito de la contaminación, y conserva las pruebas volátiles; c) *Obtención*, consistente en la extracción de información (pruebas digitales) de los dispositivos digitales incautados, de manera que se conserve la integridad de las pruebas, garantizándose que los datos no se alteren; d) *Conservación*, con el cual se busca proteger las pruebas digitales contra las modificaciones, debiéndose mantener la integridad de dichas pruebas en cada fase de su manejo, para lo cual se debe mantener en todo momento la cadena de custodia; y, e) *Análisis*, entendiéndose al análisis forense digital que implica evaluar e interpretar las pruebas digitales y comunicar los resultados del análisis.

Tercero.- Se determinó y estableció que los problemas de la actuación probatoria en juicio de la prueba digital en los delitos informáticos en Lima Norte en el año 2021 están referidos a los cuestionamientos que se efectúan en primer lugar al recojo de la evidencia digital, tanto al efectuarse la cadena de custodia, como en la correcta manipulación del dispositivo que almacena la evidencia digital, esto es a través de un procedimiento que garantice su fiabilidad y autenticidad.

Cuarto.- Se identificó los mecanismos y los instrumentos nacionales para la obtención de la prueba digital en los delitos informáticos en Lima Norte en el año 2021 que son utilizados por los operadores de justicia, como son el Manual para el Recojo de la Evidencia Digital – Resolución Ministerial N° 848-219-IN que está referida al aseguramiento físico de los dispositivos electrónicos, el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados - Resolución N° 729-2016-MP-FN, Directiva N° 03-19-2015-DIRGEN-PNP/EMG-PNP – Normas y Procedimientos Policiales para Proteger la Escena del Delito y garantizar la cadena de custodia, las mismas que son normas destinadas para el recojo y custodia de la evidencia física, que para el caso de Delitos informáticos solo serviría para el recojo del soporte físico de la evidencia digital, mas no respecto de su contenido digital o alguna actuación concreta de dicha información como es en los casos de flagrancia delictiva, menos aún está referida en los supuestos que la información se va a extraer del mundo digital como es el caso de la información de correos electrónicos, Facebook u otras redes sociales; y respecto a las normas internacionales tenemos al Convenio de Budapest que en el Perú entró en vigencia desde el 01 de diciembre del 2019, el cual está mas orientada al marco normativo para perseguir e implementar los delitos informáticos, y que promueve la cooperación internacional.

VI. RECOMENDACIONES

Primero.- Que el Estado a través del MEF dote de mayor presupuesto al Ministerio Público y a la Policía Nacional destinado a la implementación de equipos informáticos periciales, adquisición de software y licencias de programas destinados para la realización de pericias digitales, así como se incremente el número de peritos digitales y se descentralice la realización de dichas pericias, a fin que se realicen con una mejor eficacia y de manera más celeridad.

Segundo.- que el procedimiento para la obtención de la prueba digital en los delitos informáticos a través de la identificación, recolección, obtención conservación y análisis de la prueba digital, sea implementado en un Protocolo Interinstitucional aplicable a los operadores de justicia como son el Ministerio Público y la Policía Nacional del Perú a fin de unificar criterios, procedimientos, que pueda contener no solo el tratamiento y obtención de la prueba digital contenida en soporte físico como son laptops, Smartphone, ordenadores, etc., sino también la que proviene del entorno digital como es el caso de aquella información almacenada en correos electrónicos, redes sociales (whatsapp, Facebook, Instagram, TikTok etc), así como la Búsqueda en Fuentes Abiertas – OSINT, y demás que tengan naturaleza de procedencia digital.

Tercero.- Como parte del Protocolo Interinstitucional a implementarse para la obtención de la prueba digital, se precise que dicho procedimiento se efectúe acompañado de personal especializado en su manipulación, debidamente provistos con el equipo pericial pertinente, como son el UFED y código HASH, para lo cual se implemente al Ministerio Público y Policía Nacional del Perú de una Oficina de Coordinación de diligencias externas, donde se cuente con peritos suficientes que pueda participar de manera inmediata en la realización de dichas pericias en detenciones en flagrancia, donde recabar dichas pruebas resultan trascendentales.

Cuarto.- Que el Protocolo a implementarse constituya el inicio de un nuevo marco normativo donde se dé un mayor y especializado tratamiento a la evidencia digital, implementándose en las instituciones que conocen las investigaciones donde se actúen evidencia digital, una sub especialidad dedicada a los Delitos Informáticos

como es que se continúen con la creación de Fiscalías Especializadas en Ciberdelincuencia a nivel nacional, y su vez se cree Juzgados que tengan la misma especialidad.

REFERENCIAS

REFERENCIAS BIBLIOGRÁFICAS

- Bujosa, L., Bustamante, M. y Toro, L. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración. *Rev. Bras. de Direito Processual Penal*. 7 (2), 1 – 38.
- Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St Martin's Press.
- Ley de delitos informáticos. (21 de octubre de 2013). *Ley N° 30096*.
- Ley modificatoria de delitos informáticos. (17 de febrero de 2014). *Ley 30171*.
- UNODC (2022). Ciberdelito II. Guía práctica para un abordaje integral del fenómeno, 18.
- Robles, M. (2020). *Capítulo 2: los delitos informáticos en la Ley N° 30096. Delitos informáticos y por medios electrónicos en el derecho penal peruano*, 13.
- Vera, M. (2020). La necesidad de distinguir criterios en la utilización de la prueba trasladada en el proceso penal lo foráneo como propio. *Gaceta penal & procesal penal*, N° 135, ISSN: 2075-6305

REFERENCIAS ELECTRÓNICAS

- Acosta, M., Benavides, M., & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 25(89), 351-368. ISSN: 1315-9984. <https://www.redalyc.org/articulo.oa?id=29062641023>
- Acurio, S. (2016). *Delitos informáticos: generalidades*. [Tesis Doctoral, Universidad de Guadalajara]. Repositorio institucional. <http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599>
- Arias, J. (2020). *Técnicas e instrumentos de investigación científica*. <http://repositorio.concytec.gob.pe/handle/20.500.12390/2238>
- Bacigalupo, S., Bajo, M., Basso, G., Cancio, M., Díaz, J., Fakhouri, Y., ... & Rodríguez, D. (2019). Manual de Introducción al Derecho Penal. *Derecho Penal y Procesal Penal*. <https://bit.ly/3QY1B8n>

- Becker, S. y Viollier, P. (2020). A implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223. *Revista de derecho (Concepción)*, 88 (248), 1 – 35.
<https://bit.ly/3ae7xcU>
- Bélanger, P. (2017). Derechos humanos y el derecho penal en el ciberespacio. *Revista da Secretaria do Tribunal Permanente de Revisão*, 5(10), 274-286.
<https://dialnet.unirioja.es/servlet/articulo?codigo=6182258>
- Beltrán, J., Rojas, M., & Taruffo, M. (2018). *Teoría de la decisión. Tribunal Constitucional Plurinacional de Bolivia*.
<https://tcpbolivia.bo/tcp/sites/default/files/2019%20LIBRO.pdf>
- Bhattacharjee, A., & Shrivastava, U. (2018). The effects of ICT use and ICT Laws on corruption: A general deterrence theory perspective. *Government Information Quarterly*, 35(4), 703-712.
<https://doi.org/10.1016/j.giq.2018.07.006>
- Blanco, F. (2020). La ciencia de la decisión. *Revista UIS Ingenierías*, 19(2),193-197. ISSN: 1657-4583.
<https://www.redalyc.org/articulo.oa?id=553768132020>
- Blossiers, J. (2018). *El delito informático y su incidencia en la empresa bancaria* [Tesis de Maestría, Universidad Francisco Villareal]. Repositorio institucional. <https://bit.ly/3u0NEwg>
- Castro, L., & Rodríguez, M. (2018). Interacción Humano-Computadora y Aplicaciones en México.
http://amexcomp.mx/files/Libro-IHC_2019.pdf
- Cisneros, C., & Jiménez, R. (2021). El delito de estafa: naturaleza, elementos y consumación. *Dilemas contemporáneos: educación, política y valores*, 8(spe4). <https://doi.org/10.46377/dilemas.v8i.2794>
- Código Procesal Penal (29 de julio de 2004). *Decreto Legislativo N° 957. Artículo 185: Clases de documentos*.
http://www.oas.org/juridico/pdfs/mesicic4_per_cod_procesal.pdf
- Devia, E. (2017). *Delito informático: Estafa informática del artículo 248.2 del Código Penal* [Tesis Doctoral, Universidad de Sevilla]. Repositorio institucional.
<https://hdl.handle.net/11441/75625>
- Flores, M. (2016). La globalización como fenómeno político, económico y social. *Orbis. Revista Científica Ciencias Humanas*, 12(34),26-41. ISSN: 1856-1594. <https://www.redalyc.org/articulo.oa?id=70946593002>

- Galvis, A. y Bustamante, M. (2019). La no equivalencia funcional entre la prueba electrónica y la prueba documental: Una lectura desde la regulación procesal colombiana. *Ius et praxis*, 25 (2), 1 – 12.
<https://bit.ly/3bN5OLT>
- Gómez, Á. (2021). Aspectos procesales de los delitos informáticos y tecnológicos. [Tesis Doctoral, Universidad Rey Juan Carlos]. Repositorio institucional.
<https://bit.ly/3l7rwpS>
- Gooding, P. (2019). Mapping the rise of digital mental health technologies: Emerging issues for law and society. *International journal of law and psychiatry*, 67, 101498. <https://doi.org/10.1016/j.fsidi.2022.301350>
- Hernández, D. (2019). *La suplantación de identidad cibernética en el Ecuador* [Tesis de Maestría, Universidad Externado de Colombia]. Repositorio institucional. <https://bdigital.uexternado.edu.co/handle/001/1822>
- Izquierdo, F. (2021). La eficacia en las investigaciones fiscales de la ciberdelincuencia económica en tiempos de pandemia. [Tesis de Maestría, Universidad Nacional de Trujillo]. Repositorio institucional.
<https://dspace.unitru.edu.pe/handle/UNITRU/17845>
- Leyva, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris et Investigatio*, (1), 29-47.
DOI: <https://doi.org/10.15381/lucerna.v0i1.18373>
- López, P., & Fachelli, S. (2015). *Metodología de la investigación social*.
<https://ddd.uab.cat/record/129382>
- López, R., Avello, R., Palmero, D., Sánchez, S., & Quintana, M. (2019). Validación de instrumentos como garantía de la credibilidad en las investigaciones científicas. *Revista Cubana de Medicina Militar*, 48 (1),
<https://bit.ly/3QYtayl>
- Madalengoitia, A. (2019). *Fundamentos jurídicos para regular el acceso y el control de la praxis arbitral en contrataciones con el estado en el Perú*. [Tesis profesional, UPAGU]. Repositorio institucional.
<http://repositorio.upagu.edu.pe/handle/UPAGU/1254>
- Martínez, A. (2019). *La prueba digital en la automatización de los procesos jurisdiccionales*. UNAM, México.
<https://archivos.juridicas.unam.mx/www/bjv/libros/9/4250/30.pdf>.
- Mendoza, F. (20 marzo, 2019). *Aproximaciones a la prueba digital*. pderecho
<https://bit.ly/3y8XmxX>

- Mori, F. (2019). *Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de lima, periodo 2008 al 2012* [Tesis de Maestría, Universidad Francisco Villareal]. Repositorio institucional. <http://repositorio.unfv.edu.pe/handle/UNFV/3519>
- Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, 33. <https://doi.org/10.1016/j.fsidi.2020.200908>
- Ochoa, A. (2021). *Desafíos globales del cibercrimen: caso Ecuador período 2014–2019*. [Tesis de Maestría, Universidad Andina Simón Bolívar]. Repositorio institucional. <http://hdl.handle.net/10644/7919>
- Ospina, M., & Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: análisis para Colombia. *Revista Criminalidad*, 62(2), 199-217. <https://bit.ly/3bsDf6g>
- Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*. [Tesis de Maestría, Universidad Cesar Vallejo]. Repositorio institucional. <https://repositorio.ucv.edu.pe/handle/20.500.12692/20372>
- Pastor, E. (2020). *Modelo de gestión del análisis forense de hechos delictivos informáticos en el marco del sistema de justicia peruano*. [Tesis Doctoral, Universidad Francisco Villareal]. Repositorio institucional. <http://repositorio.unfv.edu.pe/handle/UNFV/4346>
- Rivero (2017). A propósito de la teoría del delito: ¿es aún necesaria en el sistema acusatorio mexicano? *Revista In Jure Anáhuac Mayab*, 5(10), 75-107. http://anahuacmayab.mx/injure/wp-content/uploads/2018/04/3_teor%C3%ADa_delito.pdf
- Rodríguez, E. (2013). América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?. <https://econ.uchile.cl/uploads/publicacion/9ba7739a0ac26598402dab53c990c58e49fc259a.pdf>
- Salgado, C. (2021). ¿Qué es lo que realmente nos importa de la corrupción? Una inmersión en nuestra mente cultural. <https://bdigital.uexternado.edu.co/handle/001/4424>
- Suárez, J. (2022). Vigencia de la ciberseguridad en el marco de la seguridad informática chilena. Convenio de Budapest. *Aula Virtual*, 3(6), 132-148. <http://aulavirtual.web.ve/revista/ojs/index.php/aulavirtual/article/view/121>

- Tomsett, R., Preece, A., Braines, D., Cerutti, F., Chakraborty, S., Srivastava, M., ... & Kaplan, L. (2020). Rapid trust calibration through interpretable and uncertainty-aware AI. *Patterns*, 1(4), <https://doi.org/10.1016/j.patter.2020.100049>
- Vadell, M., Rúa, M., & Garzón, O. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, 7(2), 1347-1384. <https://bit.ly/3a6mlKh>
- Valarezo, E., Valarezo, R., & Durán, A. (2019). Algunas consideraciones sobre la tipicidad en la teoría del delito. *Revista Universidad y Sociedad*, 11(1), 331-338. <https://bit.ly/3bDT6PC>
- Vargas, J. (2019). *El delito de estafa y la mínima intervención penal* [Tesis de Maestría, Universidad Técnica de Ambato]. Repositorio institucional. <https://bit.ly/3nuy3Bq>
- Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius Et Praxis*, (053), 95-110. <https://doi.org/10.26439/iusetpraxis2021.n053.4995>
- Zavrsnik A. (2021). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*, 18(5): 623-642. DOI:[10.1177/1477370819876762](https://doi.org/10.1177/1477370819876762)

ANEXOS

ANEXO 1

TABLA DE CATEGORIZACIÓN

| PROBLEMAS | OBJETIVOS | CATEGORIA | SUBCATEGORIA | CÓDIGOS |
|--|--|--------------------|---|---------------------|
| PROBLEMA GENERAL | | | | |
| ¿Cuáles son los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021? | Identificar los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021. | Prueba Digital | - Procedimientos. - Actuación probatoria en juicio. | PJ/CSJLN MP/DFLN |
| PROBLEMAS ESPECÍFICOS | | | | |
| OBJETIVOS ESPECÍFICOS | | | | |
| 1.- ¿Cuáles son los procedimientos para la obtención a nivel preliminar de la prueba digital en los delitos informáticos en Lima Norte en el año 2021? | 1.- Determinar los procedimientos para la obtención a nivel preliminar de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. | Delito Informático | - Mecanismos e instrumentos nacionales. - Cooperación internacional. | PJ/CSJLN MP/DFLN |
| 2.- ¿Cuáles son los problemas de la actuación probatoria en juicio de la prueba digital en los delitos informáticos en Lima Norte en el año 2021? | 2.- Determinar y establecer los problemas de la actuación probatoria en juicio de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. | | | |
| 3.- ¿Cuáles son los mecanismos y los instrumentos nacionales y de cooperación internacional para la obtención de la prueba digital en los delitos informáticos en Lima Norte en el año 2021? | 3.- Identificar y establecer los mecanismos y los instrumentos nacionales y de cooperación internacional para la obtención de la prueba digital en los delitos informáticos en Lima Norte en el año 2021 | | | |

ANEXO 2:

CATEGORÍA, SUBCATEGORÍAS Y MATRIZ DE CATEGORIZACIÓN.

| Categorías | Definición Conceptual | Subcategorías | Definición Conceptual |
|---------------------------|---|--|--|
| Prueba digital | Es aquella evidencia cuya técnica de obtención fue a través de dispositivos tecnológicos, por ende, se presenta bajo el formato de imágenes, videos o audios, los cuales, por su naturaleza, se hayan almacenados en equipos, teléfonos móviles u otros similares, sin que ello impida, y que su incorporación y actuación probatoria en juicio, debe efectuarse acorde a las reglas de juicio, debiendo ser valorado como prueba documental conforme al artículo 185º del Código Procesal Penal (Mendoza, 2022). | -Procedimientos. - Actuación probatoria en juicio. | Conforme a Vadell et al. (2021) es el cumplimiento normalizado de exigencias técnicas y legales para garantizar la integridad de prueba digital. Según Vera (2020), este proceso se rige por, la defensa procesal en su faz instrumental de derecho a probar y controlar la prueba, donde cada parte cuenta con la oportunidad de plantear los medios de prueba pertinentes a su tesis litigiosa, y que estos medios sean adecuadamente admitidos según criterios de razonabilidad intrínseca y extrínseca, y, que se otorguen garantías para una efectiva intervención de partes durante su juicio |
| Delito informático | Son todos aquellos actos ilícitos perpetrados a través del uso inapropiado de la tecnología, donde se logra vulnerar la privacidad y confidencialidad de datos e información de un tercero, ya sea personal, económica o laboral, con el fin de dañarlos o extraerlos infringiendo la ley (Acosta et al. 2020) En el Convenio de Budapest (2001) se señala cuáles son los mecanismos e instrumentos nacionales y de cooperación internacional, tanto para la investigación preliminar como judicial. | -Mecanismos e instrumentos nacionales. - Cooperación internacional. | Tenemos como principal referente a la Ley N° 30096- Ley de Delitos Informáticos, principal instrumento legal contra los ciberdelitos en el Perú. Su finalidad es sancionar las conductas ilícitas que vulneran los sistemas y datos informáticos, así como, otros bienes jurídicos de relevancia penal, mediante la utilización de tecnologías de la información o de la comunicación. Siendo el Convenio de Budapest el principal instrumento legal a nivel internacional en la lucha contra los delitos informáticos, el cual entró en vigor el 1° de julio de 2004 y respecto al Perú, se estableció su entrada en el 01 de diciembre del 2019 (Becker, 2020). |

ANEXO 3

Matriz de Categorización

La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

| Categorías | Subcategorías | Indicadores | Ítems |
|-----------------------|---------------------------------|----------------------------------|---|
| PRUEBA DIGITAL | Procedimientos. | Investigación a nivel preliminar | 1. ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? 2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? |
| | | Cadena de custodia | 3. ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? 4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? |
| | | Reglamento y/o directiva | 5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? |
| | Actuación probatoria en juicio. | Medios de defensa | 6. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? |
| | | Casos judicializados | 7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? |

| | | | |
|-------------------------------|--------------------------------------|--|---|
| DELITO INFORMÁTICO | Mecanismos e instrumentos nacionales | Normas nacionales | 8. ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. 9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? |
| | | Cuestionamientos de prueba digital en juicio | 10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? 11. ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? 12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué? |
| | Cooperación internacional | Instrumentos internacionales | 13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? 14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? |

ANEXO 4

Matriz de Categorización Interna

| Título: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021 Autor: Gustavo Adolfo Silva Huaman. | | | | |
|---|---|--------------------------------|----------------------------------|---|
| Problema | Objetivos | Categorías e Indicadores. | | |
| Problema General | Objetivo General | Categoría: Prueba Digital | | |
| ¿Cuáles son los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021? | Identificar los desafíos que enfrentan los operadores de justicia para la obtención de la prueba digital en los delitos informáticos en el Distrito Fiscal de Lima Norte en el año 2021. | Subcategoría | Indicadores | Items |
| | | Procedimientos | Investigación a nivel preliminar | P1 ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? P2 ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? |
| | | | Cadena de custodia | P3 ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? P4 ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? |
| Reglamento y/o directiva | P5 ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | | | |
| Problemas específicos 1.- ¿Cuáles son los procedimientos para la obtención a nivel preliminar de la prueba digital en los delitos informáticos en Lima Norte en el año 2021? 2.- ¿Cuáles son los problemas de la actuación probatoria en juicio de la prueba digital en los delitos informáticos en Lima Norte en el año 2021? 3.- ¿Cuáles son los mecanismos y los instrumentos nacionales y de cooperación internacional para la obtención de la prueba digital en los delitos informáticos en Lima Norte en el año 2021? | Objetivos específicos 1.- Determinar los procedimientos para la obtención a nivel preliminar de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. 2.- Determinar y establecer los problemas de la actuación probatoria en juicio de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. 3.- Identificar y establecer los mecanismos y los instrumentos nacionales y de cooperación internacional para la obtención de la prueba digital en los delitos informáticos en Lima Norte en el año 2021. | Actuación probatoria en juicio | Medios de Defensa | P6 ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? |
| | | | Casos judicializados | P7 ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? |

| Tipo y diseño de investigación | Participantes | Categoría: Delitos informáticos | | |
|--|--|--------------------------------------|--|---|
| | | Subcategoría | Indicadores | Items |
| Tipo: Investigación básica. | Cuatro (04) Fiscales Penales. Tres (03) Jueces Penales. | Mecanismos e instrumentos nacionales | Normas nacionales | P8 ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. P9 ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? |
| Diseño: Teoría fundamentada. | Técnicas e instrumentos | | Cuestionamientos de prueba digital en juicio | P10 ¿Cuáles con los cuestionamientos más recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? P11 ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? P12 ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué? |
| | Técnica: Entrevista. Instrumento: Guía de entrevista. | Cooperación Internacional | Instrumentos internacionales | P13 ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? P14 ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? |
| <p>Autor: Gustavo Adolfo Silva Huaman Monitoreo: La Guía de Entrevista fue aplicada a especialistas en la materia Ámbito de Aplicación: Jueces y Fiscales del Distrito Fiscal de Lima Norte</p> | | | | |

ANEXO 5



ESCUELA DE POSGRADO

GUÍA DE ENTREVISTA DIRIGIDA A FISCALES PENALES

TÍTULO: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

Entrevistado (a) :.....

Edad:..... años

Sexo:.....

Fecha:

CATEGORÍA 1: LA PRUEBA DIGITAL

1. ¿Considera usted que son necesarios la prueba digital durante la investigación preliminar en los delitos informáticos? ¿Por qué?
2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos?
3. ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?
4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital?
5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?
6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?
7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta ha sido materia de debate o cuestionamiento? ¿Por qué?

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.

9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?
10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?
11. ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?
12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?
13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?
14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

FIRMA

GUÍA DE ENTREVISTA DIRIGIDA A JUECES PENALES

TÍTULO: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

Entrevistado (a) :.....

Edad:..... años

Sexo:.....

Fecha:

CATEGORÍA 1: LA PRUEBA DIGITAL

1. ¿Considera usted que son necesarios la prueba digital durante la investigación preliminar en los delitos informáticos? ¿Por qué?
2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos?
3. ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?? ¿Por qué?
4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital?
5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?
6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?
7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué?

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.

9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?
10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?
11. ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?
12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?
13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?
14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

FIRMA

ANEXO 6

CERTIFICADO DE VALIDEZ DE CONTENIDO DE INSTRUMENTOS

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL, DIRIGIDA A FISCALES PENALES

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? | X | | X | | X | | | |
| 2 | ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? | X | | X | | X | | | |
| 3 | ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? | X | | X | | X | | | |
| 4 | ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? | X | | X | | X | | | |
| 5 | ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | X | | X | | X | | | |
| 6 | ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué? | X | | X | | X | | | |
| 7 | ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? | X | | X | | X | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL PARA FISCALES PENALES

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|------------------------------------|--------------------|---|
| Nombres y Apellidos | Elder Jaime Miranda Aburto | DNI N° | 07626166 |
| Dirección domiciliaria | Avenida Arenales 1823-Int. F-Lince | Teléfono / Celular | 999 748 026 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Doctor en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 25/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS DIRIGIDA A FISCALES PENALES.

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 8 | ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. | x | | x | | x | | | |
| 9 | ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? | x | | x | | x | | | |
| 10 | ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 11 | ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 12 | ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 13 | ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |
| 14 | ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS, DIRIGIDA A FISCALES PENALES.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|----------------------------|--------------------|---|
| Nombres y Apellidos | Elder Jaime Miranda Aburto | DNI N° | 07626166 |
| Dirección domiciliaria | | Teléfono / Celular | 999 748 026 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Doctor en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 25/07/2022 |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL, DIRIGIDA A JUECES PENALES

| Nº | Formulación del ítem | Pertinencia ^{a1} | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|---------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? | X | | X | | X | | | |
| 2 | ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? | X | | X | | X | | | |
| 3 | ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? | X | | X | | X | | | |
| 4 | ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? | X | | X | | X | | | |
| 5 | ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | X | | X | | X | | | |
| 6 | ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué? | X | | X | | X | | | |
| 7 | ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? | X | | X | | X | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL PARA JUECES PENALES

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|------------------------------------|--------------------|---|
| Nombres y Apellidos | Elder Jaime Miranda Aburto | DNI N° | 07626166 |
| Dirección domiciliaria | Avenida Arenales 1823-Int. F-Lince | Teléfono / Celular | 999 748 026 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Doctor en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 25/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS DIRIGIDA A JUECES PENALES.

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 8 | ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. | x | | x | | x | | | |
| 9 | ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? | x | | x | | x | | | |
| 10 | ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 11 | ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 12 | ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 13 | ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |
| 14 | ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS, DIRIGIDA A JUECES PENALES.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|----------------------------|--------------------|---|
| Nombres y Apellidos | Elder Jaime Miranda Aburto | DNI N° | 07626166 |
| Dirección domiciliaria | | Teléfono / Celular | 999 748 026 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Doctor en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 25/07/2022 |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

ANEXO 7

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL, DIRIGIDA A FISCALES PENALES

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? | X | | X | | X | | | |
| 2 | ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? | X | | X | | X | | | |
| 3 | ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? | X | | X | | X | | | |
| 4 | ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? | X | | X | | X | | | |
| 5 | ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | X | | X | | X | | | |
| 6 | ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué? | X | | X | | X | | | |
| 7 | ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? | X | | X | | X | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL PARA FISCALES PENALES

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|---|--------------------|--|
| Nombres y Apellidos | Fiorella Linares Perez | DNI N° | 42988692 |
| Dirección domiciliaria | Av. Cordialidad Mz. V V2 lote 14- La Floresta de Pro – Los Olivos | Teléfono / Celular | 993952121 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Magister en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 27/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

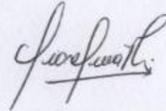
CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS DIRIGIDA A FISCALES PENALES.

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. | x | | x | | x | | | |
| 2 | ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? | x | | x | | x | | | |
| 3 | ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 4 | ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 5 | ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 6 | ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |
| 7 | ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS, DIRIGIDA A FISCALES PENALES.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|---|--------------------|---|
| Nombres y Apellidos | Fiorella Linares Perez | DNI N° | 42988692 |
| Dirección domiciliaria | Av. Cordialidad Mz. V V2 lote 14- La Floresta de Pro – Los Olivos | Teléfono / Celular | 993952121 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Magister en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 27/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

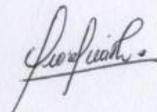
CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL, DIRIGIDA A JUECES PENALES

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? | X | | X | | X | | | |
| 2 | ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? | X | | X | | X | | | |
| 3 | ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? | X | | X | | X | | | |
| 4 | ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? | X | | X | | X | | | |
| 5 | ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | X | | X | | X | | | |
| 6 | ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué? | X | | X | | X | | | |
| 7 | ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? | X | | X | | X | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL DIRIGIDA A JUECES PENALES.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|---|--------------------|---|
| Nombres y Apellidos | Fiorella Linares Perez | DNI N° | 42988692 |
| Dirección domiciliaria | Av. Cordialidad Mz. V V2 lote 14- La Floresta de Pro – Los Olivos | Teléfono / Celular | 993952121 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Magister en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 27/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS DIRIGIDA A JUECES PENALES.

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos Explique. | x | | x | | x | | | |
| 2 | ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? | x | | x | | x | | | |
| 3 | ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 4 | ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 5 | ¿Considera usted que existe una problemática en la realización de peritaje en la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 6 | ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |
| 7 | ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS DIRIGIDA A JUECES PENALES.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|---|--|-------------|
| Nombres y Apellidos | Fiorella Linares Perez | DNI N° | 42988692 |
| Dirección domiciliaria | Av. Cordialidad Mz. V V2 lote 14- La Floresta de Pro – Los Olivos | Teléfono / Celular | 993952121 |
| Título profesional/ Especialidad | Abogado | Firma  | |
| Grado Académico | Magister en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 27/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría.

ANEXO 8

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL, DIRIGIDA A FISCALES PENALES

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? | X | | X | | X | | | |
| 2 | ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? | X | | X | | X | | | |
| 3 | ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? | X | | X | | X | | | |
| 4 | ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? | X | | X | | X | | | |
| 5 | ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | X | | X | | X | | | |
| 6 | ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué? | X | | X | | X | | | |
| 7 | ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? | X | | X | | X | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL PARA FISCALES PENALES

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|---|--------------------|---|
| Nombres y Apellidos | Jose Walter Lopez Fernandez | DNI N° | 45977880 |
| Dirección domiciliaria | Calle La Victoria N° 131 – San Martin de Porres | Teléfono / Celular | 966420481 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Magister en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 27/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

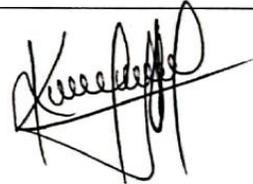
CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS DIRIGIDA A FISCALES PENALES.

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. | x | | x | | x | | | |
| 2 | ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? | x | | x | | x | | | |
| 3 | ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 4 | ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 5 | ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 6 | ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |
| 7 | ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS, DIRIGIDA A FISCALES PENALES.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable [/]

| | | | |
|----------------------------------|---|--------------------|---|
| Nombres y Apellidos | Jose Walter Lopez Fernandez | DNI N° | 45977880 |
| Dirección domiciliaria | Calle La Victoria N° 131 – San Martin de Porres | Teléfono / Celular | 966420481 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Magister en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 27/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL, DIRIGIDA A JUECES PENALES

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? | X | | X | | X | | | |
| 2 | ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? | X | | X | | X | | | |
| 3 | ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? | X | | X | | X | | | |
| 4 | ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? | X | | X | | X | | | |
| 5 | ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | X | | X | | X | | | |
| 6 | ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué? | X | | X | | X | | | |
| 7 | ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? | X | | X | | X | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE PRUEBA DIGITAL DIRIGIDA A JUECES PENALES.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|---|--------------------|--|
| Nombres y Apellidos | Jose Walter Lopez Fernandez | DNI N° | 45977880 |
| Dirección domiciliaria | Calle La Victoria N° 131 – San Martin de Porres | Teléfono / Celular | 966420481 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Magister en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 27/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS DIRIGIDA A JUECES PENALES.

| Nº | Formulación del ítem | Pertinencia ¹ | | Relevancia ² | | Claridad ³ | | Observaciones | Sugerencias |
|----|---|--------------------------|----|-------------------------|----|-----------------------|----|---------------|-------------|
| | | Si | No | Si | No | Si | No | | |
| 1 | ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. | x | | x | | x | | | |
| 2 | ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? | x | | x | | x | | | |
| 3 | ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 4 | ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 5 | ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué? | x | | x | | x | | | |
| 6 | ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |
| 7 | ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | x | | x | | x | | | |

OPINIÓN DE APLICABILIDAD DE LA GUÍA DE ENTREVISTA SEMIESTRUCTURADA SOBRE DELITOS INFORMÁTICOS DIRIGIDA A JUECES PENALES.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

| | | | |
|----------------------------------|---|--------------------|---|
| Nombres y Apellidos | Jose Walter Lopez Fernandez | DNI N° | 45977880 |
| Dirección domiciliaria | Calle La Victoria N° 131 – San Martin de Porres | Teléfono / Celular | 966420481 |
| Título profesional/ Especialidad | Abogado | Firma |  |
| Grado Académico | Magister en Derecho | | |
| Metodólogo/ temático | Temático | Lugar y fecha | 27/07/2022. |

¹ **Pertinencia:** El ítem corresponde al concepto teórico formulado.

² **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

³ **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para evaluar la categoría.

ANEXO 9

MATRIZ DE TRIANGULACIÓN FISCALES PENALES

| Preguntas | Fiscal 1 Erika Beatriz Huacachi Zanzi | Fiscal 2 Guillermo Rogelio Dominguez Romero | Fiscal 3 Samuel Eli Ladron de Guevara | Fiscal 4 Gladys Eulalia Amable Basilio | Conceptos Identificados | Categorías o conceptos emergentes | Semejanzas | Diferencias | Interpretación |
|--|---|--|---|---|--|---|---|---|---|
| 1 ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? | Si, para la búsqueda o corroboración de información | Si son necesarios, porque los delitos informáticos requieren de fuentes tanto tecnológicos que servirán para determinar la comisión o vinculación de un hecho delictivo para acreditarlos | Si, porque permiten probar la hipótesis fiscal. Asimismo porque corresponde a la naturaleza del delito mencionado. | Sí, porque permite tener los elementos de juicio a nivel de sospecha reveladora del delito que se investiga. | Búsqueda o corroboración Fuentes Probanza Elementos de juicio | La probanza en la investigación | Tres entrevistados coinciden en la necesidad de la prueba digital para sustentar la tesis de la investigación | Un participante señala que la prueba digital es necesario en la búsqueda o corroboración de información | La prueba digital resulta necesario a fin de probar la tesis fiscal en juicio, la misma que es relevante desde la investigación |
| 2 ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? | 1) El ya no contar con los soportes donde se encontraría la prueba, 2) Falta de cuidado en guardar adecuadamente la información, Falta de software para obtención acceso a la información digital | Las pruebas digitales tienen la posibilidad de ser manipuladas, pudiéndose alterar su soporte digital, otras es la obtención de la misma, ya que las pruebas digitales son ofrecidas sin previa verificación, pudiendo quitarle garantía a su carga probatoria estimado por el perito informático, cuando su validez sea cuestionada | En primer lugar su carácter novísimo en la actualidad, lo que deriva que tengamos operadores (policías, fiscales y jurisdiccionales) con poca preparación y escasa experticia | No existe una cultura de aseguramiento de la escena del delito en caso de prueba digital, es decir, no se protege ni delimita la escena para evitar la modificación o destrucción de las evidencias digitales, más aún, si muchos, desconocen sobre evidencia digitales que pueden ser útiles para la investigación. Asimismo, no se sigue un procedimiento de obtención de información desde su fuente, restando de esta manera autenticidad e integridad a la información obtenida. | Volatilidad de la prueba digital Inadecuado manejo de aseguramiento de prueba Novísimo | Volatilidad y errores en la recolección de prueba digital | Tres participantes indican el carácter volátil y frágil de la prueba digital, así como los errores al recolectarlos | Un participante indica el carácter novísimo de la obtención de la prueba digital | La recolección de la prueba digital presenta diversos problemas que dificultan su preservación |

| | | | | | | | | | |
|---|--|---|---|---|--|--|--|--|--|
| 3. ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? | Los formatos para los soportes físicos son los mismos en descripción de las características del soporte mas no de algún registro o codificación o autenticidad de su contenido al momento de su obtención. | Si, porque la cadena de custodia digital debe garantizar la fiabilidad de la prueba digital con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba, por lo que dentro del procedimiento de prueba pericial informática tecnológica resulta adecuado garantizar su autenticidad | Si, porque por su propia naturaleza son distintos. No es lo mismo un objeto material físico, como la evidencia digital que si bien se soporta en un medio magnético, no obstante requiere otro tratamiento. | No, ya que la información obtenida se debe de asegurar mediante medios físicos | Soporte físico Cadena de custodia digital Evidencia digital | cadena de custodia en evidencia Digital | Dos participantes indican que si existe diferencia en la cadena de custodia de la prueba digital de los delitos informáticos en relación con otros delitos | Dos participantes indican que no existe diferencia en la cadena de custodia de la prueba digital de los delitos informáticos en relación con otros delitos | La cadena de custodia de la prueba digital de delitos informáticos es la misma en relación a otros delitos, pero solo respecto del formato con el cual se levanta el soporte físico, sin embargo existe otra cadena de custodia a través de software o programas que se practican en la evidencia digital a fin de asegurar su inalterabilidad, preservación y fiabilidad. |
| 4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? | Ninguno | Considero que debería cumplirse las formas del debido proceso y adecuar las medidas a cada caso, así como su vigencia, y las razones por las que perdería efecto. | He tenido oportunidad de ver en los informes periciales el uso del "Centro premium celebre". Asimismo he oído del código HASH | La cadena de custodia. | Debido proceso Programa "Centro premium celebre" Código Hash Cadena de custodia | Programas de aplicación para pruebas digitales | Dos participantes hacen referencia a las medidas convencionales de preservación de la prueba | Un participante precisa programas de recolección o preservación aplicable solo a la evidencia digital | La evidencia digital además de los mecanismos convencionales de aseguramiento y protección, hace uso de herramientas tecnológicas tanto para su recolección, extracción, preservación y traslado de la misma |
| 5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | No. | La Ley 30096 – Ley de Delitos Informáticos. Manual para el recojo de evidencia digital | Tengo conocimiento del Manual para el recojo de la evidencia digital aprobado por Resolución Ministerial N° 848-2019-IN, la Resolución N° 729-2016-MP-FN y la Directiva N° | NCPP y el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados (Aprobado por Resolución n° 729-2006-MP-FN del 15 de junio del 2006). | Ley 30096 Manual para el recojo de evidencia digital Directiva N° 03-19-2015- DIRGEN- PNP/EMG- PNP Convenio de Budapest Reglamento de la | Normatividad para recojo y preservación de evidencia digital | Dos participantes coinciden en señalar la existencia del Manual para el recojo de evidencia digital, y hacen referencia a otras dos normas relacionadas | Un participante indica el Reglamento de la Cadena de Custodia | El Manual para el recojo de evidencia digital es un documento expedido por el Ministerio del Interior y esta referido básicamente a la recolección y preservación del soporte físico de la evidencia digital |

| | | | | | | | | | |
|---|---|---|--|--|---|---|--|---|---|
| | | | 03-19-2015- DIRGEN- PNP/EMG- PNP y el Convenio de Budapest | | Cadena de Custodia | | con evidencia digital | | |
| 6 ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué? | La duda de posible adulterabilidad o que evita la probabilidad de haber sido alterado la prueba mediante supresión o adición de información, revisar el contenido de información en el acta de cadena de custodia | La cadena de custodia y prueba digital. La extracción de la prueba digital (HASH) | Considero que una tutela de derechos, porque permitiría excluir prueba digital obtenida de manera ilegal o manipulada de tal manera que no garantice fiabilidad | Tutela de Derechos, inadmisibilidad de ofrecimiento de pruebas. | Duda del medio de prueba. Cuestionamiento de la recolección y custodia de la prueba digital, Tutela de Derechos Inadmisibilidad de ofrecimiento de prueba | Vulneración de la cadena de custodia y recolección Mecanismos procesales de Defensa | Dos entrevistados señalan la Tutela de Derechos como mecanismos para la exclusión de la prueba digital | Un participante hace alusión a la duda en la obtención de la prueba, otro participante se refiere al cuestionamiento de la cadena de custodia, y otro participante agrega inadmisibilidad de ofrecimiento de pruebas. | Como mecanismo procesal tenemos en primer orden la Tutela de Derechos a fin de cuestionar durante la investigación la prueba digital, sin embargo también se puede solicitar la exclusión de dicha prueba mediante tachas o la inadmisibilidad en la etapa intermedia |
| 7 ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta ha sido materia de debate o cuestionamiento? ¿Por qué? | Ninguno | Casos judicializados, aún ninguno | Si bien me encuentro participando en procesos penales en los cuales existen prueba digital, no obstante aún no ha transitado a la etapa de juicio oral, tampoco se ha cuestionado su mérito aún. | En uno, en el cual se cuestionó las capturas de conversaciones mediante el aplicativo WhatsApp toda vez que en la recolección de dicha información no se realizó desde el celular o aparato en el cual obraba la misma, solo se tenía las capturas presentadas por la parte denunciante. El abogado defensor del imputado indicaba que no se tenía certeza si esa información era auténtica por cuanto eran capturas que | Capturas de conversaciones de WhatsApp Fiabilidad de la información de la evidencia digital | Fiabilidad, preservación y alteración de la evidencia digital | Tres entrevistados indican que aún no han tenido experiencia de casos judicializados donde se actúe prueba digital | Un entrevistado señala el cuestionamiento efectuado a una captura de conversación WhatsApp dado que no se recabó dicho medio de prueba de su fuente original | Solo un entrevistado indico su experiencia en juicio con evidencia digital |

| | | | | | | | | | |
|---|--|---|---|---|---|--|---|--|---|
| | | | | podrían haber sido manipuladas, teniendo en cuenta la tecnología. | | | | | |
| 8 ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. | Requerimiento físico de quien tiene el soporte de la información conteniendo la prueba, su visualización de ser el caso y si se tiene que realizar una pericia con personal idóneo (perito) dicho soporte debe ser sometido para su examen | Que la prueba digital se encuentre en lugar correcto, efectuar la cadena de custodia y proteger la evidencia. | En caso el primer interviniente no sea especializado dependerá de si se trata de dispositivos transportables o no transportables, en cuyo caso se deberá dar el trato de evidencia digital, y su correspondiente e custodia | Son copia imagen, video, Análisis digital forense, etc. | Visualización y examen Cadena de custodia Copia imagen y análisis forense | Prácticas de aseguramiento de la cadena de custodia y análisis forense | Tres entrevistados señalaron como punto de partida el aseguramiento de la prueba digital, cadena de custodia para luego ser sometido al examen de análisis forense | Un entrevistado indicó como primer procedimiento la copia imagen de la evidencia digital. | Debe tenerse presente que en la mayoría de casos se recabara el soporte que contiene la prueba digital para luego ser examinado y reproducido; sin embargo, también existen casos, donde es imposible transportar la fuente de la prueba digital, o por la inmediatez se practicará las primeras diligencias en el lugar de los hechos donde, esto es una búsqueda rápida o copia imagen. |
| 9 ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? | No, aun existe poca regulación e información sobre el tema | Considero que la normatividad explícita es suficiente, lo que debe cambiar es el mejoramiento de los equipos periciales para hacer mas dinámico y factible la recopilación de pruebas | No, recién la realidad está generando casuística que sobrepasa el marco normativo actual, por lo que no sería suficiente para un adecuado trato legal, por ende puede ser cuestionada | No, porque dada la naturaleza de la prueba en estos delitos, se requiere procedimiento distinto a los otros medios de prueba para asegurar la mismidad de la misma. | Escasez de regulación e información de Mejoramiento o de equipos periciales | Escasez de regulación e información de normas para recolección de prueba digital | Tres entrevistados indicaron que es insuficiente la normatividad actual para asegurar la que la recolección y obtención de la prueba digital no sea cuestionada en juicio | Un entrevistado indicó que la normatividad actual es suficiente, pero es necesario el mejoramiento de equipos periciales | Existe pocas normas que regulan la obtención y recolección de la prueba digital de manera especializada o específica |

| | | | | | | | | | |
|--|--|---|---|--|--|--|---|--|--|
| <p>10. ¿Cuáles con los cuestionamientos más recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?</p> | <p>No he participado en juicio por ese tipo de delito</p> | <p>La fecha de la obtención de la prueba digital y la fecha con que se realizó la pericia respectiva, toda vez que se trata de desacreditar y reducir su valor probatorio</p> | <p>Si bien no he participado, considero que podría ser su originalidad, adecuada manipulación y correcto embalaje.</p> | <p>El procedimiento de recojo de evidencias, por ejemplo, en el caso de los mensajes WhatsApp, fotos, etc, contenidas en el celular, el procedimiento correcto sería que deben ser recopilados del mismo aparato celular mediante visualización de dicho aparato, redactándose el acta correspondiente con la información pertinente, sin embargo muchas veces lo que se actúa en juicio son las capturas de mensaje o las fotografías presentadas a por una de las partes, por lo que el abogado cuestiona la autenticidad de dichas capturas, al no haberse seguido un procedimiento que garantice la mismidad de la información actuada en juicio oral.</p> | <p>Data de recolección y actuación de la prueba digital Conservación de la prueba digital Originalidad</p> | <p>Data de recolección y actuación de prueba digital</p> | <p>Tres entrevistados coinciden al señalar que los cuestionamientos más recurrentes son la fecha de recolección, así como de la actuación de la prueba digital, y la conservación del mismo</p> | <p>Un entrevistado indico que también es cuestionable la originalidad de la prueba digital</p> | <p>Resulta importante efectuar una adecuada recolección, conservación y actuación de la prueba digital a fin de evitar cuestionamientos en juicio</p> |
| <p>11. ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?</p> | <p>No he tenido alguno en investigación por ese tipo de delito</p> | <p>Se cuestiona: la forma como se obtuvo la misma, con el fin de desacreditar la misma. La manipulación que tuvo la misma, para restarle nivel probatorio. La legalidad de la misma</p> | <p>La correcta manipulación de los dispositivos informáticos. Porque si no se procede de manera correcta y especializada se afecta la</p> | <p>Los cuestionamientos más recurrentes son: No se sigue un procedimiento que garantice la autenticidad de la información que se va actuar en juicio oral.</p> | <p>Obtención y manipulación de prueba digital Procedimiento que garantice fiabilidad y autenticidad</p> | <p>Procedimiento de obtención de prueba digital que garantice su fiabilidad y autenticidad</p> | <p>Dos entrevistados indican como cuestionamientos más recurrente la obtención y manipulación de la prueba digital</p> | <p>Un entrevistado se refirió al procedimiento que garantice a autenticidad de la prueba digital</p> | <p>Los cuestionamientos a la prueba digital radican en su obtención y manipulación, por lo que se debe garantizar la fiabilidad y autenticidad de la misma</p> |

| | | | | | | | | | |
|---|---|--|---|--|---|---|---|--|---|
| | | | fiabilidad de la prueba digital | | | | | | |
| 12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué? | Si, falta de obtención de programas, licencias de software para la obtención de información o pericias. | La problemática en el sentido de la demora del mismo, por parte de los peritos informáticos y la deficiencia de equipos tecnológicos para el resultado del mismo y en otros falta de personal idóneo | Si, porque existe escasez de peritos, lo que deriva en que las pericias tarden, y con ello la posibilidad de realizar otros actos de investigación derivados del mismo | No se cuenta con muchos peritos forenses. Además, los peritos del IML tienen competencia a nivel nacional por lo que su carga es abundante, lo que dilata la emisión de sus informes, retardando las investigaciones. En igual sentido ocurre con los peritos de la Policía Nacional del Perú, pues está centralizado. | Ausencia de programas y licencia de software Demora y problemas logísticos de pericias | Problemas y carencia de logística en las pericias | Tres entrevistados coinciden al indicar que existe una deficiencia en los equipos tecnológicos, personal idóneo, y escaso número de peritos | Un entrevistado hace referencia señala falta de programas y software para las pericias | Dado que las pericias se realizan por los órganos de apoyo de los operadores de justicia, existe un escasa logística y actualización de los equipos para la realización de pericias |
| 13 ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | En forma genérica se tiene como base al NCPP | El manual para el recojo de la evidencia digital. Ley 29733 – Ley de Protección de datos personales | Considero que son los enumerados en la respuesta 5, Manual para el recojo de la evidencia digital aprobado por Resolución N° 848-2019-IN, la Resolución N° 729-2016-MP-FN y la Directiva N° 03-19-2015-DIRGEN-PNP/EMG-PNP | NCPP, Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados (Aprobado por Resolución N° 729-2006-MP-FN del 15 de junio del 2006), Acuerdos Plenarios N° 5-2010/CJ-116 y N° 6-2012/CJ-116, de la Corte Suprema de Justicia de la República | NCPP Manual para el recojo de la evidencia digital Ley de Protección de datos personales Reglamento de cadena de custodia Procedimiento para protección de escena del delito Acuerdos plenarios | Normas para recojo de evidencias en general | Dos entrevistados coinciden en señalar las normas del NCPP, así como el Manual para recojo de evidencia digital, y otros dos indican la Ley de Protección de datos personales | Un entrevistado hace referencia al Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados y otro entrevistado se refiere a acuerdos plenarios y al Procedimiento para protección de escena del delito | Las normas señaladas están referidas al recojo del soporte físico de evidencia |

| | | | | | | | | | |
|---|------------|--|---|---|---|--|---|---|---|
| 14 ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos? | Desconozco | El Convenio sobre la Ciberdelincuencia | El Convenio de Budapest o sobre Ciberdelincuencia y la Norma ISO/IEC27037 .2012 | Convención de Cibercriminalidad (Budapest, 2001), Protocolo del grupo de trabajo científico en evidencia digital (SWGDE) "Best Practices for Computer Forensics". | Convenio de Budapest Norma ISO/IEC27037.2012 Protocolo del grupo de trabajo científico en evidencia digital (SWGDE) | Convenio de Budapest o sobre Ciberdelincuencia | Tres entrevistados coinciden en señalar el Convenio de Budapest | Un entrevistado indica la Norma ISO/IEC27037 .2012, otro indica el Protocolo del grupo de trabajo científico en evidencia digital (SWGDE) | El Convenio de Budapest contiene los delitos informáticos susceptibles de persecución, sin embargo no está referida a la recolección de evidencia digital, que si contiene las otras normas señaladas por los entrevistados, pero son de carácter nacional. |
|---|------------|--|---|---|---|--|---|---|---|

ANEXO 10

MATRIZ DE TRIANGULACIÓN JUECES PENALES

| Preguntas | Juez 1 Valery Raul Romero Palacios | Juez 2 Luis Alberto Dejo Apaestegui | Juez 3 Enrique Palomino Gutierrez | Conceptos Identificados | Categorías o conceptos emergentes | Semejanzas | Diferencias | Interpretación |
|--|--|---|--|---|--|--|--|--|
| 1 ¿Considera usted que son necesarios la prueba digital durante la investigación en los delitos informáticos? ¿Por qué? | Si, toda vez que toda información obtenida o transmitida a través de un medio tecnológico electrónico o dispositivo digital va a coadyuvar con la estrategia de investigación fiscal | Considero que si, dado que la prueba digital es uno de los principales elementos que servirá para sustentar una posible formalización de la investigación o las medidas coercitivas que pueda requerir el Ministerio Público, sin la cual difícilmente tendrá futuro algún caso | Considero que la evidencia digital resulta relevante durante la investigación preliminar en los delitos informáticos, a fin de que la Fiscalía pueda sustentar una Formalización y continuación de Investigación Preparatoria y demás requerimientos | Estrategia de investigación Sustento de formalización de investigación Preparatoria | Estrategia de investigación | Los entrevistados coinciden en indicar que es importante la prueba digital durante la investigación en los delitos informáticos, precisando dos de ellos, que servirá para la Formalización de Investigación | Ninguna | La prueba digital resulta necesario a fin de probar la tesis fiscal en los delitos informáticos |
| 2 ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? | Considero que serían en principio cautelar en forma correcta la prueba digital (cadena de custodia); segundo, considero que su actuación y posterior valoración del mismo sistema de justicia es nuevo | Uno los problemas que tiene el Ministerio Público para la obtención de la prueba digital, es que es de difícil obtención, y sobre todo presentan problemas en su recolección y preservación, que es aprovechado por la defensa del imputado a fin de cuestionarla y pretender excluirlas de la investigación, de igual manera se cuestiona la forma como se actúan a nivel preliminar | En mi labor jurisdiccional, no podría precisar las dificultades que tiene la Fiscalía para la obtención de una prueba digital en la investigación preliminar en los delitos informáticos | Cadena de custodia Difícil obtención | Cuestionamientos a la cadena de custodia | Dos participantes señalan que los problemas se presentan al momento de la recolección | Un participante precisa que la problemática se presenta en la cadena de custodia, y otro participante indica que es en la recolección y también en la preservación y en su actuación | La obtención de la prueba digital requiere la debida diligencia en su recolección, preservación y actuación |
| 3. ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de | Considero que si, toda vez que la prueba digital va a necesitar diversos mecanismos | En líneas generales no existe diferencia, por cuanto la cadena de custodia es un elemento que garantiza que no se realice manipulación | Considero que debería existir, pues la obtención de una evidencia digital, resulta ser más compleja | Mecanismos de aseguramiento Cadena de custodia | Aseguramiento de evidencia digital | Dos entrevistados coinciden en señalar que si existe diferencia en la cadena | Un entrevistado indica que en sentido amplio no existe diferencia, dado que la cadena de | La cadena de custodia de la prueba digital de delitos informáticos es similar en relación a otros delitos, pero solo respecto del formato con el cual se |

| | | | | | | | | |
|---|---|---|---|--|--|--|--|---|
| la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué? | para asegurar la evidencia que se encuentre en un medio electrónico o dispositivo digital | externa del bien recogido. | | | | custodia para delitos informáticos en comparación de delitos comunes | custodia esta referida al elemento externo | levanta el soporte físico, sin embargo existe otra cadena de custodia a través de software o programas que se practican en la evidencia digital a fin de asegurar su inalterabilidad, preservación y fiabilidad. |
| 4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital? | El mecanismo será la cadena de custodia; pero aplicaciones o programas, desconozco | El mas conocido es la función HASH que es un algoritmo con el cual se crea una serie alfa numérica con lo cual se asegura y se verifica que la información digital no sea alterada, así como el software forense UFED mediante el cual se efectúa una búsqueda de determinada información necesaria para la investigación en dispositivos como el caso de equipos celulares | Uno de los programas que sirven para preservar la inalterabilidad de la prueba digital es la función HASH que verifica que la información digital no sea alterada | Cadena de custodia Función Hash Software UFED | Aseguramiento físico y digital de prueba digital | Dos entrevistados coinciden en señalar a la función Hash a fin de preservar la evidencia digital | Un entrevistado hace referencia a la cadena de custodia, otro entrevistado indica el software UFED | La evidencia digital además de los mecanismos convencionales de aseguramiento y protección, hace uso de herramientas tecnológicas tanto para su recolección, extracción, preservación y traslado de la misma |
| 5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos? | Solo sobre el D.L. N° 1412 y su reglamento | El Ministerio Público recientemente ha publicado una Guía práctica para requerir información a proveedores internacionales de internet, luego de ello, no existiría mas información dado que la investigación de dichos delitos es relativamente nueva. | Al ser un tema no muy desarrollado por ser nuevo solo tengo conocimiento que la Fiscalía Especializada ha publicado una Guía práctica para requerir información a proveedores internacionales de internet | D.L. N° 1412 – Ley de Gobierno Digital Guía práctica para requerir información a proveedores internacionales de internet | Guía práctica para requerir información a proveedores internacional es de internet | Dos entrevistados coinciden en señalar el conocimiento de la Guía práctica para requerir información a proveedores internacionales de internet | Un entrevistado hace mención al D.L. N° 1412 y su reglamento, norma que aprueba la Ley de Gobierno Digital | La Guía práctica para requerir información a proveedores internacionales de internet, está orientada a la solicitud de información a empresas ubicadas en el extranjero, no se invocó una norma para obtener prueba digital |
| 6. ¿Qué medios de defensa considera usted | Creo que se podría formular una Tutela de | Tachas contra un determinado medio de | Contra una prueba digital obtenido por el Ministerio Público en | Tutela de Derechos Nulidad | Mecanismos y medios que buscan | Dos entrevistados coinciden al | Un entrevistado señala que se podría | Como mecanismo procesales tenemos la Tutela de Derechos a fin de |

| | | | | | | | | |
|--|---|---|---|---|---|--|--|--|
| que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué? | Derechos o deducir Nulidad; toda vez que se debe respetar la cadena de custodia; y la obtención de la prueba digital no debe afectar derechos fundamentales | prueba, a fin de solicitar su exclusión. | los delitos informáticos durante el proceso y que se presume irregular se interpondrá una tacha de prueba solicitando su exclusión | Tachas | exclusión de medio de prueba | señalar tachas contra la prueba digital | interponer Tutela de Derechos y Nulidad | cuestionar durante la investigación la prueba digital, sin embargo también se puede solicitar la exclusión de dicha prueba mediante tachas o nulidad |
| 7 ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué? | Ninguno | En uno, donde la prueba digital ofrecida era el contenido de un teléfono celular extraído en una pericia digital, y el cuestionamiento de la defensa del imputado fue contra la formalidad en la obtención de la misma, que no se actuó garantizando el derecho de defensa, y que lo obtenido pudo haber sido manipulado. | Por la asunción reciente del cargo, aún no he tenido la oportunidad de ver un caso donde se haya debatido prueba digital | Pericia digital Formalidad para obtención de la prueba Derecho de Defensa | Rigurosidad para la obtención de la prueba digital y no afectar el Derecho de Defensa | Dos entrevistados indican que no han participado en casos que se hayan actuado prueba digital | Un entrevistado refirió un caso de cuestionamiento a la formalidad de la prueba digital | Solo un entrevistado indico su experiencia en juicio con evidencia digital |
| 8 ¿Cuáles son los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique. | Considero que es el procedimiento de la cadena de custodia, a efectos de cautelar el medio de prueba y posteriormente no haya ningún cuestionamiento | Generalmente la obtención de la prueba digital es a través de una pericia que la practica la Policía Nacional del Perú o la Oficina de Peritajes del Ministerio Público. | Considero que uno de los procedimientos que realiza la Fiscalía para la obtención de la prueba digital es a través de una pericia practicada en la Oficina de Peritajes de la misma institución | Cadena de custodia Peritajes | Peritajes | Dos entrevistados comulgan al indicar el conocimiento de los peritajes que se efectúan a la prueba digital | Un entrevistado hizo referencia a la cadena de custodia como procedimiento para cautelar la prueba digital | Se concluye que los peritajes de la prueba digital son el principal procedimiento para su obtención. |

| | | | | | | | | |
|---|--|--|---|--|--|--|--|---|
| 9 ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio? | Considero que deben diseñarse protocolos de actuación conjunta – Protocolos interinstitucionales | No existe una norma exacta referida a dicho tema | Desconozco la normatividad vigente para la recolección y obtención de la prueba digital, pero si la obtención ha sido efectuada de forma irregular será cuestionada su valoración por el Juzgador | Protocolos interinstitucionales | Protocolos interinstitucionales | Dos entrevistados indican que desconocen norma | Un entrevistado indica la realización de un Protocolo interinstitucional | Se tiene que la existencia de Protocolos interinstitucionales resultaría factible y necesario para un mejor desempeño de los operadores de justicia |
| 10 ¿Cuáles con los cuestionamientos más recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué? | La cadena de custodia Su debida custodia y actuación | El derecho de defensa, donde no se citó a la defensa para que participe de la pericia que extrae la información del equipo electrónico. | No he tenido la oportunidad de realizar un juicio sobre este tema pero considero que se cuestionaría su originalidad y su obtención regular | Cadena de custodia y debida actuación Derecho de defensa | Cadena de custodia y debida diligencia | No existen coincidencias | Resultan respuestas diversas de los entrevistados donde señalan cadena de custodia, Derecho de Defensa y originalidad y obtención de la prueba | La prueba digital debe recabarse adecuadamente a efectos de evitar cuestionamientos de la cadena de custodia y que no afecten su originalidad |
| 11. ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué? | Su obtención y custodia, estos, cadena de custodia | La forma y modo de cómo se recolecta la prueba digital, dado que no se garantizaría que no sea alterado dicha prueba o los soportes electrónicos que guardan la información. | Considero que uno de los cuestionamientos para la recolección y obtención de la evidencia digital se da con la manipulación de los dispositivos informáticos que podría alterar dicha prueba | Cadena de custodia Recolección de prueba digital Manipulación de dispositivos informáticos | Cuestionamientos en la recolección y cadena de custodia de la prueba digital | Dos entrevistados coinciden en señalar la recolección de la prueba digital como punto de cuestionamiento | Un entrevistado indica la cadena de custodia como materia de cuestionamiento | Los cuestionamientos a la prueba digital radican en su obtención y manipulación, por lo que se debe garantizar la fiabilidad y autenticidad de la misma |
| 12. ¿Considera usted que existe una | Podría darse en tanto no se contaría con un | No existe la tecnología suficiente para la realización de todos los | Al ser un tema nuevo si existe problemas en la realización de peritajes | Escasez de peritos | Problemas en los peritajes y la | Todos coinciden que la problemática | Un entrevistado enfoca su punto en la poca | Dado que las pericias se realizan por los órganos de apoyo de los operadores |

| | | | | | | | | |
|--|---|---|---|--|---|--|--|---|
| <p>problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?</p> | <p>gran número de peritos especializados sobre la materia</p> | <p>peritajes en prueba digital, sobre todo en celulares de alta gama.</p> | <p>a una evidencia digital pues a veces los peritos no se ponen de acuerdo sobre la conclusión y hay pericias distintas</p> | <p>informáticos y tecnología Pericias con resultados diversos</p> | <p>tecnología empleada en ella</p> | <p>existente radica en las pericas</p> | <p>cantidad de peritos especializados, otro entrevistado señala la poca tecnología, y el tercero indica conclusiones diversas de las pericias</p> | <p>de justicia, existe un escasa logística y actualización de los equipos para la realización de pericias</p> |
| <p>13 ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?</p> | <p>Seria el D.L. 1412 y su reglamento</p> | <p>Es la misma aplicable a la recolección de cualquier medio de prueba</p> | <p>Considero que el Reglamento para el recojo de evidencia digital, así como la Resolución 729-2016-MP-FN – Reglamento de Cadena de Custodia de Bienes incautados</p> | <p>D.L. 1412 – Ley de Gobierno digital Reglamento para el recojo de evidencia digital Reglamento de Cadena de Custodia de Bienes incautados</p> | <p>Normas para recojo de bienes incautados en general</p> | <p>Dos entrevistados se refieren al Reglamento de Cadena de Custodia de Bienes incautados</p> | <p>Un entrevistado hace referencia a la Ley de Gobierno digital, uno indica Reglamento para el recojo de evidencia digital pero no precisa cual es</p> | <p>Las normas señaladas están referidas al recojo del soporte físico de evidencia</p> |
| <p>14 ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?</p> | <p>Desconozco</p> | <p>La Guía práctica para requerir información a proveedores internacionales de internet, así como los convenios celebrados por el Perú con otros países que le permite solicitar información vía Cooperación Internacional luego de solicitar las medidas limitativas de derechos en el Perú.</p> | <p>Tengo conocimiento que son el Convenio de Budapest, así como convenios celebrados por el Perú con otros países sobre ciberdelincuencia.</p> | <p>Convenio de Budapest Guía práctica para requerir información a proveedores internacionales de internet Convenios celebrados por el Perú con diversos países sobre ciberdelincuencia</p> | <p>Convenio de Budapest o sobre Ciberdelincuencia</p> | <p>Dos entrevistados coinciden en señalar los Convenios celebrados por el Perú con diversos países sobre ciberdelincuencia</p> | <p>Un entrevistado indica Guía práctica para requerir información a proveedores internacionales de internet, y otro entrevistado refiere el Convenio de Budapest</p> | <p>Los Convenios celebrados por el Perú con diversos países sobre ciberdelincuencia están referidos a la cooperación de países en dichos delitos y su procedimiento</p> |

ANEXO 11 CONSENTIMIENTO INFORMADO



UNIVERSIDAD CÉSAR VALLEJO

"Año del Fortalecimiento de la Soberanía Nacional"
"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

CONSENTIMIENTO INFORMADO

Estimado (a) participante:

GLADYS EULALIA AMABLE BASILIO

Fiscal Provincial Penal

El alumno, viene realizando la investigación titulada: *"La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021"*.

Por medio de la presente se le hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando con la entrevista semiestructurada diseñada para el cumplimiento de los objetivos trazados. Los datos e información que usted brinde serán utilizados únicamente para fines académicos y del estudio mencionado; además se respetará en todo momento su confidencialidad y en especial su identificación.

La información que usted brinde será de importante ayuda, debido a que sus respuestas permitirán generar conocimiento relevante para analizar y comprender el problema planteado.

Debido al distanciamiento social en que nos encontramos por la pandemia provocada por la Covid - 19, la entrevista se realizará a través del llenado de la guía de entrevista que se adjunta al presente documento.

Por lo expuesto, la participante acepta voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando la presente en señal de conformidad.

Lima, 21 de julio de 2022.


GLADYS EULALIA AMABLE BASILIO
FISCAL PROVINCIAL
3ra. Fiscalía Provincial Penal Corporativa
Distrito Fiscal de Lima Norte
I.F.F.P. (I.F.S.P.)

Firma y sello

CONSENTIMIENTO INFORMADO

Estimado (a) participante:

ERIKA BEATRIZ HUACACHI ZANZI

Fiscal Provincial Penal

El alumno, viene realizando la investigación titulada: *“La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021”*.

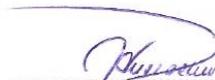
Por medio de la presente se le hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando con la entrevista semiestructurada diseñada para el cumplimiento de los objetivos trazados. Los datos e información que usted brinde serán utilizados únicamente para fines académicos y del estudio mencionado; además se respetará en todo momento su confidencialidad y en especial su identificación.

La información que usted brinde será de importante ayuda, debido a que sus respuestas permitirán generar conocimiento relevante para analizar y comprender el problema planteado.

Debido al distanciamiento social en que nos encontramos por la pandemia provocada por la Covid - 19, la entrevista se realizará a través del llenado de la guía de entrevista que se adjunta al presente documento.

Por lo expuesto, la participante acepta voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando la presente en señal de conformidad.

Lima, 15 de julio de 2022.



ERIKA BEATRIZ HUACACHI ZANZI
FISCAL PROVINCIAL
3ra. Fiscalía Prov. Penal Corporativa de Carabaylo
Segundo Despacho - D.F. Lima Norte

Firma y sello

CONSENTIMIENTO INFORMADO

Estimado (a) participante:

SAMUEL ELÍ LADRON DE GUEVARA LANDA

Fiscal Provincial Penal

El alumno, viene realizando la investigación titulada: *"La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021"*.

Por medio de la presente se le hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando con la entrevista semiestructurada diseñada para el cumplimiento de los objetivos trazados. Los datos e información que usted brinde serán utilizados únicamente para fines académicos y del estudio mencionado; además se respetará en todo momento su confidencialidad y en especial su identificación.

La información que usted brinde será de importante ayuda, debido a que sus respuestas permitirán generar conocimiento relevante para analizar y comprender el problema planteado.

Debido al distanciamiento social en que nos encontramos por la pandemia provocada por la Covid - 19, la entrevista se realizará a través del llenado de la guía de entrevista que se adjunta al presente documento.

Por lo expuesto, la participante acepta voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando la presente en señal de conformidad.

Lima, 21 de julio de 2022.


.....
SAMUEL ELÍ LADRÓN DE GUEVARA LANDA
Fiscal Provincial
3ra. Fisc. Prov. Penal Corporativa de Carabayllo
Tercer Despacho - D.F. Lima Norte

Firma y sello

CONSENTIMIENTO INFORMADO

Estimado (a) participante:

GUILLERMO ROGELIO DOMINGUEZ ROMERO

Fiscal Adjunto Provincial Penal

El alumno, viene realizando la investigación titulada: *"La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021"*.

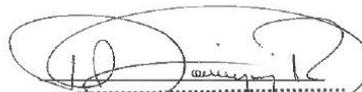
Por medio de la presente se le hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando con la entrevista semiestructurada diseñada para el cumplimiento de los objetivos trazados. Los datos e información que usted brinde serán utilizados únicamente para fines académicos y del estudio mencionado; además se respetará en todo momento su confidencialidad y en especial su identificación.

La información que usted brinde será de importante ayuda, debido a que sus respuestas permitirán generar conocimiento relevante para analizar y comprender el problema planteado.

Debido al distanciamiento social en que nos encontramos por la pandemia provocada por la Covid - 19, la entrevista se realizará a través del llenado de la guía de entrevista que se adjunta al presente documento.

Por lo expuesto, la participante acepta voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando la presente en señal de conformidad.

Lima, 18 de julio de 2022.


.....
GUILLERMO ROGELIO DOMINGUEZ ROMERO
Fiscal Adjunto Provincial
3ra. Fisc. Prov. Penal Corporativa de Carabayillo
Tercer Despacho - D.F. Lima Norte

CONSENTIMIENTO INFORMADO

Estimado (a) participante:

ENRIQUE PALOMINO GUTIERREZ

Juez Especializado en lo Penal

El alumno, viene realizando la investigación titulada: *"La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021"*.

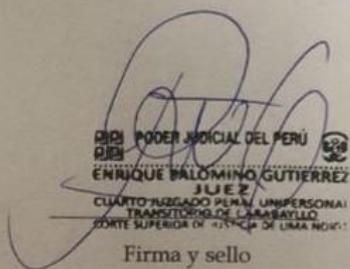
Por medio de la presente se le hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando con la entrevista semiestructurada diseñada para el cumplimiento de los objetivos trazados. Los datos e información que usted brinde serán utilizados únicamente para fines académicos y del estudio mencionado; además se respetará en todo momento su confidencialidad y en especial su identificación.

La información que usted brinde será de importante ayuda, debido a que sus respuestas permitirán generar conocimiento relevante para analizar y comprender el problema planteado.

Debido al distanciamiento social en que nos encontramos por la pandemia provocada por la Covid - 19, la entrevista se realizará a través del llenado de la guía de entrevista que se adjunta al presente documento.

Por lo expuesto, la participante acepta voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando la presente en señal de conformidad.

Lima, 19 de julio de 2022.


Poder Judicial del Perú
ENRIQUE PALOMINO GUTIERREZ
JUEZ
CUARTO JUZGADO PENAL UNIPERSONAL
TRANSITORIO DE LIMA NOROCCIDENTAL
CORTE SUPERIOR DE JUSTICIA DE LIMA NOROCCIDENTAL

Firma y sello

CONSENTIMIENTO INFORMADO

Estimado (a) participante:

LUIS ALBERTO DEJO APAESTEGUI

Juez Especializado en lo Penal

El alumno, viene realizando la investigación titulada: *"La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021"*.

Por medio de la presente se le hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando con la entrevista semiestructurada diseñada para el cumplimiento de los objetivos trazados. Los datos e información que usted brinde serán utilizados únicamente para fines académicos y del estudio mencionado; además se respetará en todo momento su confidencialidad y en especial su identificación.

La información que usted brinde será de importante ayuda, debido a que sus respuestas permitirán generar conocimiento relevante para analizar y comprender el problema planteado.

Debido al distanciamiento social en que nos encontramos por la pandemia provocada por la Covid - 19, la entrevista se realizará a través del llenado de la guía de entrevista que se adjunta al presente documento.

Por lo expuesto, la participante acepta voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando la presente en señal de conformidad.

Lima, 19 de julio de 2022.


PODER JUDICIAL DEL PERU
LUIS ALBERTO DEJO APAESTEGUI
JUEZ
SEGUNDO JUZGADO DE INVESTIGACION
PREPARATORIA - DEPARTAMENTO DE LOS RIOS
CORTE SUPLENTE DE JUSTICIA DE LIMA NORTE

Firma y sello

CONSENTIMIENTO INFORMADO

Estimado (a) participante:

VALERY RAUL ROMERO PALACIOS

Juez Especializado en lo Penal

El alumno, viene realizando la investigación titulada: *"La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021"*.

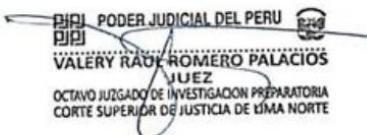
Por medio de la presente se le hace de conocimiento de la importancia de su participación para el presente estudio de investigación, colaborando con la entrevista semiestructurada diseñada para el cumplimiento de los objetivos trazados. Los datos e información que usted brinde serán utilizados únicamente para fines académicos y del estudio mencionado; además se respetará en todo momento su confidencialidad y en especial su identificación.

La información que usted brinde será de importante ayuda, debido a que sus respuestas permitirán generar conocimiento relevante para analizar y comprender el problema planteado.

Debido al distanciamiento social en que nos encontramos por la pandemia provocada por la Covid - 19, la entrevista se realizará a través del llenado de la guía de entrevista que se adjunta al presente documento.

Por lo expuesto, la participante acepta voluntariamente participar y contribuir con su experiencia y profesionalismo en la referida entrevista, firmando la presente en señal de conformidad.

Lima, 20 de julio de 2022.


PODER JUDICIAL DEL PERU
VALERY RAUL ROMERO PALACIOS
JUEZ
OCTAVO JUZGADO DE INVESTIGACION PREPARATORIA
CORTE SUPERIOR DE JUSTICIA DE LIMA NORTE

Firma y sello

6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?

Tutela de Derechos, inadmisibilidad de ofrecimiento de pruebas.

7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué?

En uno, en el cual se cuestionó las capturas de conversaciones mediante el aplicativo Whatsapp toda vez que en la recolección de dicha información no se realizó desde el celular o aparato en el cual obraba la misma, solo se tenía las capturas presentadas por la parte denunciante. El abogado defensor del imputado indicaba que no se tenía certeza si esa información era auténtica por cuanto eran capturas que podrían haber sido manipuladas, teniendo en cuenta la tecnología.

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.

Copia imagen, video, Análisis digital forense, etc.

9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?

No, porque dada la naturaleza de la prueba en estos delitos, se requiere procedimiento distinto a los otros medios de prueba para asegurar la mismidad de la misma.

10. ¿Cuáles con los cuestionamientos más recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?

El procedimiento de recojo de evidencias, por ejemplo, en el caso de los mensajes whatsapp, fotos, etc., contenidas en el celular, el procedimiento correcto sería que deben se ser recopilados del mismo aparato celular mediante visualización del mismo, redactándose el acta correspondiente con la información pertinente, sin embargo, muchas veces, lo que se actúa en juicio son las capturas de mensaje o las fotografías presentadas a por una de las partes, por lo que el abogado cuestiona


GLADYS EULALIA AMABLE BASILIO
FISCAL PROVINCIAL
3ra. Fiscalía Provincial Penal Corporativa
Distrito Fiscal de Lima Norte
TELEFONO 011 476 1111

la autenticidad de dichas capturas, al no haberse seguido un procedimiento que garantice la mismidad de la información actuada en juicio oral.

11. ¿Cuáles son los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?

Los cuestionamientos más recurrentes son: No se sigue un procedimiento que garantice la autenticidad de la información que se va actuar en juicio oral.

12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?

No se cuenta con muchos peritos forenses. Además, los peritos del IML tienen competencia a nivel nacional por lo que su carga es abundante, lo que dilata la emisión de sus informes, retardando las investigaciones. En igual sentido ocurre con los peritos de la Policía Nacional del Perú, pues está centralizado.

13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

El NCPP, Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados (Aprobado por Resolución n° 729-2006-MP-FN del 15 de junio del 2006), Acuerdos Plenarios N° 5-2010/CJ-116 y N° 6-2012/CJ-116, de la Corte Suprema de Justicia de la República.

14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

Convención de Cibercriminalidad (Budapest, 2001) y Protocolo del grupo de trabajo científico en evidencia digital (SWGDE) "Best Practices for Computer Forensics".

| Nombre del entrevistado | Sello y Firma |
|--------------------------|--|
| Gladys E. Amable Basilio |  GLADYS EULALIA AMABLE BASILIO FISCAL PROVINCIAL Jrta. Fiscalía Provincial Penal Corporativa Distrito Fiscal de Lima Norte TERCER DEPARTAMENTO |

GUÍA DE ENTREVISTA DIRIGIDA A FISCALES PENALES

TÍTULO: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

Entrevistado (a): *Frika B. Nucocani Zanzi*

Edad: *45* años

Sexo: *Femenino*

Fecha: *15/07/22*

CATEGORÍA 1: LA PRUEBA DIGITAL

1. ¿Considera usted que son necesarios la prueba digital durante la investigación preliminar en los delitos informáticos? ¿Por qué?

Si, para búsqueda o corroboración de información.

2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos?

1) El ya no cuentan con los soportes donde se almacenaría la prueba 2) falta de cuidado al guardar adecuadamente la información, 3) falta de software para obtener o acceso a la información digital.

3. ¿Existe diferencia en la cadena de custodia durante la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?

Los formatos usados para los soportes físicos son los mismos con respecto de las características del soporte mas no de algún registro o codificación del resguardo o autenticidad de su contenido al momento de su obtención.

4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital?

Ninguno.

5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?

No, -

6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?

La duda de posible adulterabilidad o que se revista la probabilidad de haber sido alterada la prueba mediante supresión o edición de información. Por lo que el contenido de información en el Acta de Cadena de Custodia.

7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué?

Ninguno. -

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.

Requerimientos físicos de quien tiene el soporte de la información conteniendo la prueba, su uso y conservación de su base y si se requiere que realicen una copia con su sello (firmado) dicho soporte debe ser remitido para su examen. -

9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?

No, aun existe poca regulación e información sobre el tema.

10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?

No he participado en juicios por ser tipo de delitos. -

11. ¿Cuáles son los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?

No he tenido alguno en investigaciones por ese tipo de delitos.

12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?

Si, falta de obtención de programas, licencias de software para la obtención de información o pericias.

13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

En forma genérica se tiene como base al NCPP

14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

Desempeño

| Nombre del entrevistado | Sello y Firma |
|-------------------------|---|
| Erika Beatriz Zanzi |  ERIKA BEATRIZ NUACACHI ZANZI FISCAL PROVINCIAL 3ra. Fiscalía Prov. Penal Corporativa de Carabaylo Segundo Despacho - D.F. Lima Norte |

GUÍA DE ENTREVISTA DIRIGIDA A FISCALES PENALES

TÍTULO: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

Entrevistado (a) : Guillermo Rogelio Dominguez Romero.....

Edad: 39 años

Sexo: Masculino..

Fecha: 18-07-2022

CATEGORÍA 1: LA PRUEBA DIGITAL

1. ¿Considera usted que son necesarios la prueba digital durante la investigación preliminar en los delitos informáticos? ¿Por qué?

Si son necesarios, porque los delitos informáticos requieren de fuentes tanto tecnológicas como dispositivos digitales, que brindan el soporte electrónico, que sirven para determinar la comisión o vinculación de un hecho delictivo o acreditarlos.

2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos?

Las pruebas digitales tienen la posibilidad de ser manipuladas, pudiéndose alterar su soporte digital, otra es la obtención de la misma, ya que los pruebas digitales son obtenidas sin previa verificación, pudiendo quitarle gerencia a su carga probatoria estimado por perito informático, cuando su veracidad sea cuestionada.

3. ¿Existe diferencia en la cadena de custodia durante la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?

Si, porque la cadena de custodia digital debe garantizar la fiabilidad de la prueba digital con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba, por lo que dentro del procedimiento de prueba puede informático-tecnológico resulte adecuado garantizar su autenticidad.

4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital?

Con el fin de recopilar y preservar eficazmente las evidencias de un delito informático, es necesario recopilar la información digital a través de herramientas protegidas y seguras, dado que usando estas herramientas se podrá asegurar la evidencia recogida no ha sido modificada ni destruida.

5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?

- la ley 20096 - Ley de Delitos Informáticos.
- manual para el recojo de evidencia digital.

6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?

- la cadena de custodia y prueba digital
- la extracción de la prueba digital (INAST)

7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué?

Casos judicializados, con ninguno.

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.

Que la prueba digital se encuentre en lugar correcto, efectuar la cadena de custodia y proteger la evidencia.

9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?

Considero que la normatividad es explícita y suficiente, lo que debe cambiarse es el mejoramiento de los equipos peritales para hacer más dinámico y efectivo la recopilación de pruebas.

10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?

la fecha de la obtención de la prueba digital y la fecha con que se realizó la prueba respectiva, toda vez que se tiene de descender y reducir su valor probatorio.

.....
.....
11. ¿Cuáles son los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?

Se cuestiona:

- Le forme como se obtuvo la misma, con el fin de desacreditar la misma
- La manipulación que tuvo la misma, para restarle nivel probatorio
- La legalidad de la misma.

12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?

La problemática en el sentido de la demora del mismo, por parte de los peritos informáticos y la deficiencia de equipos tecnológicos para el resultado del mismo y en otros jefes de personal idóneos.

13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

- El Manual para el recojo de la Evidencia Digital
- Ley 29733 Ley de Protección de datos personales

14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

- El Convenio sobre la Ciberdelincuencia

| Nombre del entrevistado | Sello y Firma |
|------------------------------------|--|
| Guillermo Rogelio Domínguez Romero |  GUILLERMO ROGELIO DOMÍNGUEZ ROMERO Fiscal Adjunto Provincial 3ra. Fisc. Prov. Penal Corporativa de Carabayillo Tercer Despacho - D.F. Lima Norte |

GUÍA DE ENTREVISTA DIRIGIDA A FISCALES PENALES

TÍTULO: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

Entrevistado (a): Samuel Eli Ladron de Guevara Landa

Edad: 37 años

Sexo: Masculino

Fecha: 16/07/2022

CATEGORÍA 1: LA PRUEBA DIGITAL

1. ¿Considera usted que son necesarios la prueba digital durante la investigación preliminar en los delitos informáticos? ¿Por qué?

Sí, porque permiten probar la hipótesis fiscal. Asimismo, porque corresponde a la naturaleza del delito mencionado.

2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos?

En primer lugar su carácter novísimo en la actualidad, lo que deriva que tengamos operadores (policiales, fiscales y jurisdiccionales) con poca preparación y escasa experticia.

3. ¿Existe diferencia en la cadena de custodia durante la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?

Sí, porque por su propia naturaleza son distintos. No es lo mismo un objeto material físico, como la evidencia digital que si bien se soporta en un medio magnético, no obstante requiere otro tratamiento.

4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital?

He tenido oportunidad de ver en los informes policiales el uso del "Centro premium Cellabrite". Asimismo, he oído del código hash.

5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?

- Por conocimiento del Manual, para el recibo de la evidencia digital aprobado por Resolución Ministerial N° 848 - 2019 - IN, La Resolución N° 729 - 2016 - RP - FN y la Directiva N° 03 - 19 - 2015 - DIRGEN - PNP / EMB - PNP, y Convenio de Budapest.
6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?
- Considero que una Tutela de derechos, porque permitiría excluir prueba digital obtenida de manera ilegal o manipulada de tal manera que no garantiza fiabilidad.
7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta ha sido materia de debate o cuestionamiento? ¿Por qué?
- Si bien me encuentro participando en procesos penales en los cuales existe prueba digital, no obstante aun no ha transitado a la etapa de juicio oral, o tampoco se ha cuestionado sea oírlo del.

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.
- Encaso el primer intervención no sea especializado dependerá de si se trata de dispositivos transportables o no transportables, en cuyo caso se deberá dar el trato de evidencia digital, y su correspondiente custodia.
9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?
- No, veien la realidad esta generando casuística que sobrepasa el marco normativo actual, por lo que no sería suficiente para un adecuado trato legal, por ende puede ser cuestionada.
10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?
- Si bien no he participado, considero que podría ser su originalidad, adecuada manipulación.

y correcto embalaje.

11. ¿Cuáles son los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?

La correcta manipulación de los dispositivos informáticos. Porque si no se puede de manera correcta y especializada se afecta la fiabilidad de la prueba digital.

12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?

Si, porque existe exceso de peritos, lo que deriva en que las pericias tarden, y con ello la posibilidad de realizar otros actos de investigación derivados del mismo.

13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

Considero que son las memoradas en la respuesta 5, a excepción del convenio de Budapest.

14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

El Convenio de Budapest o sobre cibercrimen y la Norma ISO/IEC 27037:2012.

| Nombre del entrevistado | Sello y Firma |
|--|--|
| Samuel Eli Ladron de Guevara Landa |  SAMUEL ELI LADRÓN DE GUEVARA LANDA Fiscal Provincial 3ra. Fisc. Prov. Penal Corporativa de Carabayillo Tercer Despacho - D.F. Lima Norte |

ANEXO 13

GUIA DE ENTREVISTAS DE JUECES PENALES

GUÍA DE ENTREVISTA DIRIGIDA A JUECES PENALES

TÍTULO: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

Entrevistado (a) : LUIS ALBERTO DEJO APAESTEGUI

Edad:49 años

Sexo: Masculino

Fecha: 19-07-2022

CATEGORÍA 1: LA PRUEBA DIGITAL

1. ¿Considera usted que es necesario la prueba digital durante la investigación preliminar en los delitos informáticos? ¿Por qué?

Considero que sí, dado que la prueba digital es uno de los principales elementos que servirá para sustentar una posible formalización de la investigación o las medidas coercitivas que pueda requerir el Ministerio Público, sin la cual difícilmente tendrá futuro algún caso.

2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos?

Uno los problemas que tiene el Ministerio Público para la obtención de la prueba digital, es que es de difícil obtención, y sobre todo presentan problemas en su recolección y preservación, que es aprovechado por la defensa del imputado a fin de cuestionarla y pretender excluirlas de la investigación, de igual manera se cuestiona la forma como se actúan a nivel preliminar.

3. ¿Existe diferencia en la elaboración de la cadena de custodia durante la obtención de la prueba digital de los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?

En líneas generales no existe diferencia, por cuando la cadena de custodia es un elemento que garantiza que no se realice manipulación externa del bien recogido.

4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital?

El mas conocido es la función HASH que es un algoritmo con el cual se crea una serie alfa numérica con lo cual se asegura y se verifica que la información digital no sea alterada, así como el software forense UFED mediante el cual se efectúa una

búsqueda de determinada información necesaria para la investigación en dispositivos como el caso de equipos celulares,

5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?

El Ministerio Público recientemente ha publicado una Guía práctica para requerir información a proveedores internacionales de internet, luego de ello, no existiría mas información dado que la investigación de dichos delitos es relativamente nueva.

6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?

Tachas contra un determinado medio de prueba, a fin de solicitar su exclusión.

7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué?

En uno, donde la prueba digital ofrecida era el contenido de un teléfono celular extraído en una pericia digital, y el cuestionamiento de la defensa del imputado fue contra la formalidad en la obtención de la misma, que no se actuó garantizando el derecho de defensa, y que lo obtenido pudo haber sido manipulado.

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.

Generalmente la obtención de la prueba digital es a través de una pericia que la practica la Policía Nacional del Perú o la Oficina de Peritajes del Ministerio Público.

9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?

No existe una norma exacta referida a dicho tema.

10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?

El derecho de defensa, donde no se citó a la defensa para que participe de la pericia que extrae la información del equipo electrónico.

11. ¿Cuáles con los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?
La forma y modo de como se recolecta la prueba digital, dado que no se garantizaría que no sea alterado dicha prueba o los soportes electrónicos que guardan la información.
12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?
No existe la tecnología suficiente para la realización de todos los peritajes en prueba digital, sobre todo en celulares de alta gama.
13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?
Es la misma aplicable a la recolección de cualquier medio de prueba.
14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?
La Guía práctica para requerir información a proveedores internacionales de internet, así como los convenios celebrados por el Perú con otros países que le permite solicitar información via Cooperación Internacional luego de solicitar las medidas limitativas de derechos en el Perú.

| Nombre del entrevistado | Sello y Firma |
|----------------------------------|--|
| Dr. Luis Alberto Dejo Apaestegui |  |

GUÍA DE ENTREVISTA DIRIGIDA A JUECES PENALES

TÍTULO: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

Entrevistado (a) : VALERY ROUL ROMERO PALACIOS

Edad: 38 años Sexo: M Fecha: 20/07/22

CATEGORÍA 1: LA PRUEBA DIGITAL

1. ¿Considera usted que son necesarios la prueba digital durante la investigación preliminar en los delitos informáticos? ¿Por qué?

Considero que si, toda vez que toda información obtenida o transmitida a través de un medio tecnológico electrónico o dispositivo digital, va a condicionar con la estrategia de investigación fiscal.

2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos?

Considero que se tiene en principio cautelar en forma correcta la prueba digital (cadena de custodia); Segundo, considero que su activación y posterior valoración aún en nuestro sistema de justicia es nuevo.

3. ¿Existe diferencia en la cadena de custodia durante la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?

Considero que si, toda vez que la prueba digital va a requerir diversos mecanismos para asegurar la evidencia que se encuentre en un medio electrónico o dispositivo digital.

4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital?

Bueno el mecanismo será la cadena de custodia; pero aplicaciones o programas, desconozco.

5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?

Solo sobre el D.L. N° 1412 y su reglamento.

-
.....
.....
.....
6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?

Creo que se podría formular una tutela de Derechos o Acción Amparo, todo vez que se debe respetar la cadena de custodia, y la obtención de la prueba digital no debe afectar derechos fundamentales.

7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué?

Ninguno.

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.

Considero que es el Procedimiento de la Cadena de custodia, a efectos de custodiar el medio de prueba, y posteriormente no haya ningún cuestionamiento.

9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?

Considero que deben diseñarse Protocolos de Actuación Conjunta. - Protocolos Interinstitucionales.

10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?

→ La cadena de custodia.
→ Su debida custodia y detención.

11. ¿Cuáles son los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?

S: obtención y custodia = Cadena de custodia.

12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?

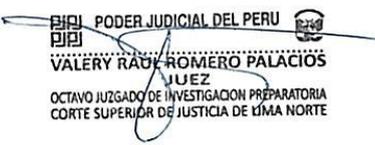
Podría darse en tanto no se cuentan con un gran número de peritos especializados sobre la materia.

13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

Señala el D.L. 1412 y su reglamento.

14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

Desconozco.

| Nombre del entrevistado | Sello y Firma |
|-----------------------------|--|
| Valery Raúl Romero Palacios |  <p>PODER JUDICIAL DEL PERU VALERY RAÚL ROMERO PALACIOS JUEZ OCTAVO JUZGADO DE INVESTIGACION PREPARATORIA CORTE SUPERIOR DE JUSTICIA DE LIMA NORTE</p> |

GUÍA DE ENTREVISTA DIRIGIDA A JUECES PENALES

TÍTULO: La obtención de la Prueba Digital en los Delitos Informáticos en el Distrito Fiscal de Lima Norte, 2021

Entrevistado (a): ENRIQUE POLOMINO GUTIERREZ

Edad: 37 años

Sexo: MASCULINO

Fecha: 20/07/2022

CATEGORÍA 1: LA PRUEBA DIGITAL

1. ¿Considera usted que son necesarios la prueba digital durante la investigación preliminar en los delitos informáticos? ¿Por qué?

CONSIDERO QUE LAS EVIDENCIAS DIGITALES RESULTAN RELEVANTES DURANTE LA INVESTIGACIÓN PRELIMINAR EN LOS DELITOS INFORMÁTICOS A FIN DE QUE LA FISCALÍA PUEDA SUSTENTAR UNA FORMALIZACIÓN Y CONTINUACIÓN DE INVESTIGACIÓN PREPARATORIA Y DEMÁS PROCEDIMIENTOS.

2. ¿Cuáles son las dificultades que ha observado en los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos?

EN MI LABOR JURISDICCIONAL, NO PODRÍA PRECISAR LAS DIFICULTADES QUE TIENE LA FISCALÍA PARA LA OBTENCIÓN DE UNA PRUEBA DIGITAL EN LA INVESTIGACIÓN PRELIMINAR EN LOS DELITOS INFORMÁTICOS.

3. ¿Existe diferencia en la cadena de custodia durante la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos en comparación de los delitos comunes? ¿Por qué?

CONSIDERO QUE DEBERÍA EXISTIR, PUES LA OBTENCIÓN DE UNA EVIDENCIA DIGITAL, RESULTA SER MÁS COMPLEJA.

4. ¿Qué mecanismos, aplicaciones o programas conoce a fin de preservar la inalterabilidad de la prueba o evidencia digital?

UNO DE LOS PROGRAMAS QUE SIRVEN PARA PRESERVAR LA INALTERABILIDAD DE LA PRUEBA DIGITAL ES LA FUNCIÓN HASH QUE VERIFICA QUE LA INFORMACIÓN DIGITAL NO SEA ALTERADA.

5. ¿Tiene conocimiento de reglamentos o directivas que regulan sobre la obtención de la prueba digital en los Delitos Informáticos?

El ser un tema no muy desarrollado por ser nuevo solo tengo
conocimiento de la Fiscalía especializada ha publicado una guía
práctica para recabar información a proveedores internacionales
de internet.

6. ¿Qué medios de defensa considera usted que se podrían utilizar contra la prueba digital obtenida por el Ministerio Público en los Delitos Informáticos durante la investigación preparatoria, etapa intermedia o juicio oral? ¿Por qué?

Contra una prueba digital obtenida por el ministerio público en
los delitos informáticos durante el proceso y que se prima irregular
se prepararía una tacha de prueba solicitando su exclusión

7. ¿En cuántos casos judicializados ha participado usted donde se actúe prueba digital, y ésta hay sido materia de debate o cuestionamiento? ¿Por qué?

por la situación reciente del cargo aún no he tenido la oportunidad
de ver un caso donde se haya usado prueba digital

CATEGORÍA 2: DELITOS INFORMÁTICOS

8. ¿Cuáles son los procedimientos que efectúa el Ministerio Público para la obtención de la prueba digital en la investigación a nivel preliminar en los Delitos Informáticos? Explique.

Considero que uno de los procedimientos que realiza la Fiscalía
para la obtención de una prueba digital es a través de una
peritaje realizado en la oficina o peritaje en la misma institución.

9. ¿Considera Ud, que la normatividad actual es suficiente para asegurar que la recolección y obtención de la prueba digital en los delitos informáticos no sea posteriormente cuestionada al momento de ser valorada en juicio?

Desconozco la normatividad vigente para la recolección y obtención de la
prueba digital, pero si la obtención a sido realizada de forma irregular
será cuestionada en su valoración por el J.P. Juez.

10. ¿Cuáles con los cuestionamientos mas recurrentes a la actuación en juicio de la prueba digital en los delitos informáticos? ¿Por qué?

No he tenido la oportunidad de realizar un juicio solo de este tema
pero considero que se cuestionaría su originalidad y su obtención regular.

11. ¿Cuáles son los cuestionamientos más recurrentes a la recolección y obtención de la prueba digital en los delitos informáticos? ¿Por qué?

Considero que uno de los cuestionamientos para la recolección y obtención de la evidencia digital se da en la manipulación de los dispositivos informáticos que podría alterar o crear pruebas.

12. ¿Considera usted que existe una problemática en la realización de peritajes en la prueba digital en los delitos informáticos? ¿Por qué?

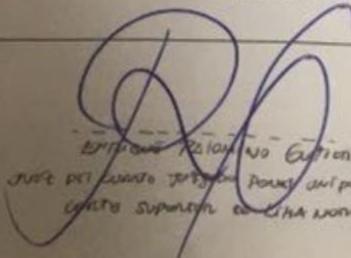
Al ser un tema nuevo si existe problemas en la realización de peritajes a una evidencia digital, pues a veces los peritos no se ponen de acuerdo sobre la conclusión y hay pareceres distintos.

13. ¿Cuáles son las normas nacionales referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

Considero que el Reglamento para el acapio de evidencia digital así como la resolución 729-2016-MP-FN

14. ¿Cuáles son los instrumentos internacionales o de cooperación internacional referidas a la recolección y obtención de la prueba digital en los delitos informáticos?

Tengo conocimiento que es el convenio de Budapest así como convenios celebrados por el Perú con otros países sobre libertad informática.

| Nombre del entrevistado | Sello y Firma |
|----------------------------|--|
| ENRIQUE POLIMINO GUTIERREZ |  ENRIQUE POLIMINO GUTIERREZ Jefe del Centro Judicial Penal del Personal Centro Superior de Lima Norte |