Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

LA PRUEBA DIGITAL Y SU INFLUENCIA EN EL DELITO DE FRAUDE INFORMÁTICO EN LA FISCALÍA PENAL PROVINCIAL DE LIMA NORTE, 2024

Línea de investigación:
Procesos jurídicos y resolución de conflictos

Tesis para optar el Título Profesional de Abogada

Autora

Canario Robles, Vivian Lizeth

Asesor

Ambrosio Bejarano, Hugo Ramiro

ORCID: 0000-0003-3796-2580

Jurado

Gonzales Loli, Martha Rocio

Moscoso Torres, Víctor Juber

Sarmiento Albacetti, Gladys

Lima - Perú

2026

RECONOCIMIENTO - NO COMERCIAL - SIN OBRA DERIVADA
(CC BY-NC-ND)

VIVIAN CANARIO ROBLES.docx

INFORME DE ORIGINALIDAD

15%	14%	5%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	3%
2	repositorio.unsch.edu.pe Fuente de Internet	1%
3	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	1%
4	repositorio.ucv.edu.pe Fuente de Internet	1%
5	www.coursehero.com Fuente de Internet	1%
6	alicia.concytec.gob.pe Fuente de Internet	<1%
7	qdoc.tips Fuente de Internet	<1%
8	repositorio.upla.edu.pe Fuente de Internet	<1%

Universidad Nacional
Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

LA PRUEBA DIGITAL Y SU INFLUENCIA EN EL DELITO DE FRAUDE INFORMÁTICO EN LA FISCALÍA PENAL PROVINCIAL DE LIMA NORTE, 2024

Línea de Investigación:
Procesos jurídicos y resolución de conflictos
Tesis para optar el Título Profesional de Abogada

Autor(a)
Canario Robles, Vivian Lizeth

Asesor(a)
Ambrosio Bejarano, Hugo Ramiro
(ORCID: Código 0000-0003-3796-2580)

Jurado
Gonzales Loli, Martha Rocio
Moscoso Torres, Víctor Juber
Sarmiento Albacetti, Gladys Yolanda

Lima – Perú
2026

DEDICATORIA

Esta tesis está dedicada:

A mis amados padres, su amor incondicional ha sido la fuerza motriz de mi formación y desarrollo. Más que palabras, su vida ha sido la mejor enseñanza, mostrándome con ejemplo el poder del esfuerzo constante y la importancia de la perseverancia. Sus valores de humildad y honestidad son el cimiento moral que me permite hoy alcanzar esta meta profesional.

AGRADECIMIENTO

Mi gratitud a Dios, por ser la luz en el camino, mi guía constante y por haberme concedido la sabiduría y fortaleza necesarias para completar esta etapa.

A mis padres, por su amor inagotable, el inestimable ejemplo de esfuerzo que me inspira y motiva a diario. Este logro es, en gran medida, fruto de su sacrificio y apoyo. Siguiendo la misma línea, a mi hermano César, por ser un motor que constantemente me impulsa a cumplir mis metas y proyectos académicos.

A mi compañero incondicional, gracias por la paciencia demostrada a lo largo de este proceso y por brindarme esa calma tan necesaria que siempre me ayuda a seguir adelante. Seguido también a mis mejores amigas, por su compañía leal y el apoyo constante que me ofrecieron en cada momento.

En el ámbito académico, al Dr. Hugo Ambrosio, mi asesor, mi más sincero agradecimiento por su orientación profesional, su invaluable aporte académico. Su acompañamiento y dirección fueron absolutamente fundamentales para la culminación exitosa de esta tesis.

A las personas entrevistadas, extiendo mi reconocimiento por su tiempo valioso y su generosidad al compartir sus conocimientos y experiencias, lo cual enriqueció significativamente esta investigación.

Finalmente, a Dom, mi compañero de desvelos, por su silenciosa y fiel compañía durante cada madrugada de trabajo.

Con todo mi corazón, gracias eternas a cada uno de ustedes.

ÍNDICE

RESUMEN

La presente investigación tuvo como finalidad analizar la influencia de la prueba digital en la investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024. En un contexto de creciente incidencia de delitos informáticos, resultó pertinente examinar cómo la prueba digital era recabada, gestionada y valorada en el proceso penal, y qué impacto podía tener en la determinación de responsabilidades. Para tal efecto, se planteó un enfoque cualitativo, de nivel descriptivo aplicando el método deductivo, empleando como técnicas la revisión documental de carpetas fiscales y la realización de entrevistas a fiscales expertos en materia de derecho penal. Se previó que esta investigación permitiría identificar las principales limitaciones normativas, tecnológicas e institucionales que enfrentan los operadores jurídicos al momento de incorporar y valorar prueba digital en casos de fraude informático. Asimismo, se proyectó que los hallazgos contribuirían a proponer recomendaciones orientadas a optimizar la actuación fiscal en delitos de naturaleza digital, fortaleciendo con ello la eficacia del sistema de administración de justicia penal frente a la criminalidad tecnológica.

Palabras clave: Prueba digital, fraude informático, delitos informáticos y valoración probatoria.

ABSTRACT

This research aimed to analyze the influence of digital evidence in the investigation of the crime of computer fraud at the Provincial Criminal Prosecutor's Office of Lima Norte during the year 2024. In a context of increasing cybercrime, it was relevant to examine how digital evidence was collected, managed, and assessed within the criminal process, and what impact it could have on the determination of criminal responsibility. To achieve this objective, a qualitative, descriptive, and analytical approach was proposed, using documentary review of prosecutorial case files and interviews with prosecutors. It was anticipated that this research would help identify the main normative, technological, and institutional limitations faced by legal operators when incorporating and evaluating digital evidence in cases of computer fraud. Likewise, the findings were expected to contribute to the development of recommendations aimed at improving prosecutorial performance in digital crimes, thereby strengthening the effectiveness of the criminal justice system in the face of technological crime.

Keywords: Digital evidence, computer fraud, computer crimes and evidentiary assessment.

I. INTRODUCCIÓN

El avance imparable de las tecnologías de la información ha generado profundas transformaciones en la forma en que las personas se relacionan, compran, trabajan e incluso cometen delitos. El uso masivo de la tecnología ha traído consigo una nueva clase de criminalidad: los delitos informáticos. En ese contexto, el fraude informático ha cobrado especial relevancia, al convertirse en una de las modalidades más frecuentes de ataque contra el patrimonio de los ciudadanos, generando no solo pérdidas económicas, sino también desconfianza en el sistema de justicia penal.

Frente a esta realidad, la prueba digital juega un rol fundamental en la investigación y sanción de estos delitos. Esta prueba, que puede presentarse en forma de correos electrónicos, registros de transferencia bancaria, mensajes, IPs o capturas digitales, se convierte en un instrumento clave para identificar a los responsables y sustentar la responsabilidad penal. Sin embargo, su obtención, conservación y valoración presentan dificultades técnicas y jurídicas que muchas veces impiden que el Ministerio Público pueda desarrollar una investigación eficaz.

En respuesta a estos desafíos, el legislador peruano ha introducido recientemente la Ley N.º 32314, promulgada en abril de 2025, la cual modifica el Código Penal y la Ley de Delitos Informáticos. Esta norma incorpora agravantes específicas para los delitos cometidos mediante el uso de inteligencia artificial, como el fraude informático, lo que refuerza el marco sancionador frente a la criminalidad tecnológica. Además, pone de relieve la importancia de fortalecer el tratamiento de la prueba digital, dado que su adecuada autenticación, custodia y valoración se vuelve indispensable para aplicar con eficacia las nuevas disposiciones penales.

Particularmente en la Fiscalía Penal Provincial de Lima Norte, se ha observado que los casos de fraude informático aumentan año tras año, pero gran parte de ellos no llegan a una sentencia condenatoria. Esto no solo se debe a la complejidad del delito, sino también a la

forma en que se maneja la prueba digital: falta de capacitación, escasa infraestructura tecnológica, dificultad para rastrear a los autores y los plazos procesales que terminan archivando los casos. En muchos procesos, la prueba digital no logra cumplir su función probatoria, y esto afecta directamente el resultado del proceso penal.

Por ello, esta investigación busca analizar cómo influye la prueba digital en el desarrollo de las investigaciones fiscales en los casos de fraude informático, específicamente en la Fiscalía Penal Provincial de Lima Norte. Se pretende identificar las principales debilidades en su uso, así como su impacto en la determinación de responsabilidad penal. Este análisis resulta necesario si se quiere avanzar hacia una persecución penal más eficiente, adaptada a los desafíos que plantea el entorno digital actual.

1.1. **Descripción y formulación del problema**

1.1.1. ***Descripción del problema***

El delito de fraude informático se ha convertido en una de las principales amenazas dentro del mundo digital, especialmente desde el incremento del uso de medios electrónicos para realizar operaciones bancarias, compras en línea y otras transacciones cotidianas. En nuestro país, esta modalidad delictiva ha ido creciendo a un ritmo acelerado, afectando el patrimonio de miles de ciudadanos y poniendo en evidencia los desafíos que enfrenta el sistema penal para investigar y sancionar adecuadamente este tipo de hechos.

En respuesta a esta situación, en el Perú se evidenció la necesidad de regular normativamente el delito de fraude informático mediante la Ley N.° 30096, posteriormente reemplazada por la Ley N.° 30171. Esta norma establece en su artículo 8° el marco penal para el delito de fraude informático. Además, en el año 2019, el Estado peruano suscribió y ratificó el Convenio de Budapest, principal instrumento internacional contra la ciberdelincuencia. A través de dicho convenio, el país se comprometió a combatir este tipo de flagelo delictivo y enfrentar las amenazas cibernéticas en colaboración con otras naciones. No obstante, estos

compromisos no se implementaron de manera eficiente, en parte debido a los efectos de la pandemia, lo que evidenció serias deficiencias en la actuación del Ministerio Público como entidad encargada de investigar y conducir diligencias frente a este tipo de delitos.

En un esfuerzo más reciente por reforzar la respuesta penal frente a esta problemática, se promulgó la Ley N.° 32314 en abril de 2025, que modificó el Código Penal y la Ley N.° 30096, incorporando agravantes específicas para los delitos cometidos mediante el uso de inteligencia artificial, como el fraude informático. Esta norma representa un avance normativo relevante, pero su sola existencia no ha sido suficiente para garantizar una aplicación práctica efectiva, especialmente en la gestión de la prueba digital durante las investigaciones fiscales.

La prueba digital se ha vuelto un elemento clave para el éxito o fracaso de una investigación penal. Sin embargo, su uso en los procesos fiscales no siempre es efectivo. La realidad muestra que muchos casos de fraude informático son archivados no porque no haya delito, sino porque no se logra recolectar y presentar adecuadamente la prueba digital. Esta situación se debe, entre otras razones, a la falta de personal especializado, a la limitada disponibilidad de herramientas tecnológicas, y al poco conocimiento técnico sobre cómo actuar frente a este tipo de evidencias.

Cabe señalar que, según la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (El Peruano, 2021), entre enero y abril de 2021 se registraron 1,188 denuncias relacionadas con delitos informáticos, siendo el fraude informático y la suplantación de identidad los más frecuentes. Las modalidades más comunes fueron la clonación de tarjetas y las compras fraudulentas por internet. Asimismo, destacó el uso del phishing, técnica que consiste en engañar a los usuarios mediante páginas web falsas que simulan ser bancos, logrando así que las víctimas ingresen sus datos personales, los cuales luego son usados por los delincuentes para realizar transacciones ilegales.

En el caso específico de la Fiscalía Penal Provincial de Lima Norte, las estadísticas

revelan un aumento constante de denuncias por fraude informático. No obstante, el número de casos que concluyen con una sentencia condenatoria es muy bajo. Esto genera frustración e inseguridad en las víctimas, quienes muchas veces desisten del proceso al ver que no hay una respuesta eficiente por parte del sistema de justicia.

Además, se ha identificado que muchos fiscales enfrentan dificultades para incorporar la prueba digital de manera adecuada dentro de la carpeta fiscal. A veces no se solicitan las pericias informáticas necesarias, no se preservan los datos desde el primer momento, o simplemente no se logra identificar al autor debido al anonimato que permite el entorno digital.

Al respecto, el artículo 159° de la Constitución Política del Perú establece que el Ministerio Público es el titular de la acción penal y defensor de la legalidad. Asimismo, el artículo 80-B de su Ley Orgánica —incorporado mediante el Decreto Legislativo N.° 52— permite la delegación de fiscales especializados en delitos informáticos, precisamente porque en muchos casos los operadores de justicia no contaban con medios de prueba idóneos ni con las herramientas necesarias para sustentar el proceso penal en estos casos.

Como medida frente a este panorama, el Ministerio Público emitió las Resoluciones N.° 1025-2020-MP-FN y N.° 1194-2020-MP-FN, los días 18 de septiembre y 30 de octubre de 2020, respectivamente, a través de las cuales se creó la Fiscalía Especializada en Ciberdelito. Esta iniciativa busca mejorar la capacidad de investigación y promover la cooperación internacional, de modo que las investigaciones puedan realizarse con mayores estándares de eficiencia, tanto en la recolección de pruebas como en la identificación de los responsables.

Por todo ello, es importante preguntarse si el uso actual de la prueba digital está siendo realmente útil para esclarecer los hechos y determinar responsabilidades penales. Este problema no solo tiene un impacto procesal, sino también social, ya que la falta de sanción en este tipo de delitos alimenta la sensación de impunidad y pone en duda la capacidad del sistema penal para adaptarse a los desafíos de la era digital.

1.1.2. Formulación del problema

1.1.2.1. Problema general

¿De qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024?

1.1.2.2. Problemas específicos

P.E.1. ¿Cómo se incorpora la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte en 2024?

P.E.2. ¿Cuáles son los factores que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal por delitos de fraude informático?

1.2. Antecedentes

1.2.1. Antecedentes nacionales

Salas y Romero (2024), en su investigación titulada "La demostración de evidencia digital en delitos de fraude cibernético en Lima Norte, Perú", realizada en la Universidad Tecnológica del Perú (UTP), tuvieron como finalidad cómo determinar la evidencia de datos digitales de Fraude Cibernético previstos en el proceso penal en Lima Norte. Se trató de un estudio cualitativo con diseño fenomenológico, aplicando entrevistas a abogados penalistas, fiscales, miembros de la policía especializados en delitos informáticos y peritos informáticos. Como resultado, identificaron que la evidencia digital solo logra eficacia procesal cuando es obtenida mediante pericia técnica especializada y sometida a criterios de utilidad, pertinencia y conducencia. Concluyeron que la ausencia de lineamientos uniformes y la limitada capacitación fiscal obstaculizan su adecuada valoración judicial.

Estrada (2024), en su artículo titulado "La impunidad en los delitos informáticos: una problemática de poco interés para legisladores, jueces y fiscales", publicado en la revista Ius Vocatio de la Corte Superior de Justicia de Huánuco, buscó examinar las causas institucionales de la alta tasa de impunidad en casos de ciberdelincuencia. Empleó un enfoque jurídico-

analítico, centrado en el rol del Ministerio Público. Se evidenció que la falta de capacitación técnica, la escasa especialización y la deficiente labor pericial dificultan la identificación de los responsables, lo que conlleva el archivamiento de los casos. El autor concluyó que, sin una respuesta institucional seria, los delitos informáticos seguirán sin recibir sanción efectiva.

Portugal (2024), en su tesis denominada "Delitos informáticos y la evidencia digital en el proceso penal peruano 2023", elaborada en la Universidad Privada San Carlos (UPSC), tuvo como propósito determinar la manera en que la evidencia digital incide en el desarrollo del proceso penal. La investigación fue de tipo jurídico descriptivo, con enfoque cualitativo y diseño transversal, aplicada a una muestra conformada por efectivos policiales del área de Investigación Criminal AREINCRI PNP. Los resultados reflejaron que, si bien la prueba digital es formalmente admisible, su eficacia probatoria depende en gran medida del modo en que se recolecta, presenta y preserva.

Gallegos (2022), en su estudio titulado "La Evidencia Digital y los Delitos Informáticos en el Sistema Jurídico Peruano, 2020", elaborado en la Universidad Peruana de la Américas, tuvo como finalidad presentar las condiciones que se deben tomar en cuenta en la revisión de las pruebas digitales y cómo se deben utilizar en los procedimientos judiciales. Como hallazgo principal, se determinó que se debería realizar la creación de un cuerpo normativo específico, contratar profesional capacitado con relación a los delitos informáticos ocurridos en el Perú. Concluyó que el tratamiento jurídico procesal de la evidencia digital influye significativamente en los delitos informáticos en el Sistema Jurídico Peruano.

Neyra (2024), en su trabajo de investigación titulada "Temas de razonamiento probatorio penal: La práctica y valoración de la prueba digital en el proceso penal peruano", elaborada en la Universidad San Martín de Porres, tuvo por objetivo delimitar el concepto, fuentes y características de la prueba digital y fijar criterios de admisibilidad y valoración bajo el art. 158 CPP (autenticidad, integridad, licitud y valoración conjunta), destacando los desafíos

de obtención frente a derechos fundamentales (secreto de comunicaciones, datos personales). Concluye que la incorporación de prueba digital es indispensable en un contexto de creciente cibercriminalidad, pero su eficacia probatoria exige que sea obtenida lícitamente y valorada conforme a sana crítica, con verificación técnica (hash, metadatos) y apoyo de peritaje informático para resolver dudas de autenticidad e integridad. Finalmente, recomienda adoptar protocolos claros de recolección y cadena de custodia digital, exigir autorización judicial cuando corresponda, y capacitar a jueces y fiscales en tecnologías forenses para asegurar decisiones fundadas y respetuosas de derechos

1.2.2. Antecedentes internacionales

Mendoza (2024), en su tesis titulada "Interpretación y desafíos de la Evidencia Digital en la Investigación criminal", desarrollada en el Instituto Universitario Argos, tuvo como propósito examinar cómo la aparición de tecnologías como la inteligencia artificial afecta la cadena de custodia y la fiabilidad de la prueba digital. La investigación fue de tipo exploratoria, con análisis doctrinario y casuístico. Se concluyó que los sistemas de justicia penal deben adaptarse no solo normativamente, sino también pericial y éticamente frente a esta nueva forma de evidencia.

Betrán (2024), en su tesis titulada "La valoración de la prueba digital en un caso de delito de coacciones en el ámbito de la violencia de género, de acoso, de vejaciones leves y revelación de secretos", elaborada en la Universidad Zaragoza (España), tuvo como finalidad examinar la compatibilidad de la prueba digital con las garantías del debido proceso penal. La investigación fue de tipo jurídico-dogmático, utilizando análisis de casos y legislación. Se concluyó que la admisión de pruebas electrónicas depende de una cadena de custodia rigurosa y de peritajes técnicos especializados, sin los cuales se compromete la validez del proceso.

Fernandes (2019), en su tesis titulada "A problemática da utilização da prova digital no processo penal brasileiro diante da ausência de regulamentação" ("El problema del uso de la

prueba digital en el proceso penal brasileño ante la falta de regulación"), defendida en la Universidade Federal de Santa Catarina (Brasil), buscó identificar las barreras institucionales que enfrenta el sistema penal brasileño para actuar en casos de fraude informático. El estudio fue cualitativo, con entrevistas a fiscales y revisión de expedientes. Se evidenció que el déficit en laboratorios forenses digitales y la escasa capacitación afectan negativamente la persecución penal. Se concluyó que la actualización normativa debe ir acompañada de inversión en capacidades operativas.

Solanke (2022), en su investigación titulada "Digital forensics AI: On practicality, optimality, and interpretability of digital evidence mining techniques" ("IA forense digital: sobre la practicidad, la optimización y la interpretabilidad de las técnicas de minería de evidencia digital"), presentada en la Universidad de Luxemburgo, tuvo como objetivo analizar el tratamiento que recibe la prueba digital en el sistema acusatorio penal. Se concluyó que, pese a avances legislativos, existen criterios dispares entre jueces respecto a la admisibilidad y valoración de evidencia electrónica.

Porras (2023), en su tesis de especialización en Derecho Procesal Penal "La incorporación de la Prueba Digital en el Proceso Penal Colombiano", publicado en la universidad Libre-Seccional Bogotá, en la cual analizó que aunque exista regulación sobre medios tecnológicos, falta un procedimiento claro para incorporar la prueba digital, y eso puede hacer que no se valore adecuadamente en juicio.

1.3. Objetivos

1.3.1. Objetivo General

Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1.3.2. Objetivos Específicos

O.E.1. Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte.

O.E.2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal.

1.4 Justificación

1.4.1 Justificación de teórica

La presente investigación busca aportar al desarrollo doctrinario y normativo del Derecho Penal y Procesal Penal en el ámbito de los delitos informáticos, específicamente respecto al uso de la prueba digital como medio de convicción. Si bien en el ordenamiento jurídico peruano se han aprobado normas orientadas a sancionar este tipo de conductas, aún existen vacíos sobre el tratamiento adecuado de la evidencia digital dentro de las etapas del proceso penal. Este estudio contribuye a la comprensión de dichas deficiencias, analizando cómo la prueba digital influye en la eficacia del proceso de investigación, desde una perspectiva jurídica que articula doctrina, jurisprudencia y práctica fiscal.

1.4.2 Justificación práctica

En la práctica, los operadores de justicia, especialmente los fiscales, enfrentan serias dificultades para recolectar, conservar e incorporar la prueba digital en las carpetas fiscales de delitos informáticos. Esta situación afecta directamente la posibilidad de obtener sentencias condenatorias y deja muchos casos en situación de archivo. Este estudio permite visibilizar estas limitaciones dentro de la Fiscalía Penal Provincial de Lima Norte, identificando los principales obstáculos que enfrentan los fiscales en la etapa preliminar del proceso penal. Con ello, se pretende aportar insumos que puedan ser considerados para fortalecer la actuación del Ministerio Público frente a estos delitos de alta complejidad tecnológica.

1.4.3 Justificación metodológica

Desde el punto de vista metodológico, esta investigación adopta un enfoque cualitativo y descriptivo, basado en entrevistas a fiscales y operadores jurídicos vinculados a la investigación de delitos informáticos. La selección de este enfoque se justifica por la necesidad de obtener una comprensión profunda del fenómeno desde la experiencia práctica de quienes aplican la norma.

Además, el estudio puede servir como antecedente metodológico para futuras investigaciones académicas que aborden temas relacionados con la cibercriminalidad, la prueba digital o el fortalecimiento de las capacidades institucionales en el sistema penal.

1.4.4 Justificación social

El incremento sostenido de los delitos de fraude informático en el Perú afecta no solo a personas naturales, sino también a empresas, instituciones públicas y al sistema financiero en general. La falta de una respuesta penal efectiva alimenta la impunidad y disminuye la confianza ciudadana en las instituciones de justicia. Por ello, este trabajo cobra relevancia social, al proponer una reflexión crítica sobre el rol que debe cumplir la prueba digital en la lucha contra la ciberdelincuencia, y cómo su tratamiento adecuado puede contribuir a una mayor protección del patrimonio y los derechos fundamentales de los ciudadanos.

II. MARCO TEÓRICO

2.1. La prueba en el Proceso Penal

2.1.1. Concepto y finalidad de la prueba

La prueba constituye un elemento esencial en el proceso penal, dado que permite comprobar la existencia del hecho delictivo y la responsabilidad penal del imputado. Según Devis (2012), la prueba es el instrumento por el cual se busca la verdad en el proceso penal, debiendo siempre observarse diversos principios fundamentales:

- Legalidad: toda actividad probatoria debe estar permitida por la ley procesal; no se admite prueba obtenida o practicada en contravención al ordenamiento jurídico.
- Contradicción: implica que ambas partes del proceso deben tener la oportunidad de conocer, objetar y contradecir las pruebas propuestas por la contraparte, asegurando el debate probatorio.
- Pertinencia: la prueba debe estar directamente relacionada con los hechos controvertidos y relevantes del proceso, evitando así actuaciones superfluas.
- Utilidad: la prueba debe ser idónea para contribuir al esclarecimiento de los hechos, es decir, debe tener una finalidad práctica en la reconstrucción del delito.
- Inmediación: el juez debe estar presente en la práctica de la prueba, para valorarla de manera directa y personal, sin intermediarios.

La carga de la prueba recae en el Ministerio Público, quien debe demostrar la culpabilidad del imputado más allá de toda duda razonable, respetando los principios antes descritos como garantía de un debido proceso (Devis, 2012).

En la doctrina, Aragoneses et al. (2003) señala que la actividad probatoria se orienta a la reconstrucción de los hechos con base en las pruebas disponibles, siendo fundamental el respeto al principio de presunción de inocencia y a los derechos fundamentales del imputado.

En ese sentido, la carga de la prueba en el proceso penal recae principalmente en el Ministerio Público, como ente acusador, quien debe probar los hechos constitutivos de delito y la responsabilidad del imputado. Este principio se vincula directamente con la garantía de la presunción de inocencia, en tanto que el imputado no tiene obligación de probar su inocencia, y solo será considerado culpable cuando existan pruebas suficientes y válidas que así lo acrediten. Aragoneses subraya que esta distribución de la carga probatoria es esencial para el equilibrio del proceso penal, ya que impide la inversión injustificada de dicha carga y refuerza el rol pasivo del imputado durante la fase probatoria, salvo que este decida ejercer su derecho de defensa activa.

2.2. La prueba digital o electrónica

2.2.1. Concepto de prueba digital

La prueba digital comprende toda información con valor probatorio contenida, transmitida o almacenada en formato electrónico. Incluye correos electrónicos, archivos digitales, registros de navegación, imágenes, mensajes en redes sociales, entre otros. Para Sanz-Magallón (2018), la prueba electrónica/digital responde a la realidad tecnológica actual y, ante la falta de regulación específica, exige aplicar por analogía las reglas de los medios probatorios tradicionales, junto con criterios técnicos y jurisprudenciales para su correcta valoración.

Además, esta prueba plantea nuevos retos para el sistema penal, especialmente en lo relativo a la autenticación, la integridad de los datos y la cadena de custodia. Como sostiene Delgado (2013), la naturaleza intangible de la prueba digital y su dependencia de tecnologías específicas obliga a jueces, fiscales y abogados a capacitarse en aspectos técnicos para una correcta valoración probatoria. Por ello, la prueba digital no solo es un nuevo tipo de evidencia, sino también una transformación del paradigma probatorio tradicional, que requiere una adaptación normativa y práctica para garantizar su eficacia y legalidad en el proceso penal.

2.2.2. Clasificación de la prueba digital

La doctrina la clasifica en documental (archivos, capturas de pantalla), testimonial (declaraciones sobre uso de tecnologías) y técnica (informes periciales informáticos). Según Silva (2019), la clasificación permite delimitar la función de cada tipo de prueba digital en el proceso penal, y valorar su eficacia probatoria de manera diferenciada.

La prueba documental se refiere a todo contenido electrónico que pueda imprimirse o visualizarse como evidencia directa de un hecho, como correos electrónicos, mensajes de texto, archivos PDF o imágenes capturadas. La prueba testimonial incluye los relatos de testigos que hayan tenido contacto o conocimiento sobre el uso de herramientas tecnológicas vinculadas al delito. Finalmente, la prueba técnica o pericial involucra el análisis especializado de dispositivos electrónicos, software, redes y registros digitales por parte de peritos en informática forense.

2.2.3. Características

La evidencia digital se caracteriza por su inmaterialidad, su fragilidad o volatilidad (puede alterarse o perderse con facilidad), la dependencia de herramientas y conocimientos técnicos para su recuperación e interpretación, y la trazabilidad (posibilidad de reconstruir su origen y el historial de accesos o cambios). Estas notas explican por qué su tratamiento no puede ser improvisado: requiere procedimientos estandarizados de recojo, preservación y análisis que aseguren integridad y autenticidad, condiciones necesarias para que pueda ser valorada válidamente en el proceso penal. En el Perú, ello se conecta con la cadena de custodia y con el deber de garantizar la autenticidad de lo incautado, previsto en el artículo 220.5 del Código Procesal Penal, y desarrollado mediante normativa del Ministerio Público y lineamientos técnicos aplicables a evidencia digital.

La inmaterialidad supone que el contenido probatorio no “existe” como un objeto físico independiente, sino que se encuentra alojado en dispositivos, sistemas o servicios, por lo que su obtención exige métodos que permitan capturarlo sin comprometer su fiabilidad. A su vez, la volatilidad implica que la información puede modificarse por acciones mínimas —o incluso por el funcionamiento ordinario del sistema—, de manera que cualquier intervención debe realizarse con precauciones forenses y dejando constancia de cada actuación relevante.

Por otro lado, la necesidad de herramientas técnicas se explica porque los datos pueden encontrarse cifrados, comprimidos o en formatos no legibles sin software especializado, lo que vuelve frecuente la intervención pericial y el uso de procedimientos forenses para adquisición, examen y análisis. En esa línea, el Ministerio Público cuenta con una Guía de Análisis Digital Forense, que establece fases de trabajo y buenas prácticas para el tratamiento de indicios digitales.

Finalmente, la trazabilidad exige que toda actuación sea registrable y verificable: quién accedió, cuándo, cómo se realizó la extracción o copia, y qué medidas de control se aplicaron. Estos registros (actas, formatos y bitácoras/audit trail) permiten controlar la cadena de custodia y reforzar la credibilidad de la evidencia al hacer posible su revisión posterior.

Estas características, en conjunto, justifican un tratamiento técnico y normativo diferenciado para la prueba digital dentro del proceso penal.

2.2.4. Diferencias entre prueba tradicional y digital

A diferencia de la prueba física, la digital requiere técnicas especializadas para su recolección, preservación, análisis y presentación, a fin de garantizar su autenticidad e integridad. De acuerdo con Delgado (2013), la diferencia radica no solo en el soporte, sino en la metodología de actuación procesal.

Por ejemplo, en el caso de un contrato impreso en papel (prueba física), basta su presentación en juicio para acreditar un acto jurídico. Sin embargo, si dicho contrato fue

firmado digitalmente y enviado por correo electrónico, se requerirá una verificación de su validez mediante certificados digitales, metadatos del correo, y posiblemente un peritaje técnico que confirme su integridad y origen. Este ejemplo evidencia que el juez no solo debe valorar el contenido, sino también el medio y las condiciones en que fue producido, lo que representa un cambio fundamental en el tratamiento probatorio.

2.3. Valoración de la prueba digital

2.3.1. Admisibilidad y validez en el proceso penal

La prueba digital es admisible siempre que se garantice su obtención legal, su integridad y autenticidad. En el Perú, el artículo VII del Título Preliminar del Código Procesal Penal establece la validez de la prueba obtenida por medios técnicos, siempre que se respete el debido proceso. Según Vázquez (2018), el principio de licitud se proyecta con especial rigor sobre las pruebas digitales, dada su facilidad de manipulación.

En esta línea, la jurisprudencia nacional e internacional ha insistido en que la admisión de pruebas digitales requiere no solo que estas hayan sido recolectadas de manera legal, sino también que se haya preservado adecuadamente su cadena de custodia. La admisibilidad implica también que la prueba sea pertinente, útil y no vulneradora de derechos fundamentales, como el derecho a la intimidad o al secreto de las comunicaciones.

Por ejemplo, en el caso de una conversación obtenida de una aplicación de mensajería, será admisible si se ha recolectado con autorización judicial, o si ha sido voluntariamente proporcionada por una de las partes, siempre que se garantice su autenticidad e integridad mediante peritaje. Caso contrario, podría ser excluida como prueba ilícita conforme al artículo 159 del mismo cuerpo normativo.

Así, la admisibilidad de la prueba digital requiere un doble control: legal (sobre su obtención) y técnico (sobre su autenticidad), siendo ambos aspectos fundamentales para garantizar un proceso penal justo y respetuoso de los derechos humanos.

2.3.2. Criterios jurisprudenciales

Jurisprudencia relevante

En el caso Casación N.º 1675-2021/Lima, la Corte Suprema reconoció la validez de pruebas electrónicas obtenidas con orden judicial y peritaje técnico, destacando la importancia de la cadena de custodia digital. Esta decisión refuerza la posición jurisprudencial que exige el cumplimiento estricto de los principios de legalidad y autenticidad en la incorporación de evidencia digital en el proceso penal.

La Corte Suprema señaló que para que una prueba digital sea válida, debe demostrarse su obtención lícita, la ausencia de manipulación, y su relevancia para el caso concreto. La decisión también hizo énfasis en la necesidad de contar con peritos especializados que expliquen al juzgador el contenido técnico de la evidencia, a fin de que esta pueda ser valorada correctamente dentro del juicio oral.

Asimismo, se alinea con el criterio del Tribunal Europeo de Derechos Humanos en casos como Bykov (2009), donde se establece que la admisión de evidencia digital debe cumplir con garantías judiciales mínimas para preservar los derechos del imputado.

El Convenio de Budapest (2001) establece directrices para la cooperación internacional en materia de ciberdelincuencia y prevé facultades procesales para la preservación y obtención de evidencia digital. Mengoa (2021) señala que estas reglas resultan relevantes para la investigación de delitos como el fraude informático, en tanto promueven mecanismos de

actuación y cooperación para asegurar información digital (por ejemplo, preservación rápida de datos y requerimientos de información), bajo criterios de legalidad y garantías.

2.4. Delitos Informáticos: Enfoque Penal

2.4.1. Concepto de ciberdelito

Los delitos informáticos son aquellos actos ilícitos cometidos mediante sistemas informáticos o dirigidos contra estos. Téllez (2003) define los delitos informáticos como “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin”.

Por su parte, Silva (2019) señala que los delitos informáticos surgen como respuesta a la expansión de las nuevas tecnologías y la creciente dependencia de la sociedad de los sistemas de información, lo que ha generado nuevas formas de lesionar bienes jurídicos tradicionales, como el patrimonio, la intimidad o la propiedad. Asimismo, Orrego (2019) enfatiza que este tipo de delitos se caracteriza por la volatilidad de sus rastros, la dificultad de atribuir responsabilidad penal directa y la necesidad de adaptación de los marcos legales tradicionales a nuevas formas de criminalidad.

2.4.2. Clasificación

Se dividen en dos grandes grupos: i) delitos contra los sistemas (acceso indebido, sabotaje informático), y ii) delitos mediante sistemas (fraude informático, pornografía infantil, estafa electrónica). La doctrina penal contemporánea subraya esta clasificación para efectos dogmáticos y procesales (Silva, 2019).

Los delitos contra los sistemas comprenden aquellos actos dirigidos a vulnerar la integridad, disponibilidad o confidencialidad de los sistemas informáticos o de los datos que contienen. Un ejemplo típico es el "hacking", es decir, el acceso ilícito a un sistema informático protegido, lo cual puede implicar la obtención de información confidencial o el control total del sistema. También se incluye el sabotaje informático, consistente en la destrucción o

alteración maliciosa de datos, redes o servicios digitales. Asimismo, la interceptación ilegal de datos durante su transmisión, mediante programas como "sniffers" o el uso no autorizado de redes, también entra en esta categoría.

Por otro lado, los delitos mediante sistemas se refieren a aquellos en los que las tecnologías de la información y comunicación son utilizadas como medio para cometer ilícitos tradicionales. El fraude informático, por ejemplo, puede realizarse a través de la manipulación de sistemas de banca electrónica para desviar fondos o generar operaciones falsas. La pornografía infantil digital implica la producción, almacenamiento o difusión de contenido ilegal por medios informáticos, mientras que la estafa electrónica incluye prácticas como el phishing o el envío masivo de mensajes falsos para obtener datos personales.

Esta distinción permite no solo una mejor comprensión del fenómeno delictivo, sino también una correcta formulación de estrategias investigativas, tipificación penal y selección de herramientas probatorias digitales (Sanz-Magallón 2018).

2.4.3. Regulación de los delitos informáticos en el Perú (Ley N° 30096)

Ley de Delitos Informáticos - tipifica diversas conductas como el acceso ilícito, interceptación de datos, falsificación informática y fraude informático, adaptándose a estándares internacionales como el Convenio de Budapest. Esta norma fue promulgada en 2013 y ha sido complementada por otras disposiciones del Código Penal y del Código Procesal Penal, que reconocen la validez y eficacia de la prueba digital en la persecución penal.

Según Ramos (2015), esta normativa constituye un avance significativo en la lucha contra la criminalidad digital, pues establece tipos penales específicos que antes carecían de una regulación expresa. La ley también introduce figuras como la suplantación de identidad digital y el uso indebido de datos personales, los cuales responden a nuevas formas de afectación de derechos fundamentales en el entorno virtual.

Orrego (2019) sostiene que esta ley, aunque valiosa, debe ser parte de un sistema integral que contemple capacitación técnica para los operadores de justicia, infraestructura tecnológica adecuada y cooperación internacional efectiva, sin los cuales la eficacia de las normas se ve severamente limitada.

Asimismo, el Decreto Legislativo N.º 1182, que regula el acceso a datos de geolocalización en tiempo real por parte del Ministerio Público, complementa el marco jurídico para la investigación de delitos informáticos y refleja un esfuerzo por equilibrar eficacia investigativa con respeto a los derechos fundamentales.

2.5. Delitos de Fraude Informático

2.5.1. Definición legal y elementos del tipo penal

El artículo 8 de la Ley N.º 30096 define el fraude informático como el acto de manipular indebidamente sistemas informáticos o datos con la finalidad de obtener un beneficio económico ilegítimo. Se trata de un delito de resultado, cuya configuración exige la afectación patrimonial de la víctima.

Doctrinariamente, Silva (2019) considera que el fraude informático representa una evolución del delito tradicional de estafa, en el que desaparece el contacto humano directo y se sustituye por la interacción con sistemas digitales, lo que complica la identificación del autor y la trazabilidad de la conducta. Asimismo, Ramos (2015) resalta que este delito se caracteriza por la utilización de conocimientos técnicos para vulnerar la seguridad informática de entidades bancarias, comerciales o gubernamentales.

La manipulación puede adoptar múltiples formas, como el ingreso de instrucciones maliciosas en sistemas automatizados de transferencias, el acceso indebido a bases de datos para alterar saldos financieros, o la utilización de técnicas como el phishing para captar credenciales de usuarios y desviar fondos. Estas conductas, aunque puedan parecer simples desde una perspectiva técnica, implican una compleja afectación jurídica al patrimonio, así

como la necesidad de desarrollar técnicas específicas de investigación y prueba, particularmente mediante evidencia digital.

Los elementos del tipo penal de fraude informático incluyen:

- Manipulación indebida: cualquier acción de alteración, interferencia, supresión o introducción de datos que afecte un sistema informático o base de datos.
- Finalidad de obtener un beneficio económico ilegítimo: debe existir una intención de lucro, directa o indirecta, a costa del patrimonio de otro.
- Resultado material: afectación patrimonial concreta, es decir, perjuicio económico para la víctima.
- Elemento subjetivo: dolo directo; el agente debe actuar con conocimiento de la ilicitud de su conducta y con intención de obtener el beneficio.

Estos elementos deben ser acreditados mediante medios probatorios válidos, preferentemente digitales, como registros de logs, evidencias extraídas de sistemas financieros o peritajes informáticos. Según Delgado (2013), la configuración típica del fraude informático exige una reconstrucción precisa del comportamiento digital del imputado, apoyada en una base tecnológica robusta y jurídicamente admisible.

2.5.2. Modalidades del fraude informático

Incluye el uso de programas maliciosos, suplantación de identidad, modificación de datos contables o bancarios, entre otros. Puede afectar tanto a entidades privadas como a instituciones públicas. Mendoza (2019) advierte que estas formas requieren pruebas eminentemente digitales para su persecución.

Entre las principales modalidades se encuentran:

- Uso de programas maliciosos (malware): como troyanos o keyloggers, que permiten el acceso remoto a sistemas informáticos para obtener contraseñas o información

financiera. Por ejemplo, un malware puede instalarse en la computadora de un trabajador bancario y capturar sus credenciales para realizar transferencias ilegales.

- Phishing o suplantación de identidad: se envían correos electrónicos fraudulentos que imitan a instituciones legítimas para obtener información confidencial del usuario, como datos de tarjetas de crédito. Este tipo de fraude se ha extendido ampliamente con la masificación del uso del correo electrónico y redes sociales.
- Modificación de datos contables o bancarios: ocurre cuando el delincuente accede a sistemas administrativos o financieros de una empresa y altera datos para desviar fondos. Por ejemplo, modificar el número de cuenta de un proveedor legítimo por una cuenta controlada por el autor del delito.
- Creación de sitios web falsos (spoofing): que simulan páginas reales de bancos u organismos del Estado para inducir al error al usuario y captar información personal y bancaria.

Estas conductas, en conjunto, conforman un repertorio complejo de mecanismos de fraude que dificultan su detección y persecución. Por ello, como subraya Delgado (2013), la investigación de estas modalidades requiere una pericia técnica avanzada y una legislación que permita adaptarse a la constante evolución de las herramientas informáticas empleadas por los delincuentes.

2.5.3. Diferencia con delitos tradicionales de estafa

A diferencia de la estafa, el fraude informático se ejecuta sin contacto directo con la víctima y a través de medios tecnológicos, lo cual complejiza la identificación del autor y la obtención de prueba. Según Silva (2019), esta diferencia justifica el tratamiento penal autónomo de los delitos informáticos.

En la estafa, el sujeto activo utiliza el engaño verbal o conductual frente a la víctima, logrando que esta, voluntariamente, entregue un bien patrimonial. En cambio, en el fraude

informático, el autor se vale de medios tecnológicos para inducir al error sin contacto personal, mediante software, correos falsos, suplantación de plataformas o manipulación de datos.

Por ejemplo, en una estafa tradicional un sujeto puede ofrecer un bien inexistente a la víctima mediante conversación directa y lograr que esta entregue dinero. En cambio, en el fraude informático, una persona puede suplantar la página web de una entidad bancaria y hacer que el usuario, sin saberlo, le proporcione sus datos de acceso, que luego serán usados para sustraer dinero de su cuenta.

Mendoza (2019) subraya que esa distancia entre autor y víctima, así como la mediación tecnológica, genera nuevas dificultades en la imputación penal, especialmente respecto a la identificación del agente, la determinación de su participación y la obtención de pruebas digitales válidas.

2.6. Actuación Fiscal en el delito de Fraude Informático

2.6.1. Funciones del Ministerio Público en la investigación penal

El fiscal es el encargado de dirigir la investigación. En delitos informáticos, su rol incluye solicitar peritajes técnicos, recopilar evidencia digital y formular cargos con base en pruebas válidas y verificables. Este tipo de delitos exige un enfoque técnico y especializado, ya que los medios tradicionales de investigación penal resultan insuficientes ante la complejidad del entorno digital.

Bernal (2017) resalta que la formación especializada del fiscal es clave para una investigación eficaz en delitos tecnológicos, pues debe entender cómo funcionan los sistemas informáticos, qué evidencias pueden extraerse y cómo preservarlas adecuadamente para que sean admisibles en juicio.

Por ejemplo, en casos de fraude informático, el fiscal debe saber interpretar los registros de logs, el tráfico de datos y los resultados del peritaje forense, además de valorar adecuadamente pruebas como direcciones IP, correos electrónicos o archivos digitales. Sin este

conocimiento técnico, corre el riesgo de formular acusaciones sin respaldo probatorio sólido, lo cual puede llevar al sobreseimiento o archivo del caso. En ese sentido, es indispensable que el Ministerio Público cuente con unidades especializadas y protocolos técnicos para la investigación de delitos informáticos, como parte de su obligación constitucional de perseguir el delito con eficiencia y legalidad.

2.6.2. Rol del fiscal en la valoración y presentación de prueba digital

La Fiscalía Penal Provincial de Lima Norte enfrenta limitaciones logísticas, escasez de especialistas en criminalidad digital, y deficiencias en la preservación de la cadena de custodia digital, lo cual puede afectar la calidad de la acusación. En palabras de Paredes (2020), estas carencias generan un alto índice de archivamiento de denuncias por delitos informáticos.

2.6.3. Dificultades prácticas y tecnológicas en el distrito fiscal de Lima Norte

La Fiscalía Penal Provincial de Lima Norte enfrenta diversas limitaciones que repercuten negativamente en la persecución de delitos informáticos:

Limitaciones logísticas y técnicas:

Existe escasez de equipos y software especializado (como herramientas forenses, sistemas de copias bit a bit y servicios de análisis log) que son indispensables para la investigación de evidencias digitales. Además, el acceso a laboratorios o centros técnicos suele ser lento o centralizado en Lima Metropolitana, lo que retrasa los procesos.

Escasez de personal especializado:

Muchos fiscales y personal de apoyo carecen de formación en criminalidad digital y metodologías forenses. Bernal (2017) señala que esta carencia limita la eficacia investigativa, pues tanto la recolección como la valoración de pruebas dependen de competencias técnicas que no siempre están disponibles.

Deficiencias en la preservación de la cadena de custodia digital:

Como señala Paredes (2020), la falta de protocolos claros y sistemáticos sobre registro de acceso, manipulación y generación de evidencias genera irregularidades que pueden invalidar pruebas en sede judicial.

Retrasos procesales:

Los retrasos para generar peritajes forenses —debido a la falta de equipos o peritos disponibles— provocan que procesos queden paralizados y que muchas investigaciones terminen archivadas por falta de respaldo técnico oportuno.

Coordinación institucional limitada:

La coordinación entre la fiscalía, la policía especializada en delitos informáticos y los peritos es débil o informal. Esto conlleva a que muchas evidencias no se recojan adecuadamente, o se documenten de forma incompleta.

Infraestructura y presupuesto insuficientes:

La asignación presupuestaria para la adquisición de tecnologías, capacitación y dotación de especialistas es insuficiente para atender la demanda creciente de casos digitales en Lima Norte.

Según Paredes (2020), esta situación no solo limita la obtención de justicia efectiva, sino que también desincentiva la denuncia de delitos informáticos, al generar la percepción de que no existirá una respuesta penal efectiva.

2.7. Relación entre prueba digital y Fraude informático

2.7.1. Necesidad de prueba digital para la persecución del fraude informático

El fraude informático se configura casi exclusivamente a través de rastros digitales. La prueba digital es, por tanto, la vía principal para acreditar el delito y vincular al imputado. Para Mendoza (2019), sin evidencia digital válida y admisible, la persecución penal de estos delitos se torna inviable.

La prueba digital permite reconstruir el modus operandi del autor, identificar dispositivos y cuentas electrónicas utilizadas, rastrear transacciones, analizar patrones de comportamiento y establecer vínculos entre el hecho delictivo y el presunto responsable.

Por ejemplo, en un caso de fraude por phishing, las evidencias pueden incluir los metadatos del correo engañoso, los datos del servidor donde se alojó la página falsa y los registros bancarios que evidencien el desvío de fondos. Toda esta información debe ser colectada mediante herramientas especializadas y con los cuidados técnicos adecuados, pues cualquier irregularidad podría afectar su validez procesal.

Autores como Delgado y también Silva coinciden en que la eficacia de la respuesta penal frente al fraude informático depende de la solidez de la prueba digital ofrecida. En consecuencia, su adecuada recolección, conservación, análisis y presentación se convierten en requisitos esenciales para lograr una imputación válida y una eventual condena penal.

2.7.2. Casuística sobre cómo influye la calidad o falta de prueba digital

Los problemas comunes en fiscalías como Lima Norte incluyen: la pérdida de información por falta de cadena de custodia, desconocimiento técnico de operadores jurídicos y ausencia de protocolos uniformes. Uno de los problemas más frecuentes es la recolección inadecuada de evidencia digital. Muchas veces los fiscales o policías incautan equipos informáticos sin aplicar técnicas de preservación, como la creación de imágenes forenses o el uso de herramientas que mantengan la integridad del contenido.

Esto ha derivado en casos donde los discos duros fueron abiertos directamente en comisarías, provocando la pérdida de información crítica o la contaminación de la prueba.

Otro problema común es la escasa capacitación técnica de jueces y fiscales. En múltiples casos, los operadores jurídicos no comprenden conceptos básicos como metadatos, logs de acceso o criptografía, lo que impide una adecuada valoración de la prueba digital. Esto

ha generado decisiones erróneas, como la exclusión de pruebas por considerar que no fueron recabadas "materialmente", pese a que cumplían con todos los estándares técnicos y legales.

La falta de protocolos también genera incertidumbre. En algunas fiscalías no existe un procedimiento unificado sobre cómo extraer datos de celulares, analizar correos electrónicos o tratar con evidencia proveniente de redes sociales. Esto produce disparidad en la calidad de las investigaciones y genera espacio para la nulidad de pruebas por actuación irregular.

Por ejemplo, en un caso tramitado en Lima Norte en 2022, una denuncia por fraude mediante transferencia electrónica fue archivada debido a que la fiscalía no logró obtener los registros del banco a tiempo, ni preservar los datos del dispositivo utilizado por el imputado. Al momento de solicitar el peritaje, el equipo había sido formateado, y no existía una copia forense que permitiera reconstruir los hechos.

Estos problemas evidencian la necesidad de fortalecer institucionalmente las fiscalías, dotarlas de personal técnico permanente y establecer protocolos estandarizados de actuación, a fin de asegurar que la prueba digital sea recabada, conservada y valorada correctamente.

2.7.3. Importancia en la decisión fiscal

Una deficiente recolección de la prueba digital puede derivar en sobreseimientos, archivos fiscales o absoluciones, generando impunidad y desprotección a las víctimas. La prueba digital, mal gestionada, se convierte en una debilidad estructural del sistema acusatorio (Paredes, 2020).

Estas consecuencias no se limitan a errores menores, sino que comprometen directamente el éxito de la investigación penal. Si durante las diligencias preliminares no se aplican protocolos adecuados para la extracción, conservación y análisis de evidencias digitales, el Ministerio Público puede verse imposibilitado de sustentar una teoría del caso sólida, lo cual conlleva al archivo del caso antes de formularse acusación.

En Lima Norte, por ejemplo, se han registrado procesos en los que la fiscalía no pudo formalizar acusación porque la evidencia digital fue extraída sin actas o sin respaldo pericial, lo que permitió que la defensa cuestione su autenticidad. También ha ocurrido que, en etapa de juicio, la ausencia de peritos capaces de sustentar el contenido técnico de las pruebas digitales generó que el juez no pueda valorarlas adecuadamente, afectando el resultado del proceso.

Por ello, Delgado (2013) advierte que la omisión de estándares técnicos en la actuación probatoria digital no solo debilita la acusación fiscal, sino que puede implicar responsabilidad funcional.

En consecuencia, la prueba digital no puede ser tratada como un elemento accesorio. Su deficiente manejo no solo favorece la impunidad, sino que mina la legitimidad del sistema penal y la confianza ciudadana en las instituciones encargadas de la persecución del delito.

Estas consecuencias probatorias no son meramente teóricas. En la práctica, múltiples procesos penales por fraude informático han fracasado debido a errores en la obtención o tratamiento de la evidencia digital. Por ejemplo, si los datos extraídos de un celular o computadora no son acompañados de un acta de incautación, una copia forense verificable o un informe pericial que respalde su autenticidad, la defensa puede solicitar su exclusión por vulneración de derechos procesales. Esto ha ocurrido en varios procesos en Lima Norte, donde pruebas clave fueron descartadas por falta de cadena de custodia adecuada o por manipulación indebida.

Asimismo, si la fiscalía presenta una evidencia tecnológica sin conocimiento técnico o sin contar con un perito que pueda explicar su relevancia y funcionamiento ante el juez, se corre el riesgo de que dicha prueba pierda eficacia probatoria. En estos casos, el juez puede considerar que no existe certeza razonable de que el imputado haya cometido el delito, lo que se traduce en la absolución del acusado.

Además, cuando el sistema de justicia penal no logra asegurar el procesamiento efectivo de los casos de fraude informático, se genera un efecto negativo en la confianza ciudadana. La percepción de impunidad alimenta la reincidencia delictiva y desalienta a las víctimas a denunciar.

III. MÉTODO

3.1. Tipo de investigación

Será cualitativa, conforme Piza y Beltrán (2019) la investigación cualitativa se caracteriza por su enfoque flexible y la integración de diversos métodos, técnicas y herramientas para comprender fenómenos en su contexto natural. Su proceso incluye fases como planteamiento del problema, revisión de literatura, recolección y análisis de datos, y reporte de resultados. Se utiliza métodos como la observación y la entrevista para recopilar datos cualitativos. Así mismo, se busca una comprensión profunda y holística de los fenómenos estudiados.

La investigación descriptiva busca comprender las situaciones, prácticas y actitudes predominantes mediante una descripción precisa de las actividades, objetos, procesos y personas involucradas (Guevara et al., 2020, p. 171).

3.1.1. Nivel de investigación

Será descriptivo, de acuerdo con Miles y Gay (2019) El propósito fundamental de la investigación básica es la formulación o perfeccionamiento de una teoría. Este enfoque se sustenta en un proceso conceptual que demanda numerosos estudios de investigación a lo largo del tiempo. En este contexto, los investigadores no persiguen obtener beneficios inmediatos de sus descubrimientos, dado que puede transcurrir un considerable periodo antes de que la investigación básica dé lugar a aplicaciones educativas prácticas.

Según el libro "El proceso de investigación" de Sabino (1992) la investigación descriptiva se define como el tipo de investigación que busca describir aspectos fundamentales de conjuntos homogéneos de fenómenos. Este enfoque utiliza criterios sistemáticos para establecer la estructura o el comportamiento de los fenómenos estudiados, proporcionando información sistemática y comparativa con otras fuentes (Martínez, 2018).

3.1.2. Diseño

La investigación adopta un enfoque no experimental, ya que se fundamenta en la observación directa de fenómenos en su estado natural, sin intervenir o manipular variables o el entorno en el que se desarrolla la actividad investigada. Los fenómenos son observados mediante la aplicación de instrumentos en un único y específico momento, caracterizando así un diseño de corte transversal. Este estudio se clasifica como descriptivo, dado que su propósito central es detallar minuciosamente cada variable e indicador de investigación.

3.1.3. Método

En la definición de Carvajal (2013) el método deductivo en la investigación se caracteriza por utilizar un tipo de razonamiento que parte de una visión más general y lógica, basada en principios o leyes, para luego aplicarse a hechos específicos. En esencia, este enfoque lógico tiene como propósito extraer conclusiones a partir de una serie de principios previamente establecidos.

3.2. Ámbito temporal y espacial

El ámbito temporal se sitúa en el año 2024, mientras que el ámbito espacial abarca la Fiscalía Penal Provincial de Lima Norte.

3.3. Variables

Según la perspectiva metodológica cualitativa que guía este estudio de investigación, se confirma la pertinencia del término Categorías, en lo que respecta a este aspecto.

Operacionalización de categorías

Categorías	Definición Conceptual	Subcategorías
Incorporación de la prueba	Villalobos (2017) es el proceso mediante el cual se obtiene, asegura y formaliza la admisión de la prueba digital en el expediente fiscal,	Tipo de evidencia digital

	cumpliendo requisitos legales y técnicos.	
Factores que afectan su eficacia	Brenner (2010) son aquellos elementos que limitan o dificultan que la prueba digital cumpla su función dentro de la investigación penal.	Limitaciones técnicas, normativas y capacitación fiscal

Fuente: Elaboración propia

3.4. Población y muestra

3.4.1. Población

Sobre "una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones" (Hernández et al., 2014).

Para nuestra propuesta de investigación, se consideró a expertos en el tema en la Fiscalía Provincial Penal de Lima Norte.

3.4.2. Muestra

Según Hernández et al. (2014), la muestra es, en esencia, un subgrupo de la población. Digamos que es una extracción de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población.

Se consideró por conveniencia estimar el tamaño de muestra en base a la cantidad total de la población de estudio seleccionada. Por ello, la muestra empleada constó de ocho fiscales (abogados) expertos en Derecho Penal.

Participantes	Cargo	Institución
Cristhian Junior Lozano Valverde	Fiscal Adjunto Provincial	Ministerio Público
Shirley Stefani Requejo Fernández	Fiscal Provincial	Ministerio Público
José Raúl Hinostroza Espinoza	Fiscal Adjunto Provincial	Ministerio Público
Jorge Luis Porras Rosales	Fiscal Adjunto Provincial	Ministerio Público

Irving Poul Bustillos Villalta	Fiscal Adjunto Provincial	Ministerio Público
Elva Beneranda Cruz Mendez	Fiscal Adjunta Provincial	Ministerio Público
Carlos Daniel Cabrel Rios	Fiscal Adjunto Provincial	Ministerio Público
Karina Noemi Dávalos Navarro	Fiscal Provincial	Ministerio Público

3.5. Instrumentos

Conforme a Arias (2020) la ficha de entrevista se configura como un documento instrumental diseñado con el propósito principal de recopilar información de la persona entrevistada para el estudio. Este instrumento puede ser confeccionado tanto de manera manual como computarizada, y su edición está reservada exclusivamente al investigador, impidiendo cualquier manipulación por parte del entrevistado. El instrumento será:

a. Guía de entrevista.

3.6. Procedimientos

Se llevó a cabo la recopilación de información a través de la investigación y la búsqueda de material bibliográfico a nivel nacional e internacional, con el objetivo de respaldar de manera más sólida el fundamento científico. Posteriormente, para la implementación de las pautas de entrevista, se contactó a ocho expertos en derecho penal con el propósito de obtener sus opiniones, conocimientos, experiencias y profesionalismo, de acuerdo con las directrices establecidas en la guía, con el fin de cumplir con los objetivos propuestos en este trabajo de investigación.

3.7. Análisis de datos

Para Aranzamendi (2010) los métodos y técnicas relacionados a la investigación cualitativa, son la deducción, inducción y la hermenéutica conforme a una investigación de naturaleza jurídica, permitiendo así el correcto análisis de la información a obtener para la consecución de los fines propuestos por medio de los objetivos planteados.

IV. RESULTADOS

4.1. Análisis e interpretación de resultados

A continuación, procederemos a dar desarrollo a nuestros resultados, los mismos que están conformados por la aplicación de entrevistas, las mismas que fueron dirigidas a 8 fiscales que muy amablemente procedieron a dar sus opiniones o percepciones del tema. Asimismo, para este caso, se tuvo a bien la formulación de 10 preguntas que están alineadas a nuestros objetivos (general y específicos). Quedando conformado de la siguiente manera.

De acuerdo con el objetivo general se analizó de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024. Considerando la primera pregunta para el cumplimiento de este objetivo: ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

El primer entrevistado menciona que es fundamental ya que, en la actualidad la criminalidad se ha expandido a través de los sistemas informáticos; por otro lado, el segundo entrevistado mencionó que es relevante la información digital extraída de las aplicaciones de las entidades bancarias, pues comúnmente este tipo de delito se comete a través de las llamadas "bancas digitales". Asimismo, el tercer entrevistado indicó que la prueba digital para este tipo de delitos, resulta la más idónea en la investigación por la misma forma en que se comenten estos delitos; junto con ello, el cuarto entrevistado mencionó que sí tiene relevancia, porque generalmente en este tipo de delitos las personas investigadas captan a las víctimas a través de correos electrónicos, mensajes de WhatsApp, mensaje de texto, siendo que las víctimas solamente cuentan con ese tipo de evidencias al momento de formular su denuncia.

El quinto entrevistado explicó que la prueba digital es relevante en la investigación del delito de fraude informático, por cuanto es un delito que se comete en clandestinidad y con el uso de tecnología. El sexto entrevistado considera que es central y determinante, ya que esto

va a permitir reconstruir hechos con registros técnicos (transferencias, correos electrónicos y entre otros). El séptimo entrevistado confirmó que es fundamental, específicamente explicó que, en los delitos de fraude informático, la prueba digital no solo constituye el principal medio probatorio, sino que muchas veces es la única forma de evidenciar el modus operandi del investigado. Desde correos electrónicos, direcciones IP, trasferencias bancarias virtuales, hasta el rastreo de dispositivos electrónicos, todo cobra valor probatorio. Por último, el octavo entrevistado expuso que la prueba digital es relevante, ya que los delitos informáticos tienen relación con actos ilícitos que afectan los sistemas y datos informáticos que se comenten mediante el uso de tecnologías de la información o de la comunicación, por lo tanto, la prueba digital al ser una evidencia de carácter electrónica, es el medio más idóneo para acreditar los hechos relacionados a los delitos informáticos.

Ahora bien, considerando la segunda pregunta ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos? Para esto el primer entrevistado mencionó que es determinante, ya que te permite identificar la ubicación, el equipo que utilizó para el hecho ilícito e individualizar al autor o coautores. El segundo entrevistado afirmó ello ya que justamente con el reporte extraído por las entidades bancarias que registra los movimientos no autorizados en plataformas digitales es que se llama a la ruta de las transacciones fraudulentas, logrando identificarse a los autores. Adicionalmente, el tercer entrevistado expresó que, por su naturaleza delictiva, si resulta determinante, porque es muy difícil una prueba documental (material), sino la prueba digital permanece pendiente hasta su extracción oficial. El cuarto entrevistado explicó que sí es determinando para resolver este tipo de casos, ya que, a través de estos medios de prueba, se puede llegar a identificar a las personas que envían los mensajes de correo electrónico, WhatsApp u otros a sus víctimas.

El quinto entrevistado menciona que es determinante, porque constituye una de las pruebas más idóneas para resolver este tipo de casos. El sexto entrevistado explicó que en

algunos casos estos han sido de mucha ayuda para poder reconstruir los hechos y poder lograr en algunos casos, la identificación de los investigados y hasta la formalización de la investigación preparatoria. El séptimo afirmó que en la mayoría de casos es determinante. En varios procesos, el acceso a registros de servidores, chats de WhatsApp o movimientos bancarios en línea, han permitido reconstruir los hechos con precisión y lograr la formalización de la investigación preparatoria o incluso sentencias condenatorias. Por último, el octavo mencionó que sí es muy importante, ya que la prueba digital, tales como correos, mensajes y audios a través de redes sociales, constituyen pruebas determinantes para la obtención de información corroborante de los delitos, ya que son el soporte a través de los cuales se concretizan estos delitos.

Por otro lado, de acuerdo con el primer objetivo específico se describió cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024. Para esto se consideró la pregunta ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga? Entonces, se desarrolló considerando las respuestas de los entrevistados

El primer entrevistado menciona que las transferencias bancarias que se realizan al introducir datos personales del titular de una cuenta y así poder disponer y generar un beneficio económico. El segundo entrevistado expresó que en casos en general, con mayor frecuencia se presentan los registros fílmicos y otros medios audiovisuales. Asimismo, el tercer entrevistado expresó que las más comunes son los movimientos de estados de cuenta, la extracción propia de información de aplicativos bancarios o monetario digital en los celulares. También, el cuarto entrevistado comentó que generalmente los denunciantes presentan las capturas de pantalla de sus teléfonos celulares, donde reciben los mensajes por WhatsApp, asimismo, presentan las impresiones de los correos electrónicos que reciben de estas personas o de las entidades bancarias, comunicándoles a las personas los movimientos de dinero de su cuenta bancaria.

Con ello, el quinto entrevistado explicó que se presenta, por ejemplo, estado de cuenta bancaria, captura de mensajes de texto donde se comunica sobre la operación realizada, capturas de transferencias dinerarios. De la misma manera, el sexto entrevistado coincidió mencionando que en su mayoría son los registros bancarios (movimientos, IP), correos electrónicos, capturas de pantallas o la información que se puede extraer de un aparato electrónico. Coincidentemente el séptimo entrevistado comentó que como tipos de evidencia principalmente se tiene a registros de operaciones bancarias, captura de pantalla, correos electrónicos, mensajes de redes sociales y archivos extraídos de celulares o computadoras mediante peritajes informáticos. Por último, el octavo entrevistado expuso que los celulares y computadoras, que contienen información relacionada a mensajes y llamadas, almacenamiento o intercambio de información a través de redes sociales, las cámaras de videovigilancia públicos o privados.

Asimismo, se tiene las respuestas a la pregunta ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal? El primer entrevistado mencionó que a través del requerimiento del levantamiento de secreto de las comunicaciones y/o bancario. El segundo entrevistado comenta que, si el soporte es un USB, memoria, o CD, se incorpora mediante la cadena de custodia, y luego se introduce como medio probatorio a través de la preservación que se realiza generalmente mediante actas. Por otro lado, el tercer entrevistado mencionó que las más recurrente es la diligencia de extracción digital de información de un equipo celular. Otro es la extracción de información de correctos electrónicos, etc. El cuarto entrevistado que para preservar la evidencia digital (copia de los videos de seguridad, captura de pantalla, identificar dirección web, URL e ID de redes sociales, preservación de cuentas de redes sociales, captura de información volátil, entre otros).

El quinto entrevistado comentó que al principio, se requiere de forma documental y luego, de ser posible, se revisa la fuente de prueba, es decir, de donde proviene. El sexto

entrevistado mencionó que los agraviados suelen remitir estas pruebas y estas son aseguradas en una cadena de custodia. También son mediante los requerimientos a bancos o empresas telefónicas para solicitar esa información y luego de ello ser incorporada a la carpeta fiscal. El séptimo expone específicamente que primero, se solicita su obtención mediante una diligencia fiscal, como una incautación o levantamiento del secreto de las comunicaciones. Luego, se incorpora el informe técnico del perito de informática forense, que da cuenta del contenido y de la cadena de custodia. Todo se registra formalmente en la carpeta fiscal. Por último, el octavo entrevistado explicó que se debe proceder al aseguramiento de la escena del delito donde se encuentre la evidencia digital. Antes del ingreso a la escena, se debe coordinar con los peritos especializados para la forma de reconocer, identificar la evidencia digital relevante, para proceder a su adquisición y captura de la evidencia digital, luego se debe preservar la evidencia con la debida cadena de custodia.

De acuerdo con la pregunta ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación? El primer entrevistado mencionó que sí; mientras que el segundo entrevistado expuso que desconoce si existe algún lineamiento específico. Asimismo, el tercer entrevistado explicó que específicamente no existe un lineamiento para el tratamiento de prueba digital; sin embargo, se trata de adoptar los actos de investigación. El cuarto entrevistado manifestó que no se cuenta de manera formal con un protocolo de actuación para este tipo de investigaciones.

Por otro lado, el quinto entrevistado expuso que el Ministerio Público como órgano, constitucionalmente autónomo se encuentra sujeto a lo regulado en el Código Procesal Penal respecto al tratamiento de la prueba en general. Asimismo, el sexto entrevistado expuso que existe el Reglamento de Cadena de Custodia del Ministerio Público, Manual para el recojo de evidencia Digital (RM 848-2019-IN), lineamientos y guías de la Unidad Fiscal Especializada en Ciberdelincuencia; mientras que el séptimo entrevistado explicó que si, existe un Manual

de Actuación Fiscal para delitos informáticos, y también lineamiento del equipo especialista en ciberdelincuencia del Ministerio Público. Sin embargo, aún se requiere una mayor difusión y actualización de estos documentos para todos los despachos fiscales. Por último, el octavo entrevistado mencionó que sí, se cuenta con el Manual de evidencia digital, además del Reglamento de la cadena de custodia de elementos materiales, evidencias y administración de bienes incautados, aprobado por la Resolución N° 729-2006-MP-FN.

A su vez, considerando el segundo objetivo específico**, se i**dentificó los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024. Se consideró ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraudes informático? Para esto el primer entrevistado mencionó que la demora en recibir la información por parte de las entidades privadas (bancarias o aplicativos). Asimismo, el segundo entrevistado mencionó que suele suceder que los equipos informáticos no cuentan con las características para soportar la reproducción de ciertas evidencias digitales, ya sea por problemas de software o hardware. El tercer entrevistado explicó que primero es la falta de colaboración de los investigados, incluso de la parte agraviada, lo que nos lleva a solicitar los levantamientos que demoran en su respuesta. Al mismo tiempo, el cuarto entrevistado expuso que no existe un protocolo de actuación para este tipo de casos, cada despacho fiscal investiga estos casos según su criterio.

El quinto entrevistado mencionó que, en algunos casos, se requieren direcciones IP o metadatos, que por lo general resulta ser una información compleja en su entendimiento. Por otro lado, el sexto entrevistado explicó que la falta de capacitación sobre los delitos informáticos, la demora en las respuestas de las entidades e incluso de las partes agraviadas, y las brechas de equipamiento y peritaje. El séptimo entrevisto expuso que hay varias, la falta de personal especializado, la demora en obtener información de proveedores de servicio digitales

y, en algunos casos, la imposibilidad de acceder a datos alojados en el extranjero. También hay brechas tecnológicas entre el accionar delictivo y la capacidad investigativa. Finalmente, el octavo entrevistado explicó que las dificultades se deben a la disponibilidad de peritos suficientes para la recolección de evidencia digital, sobre todo en los turnos fiscales, lo que genera un retraso en la obtención de la prueba digital. La casi nula coordinación con otros países para identificar a los titulares de líneas telefónicas extranjeras.

Respecto a la pregunta ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba? El primer entrevistado menciona que dependiendo en la especialidad que se desempeñen, los fiscales y personal administrativo que ven todos los delitos no tienen el conocimiento especializado para realzar un trabajo estratégico a diferencia de los fiscales especializados en la materia que cuenta con el conocimiento y las herramientas. El segundo entrevistado explicó que no todos los fiscales están debidamente capacitados, la investigación de delitos informáticos requiere de conocimientos especializados, es por lo que resulta necesario que se amplíen las unidades de ciberdelincuencia del Ministerio Público a otros distritos fiscales además de Lima Centro. Asimismo, el tercer entrevistado expuso que tratándose de delitos “modernos”, aun es poca la capacitación para el tratamiento de este tipo de pruebas. El cuarto entrevistado explicó que los fiscales y personal del Ministerio Público no cuentan actualmente con la capacitación adecuada para este tipo de investigaciones.

El quinto entrevistado mencionó que no, si bien se creó hace un tiempo las fiscalías de ciberdelincuencia, hasta el momento no se ha visto reflejado su apoyo. El sexto entrevistado explicó que al ser una fiscalía que ve delitos comunes y no una fiscalía especializada, se requiere de una mayor capacitación para este tipo de delito y así poder sacarle un mejor provecho a este tipo de pruebas digitales. Adicionalmente, el séptimo entrevistado indicó que en general no hay una clara necesidad de capacitación constante. Algunos despachos reciben apoyo del equipo de ciberdelincuencia, pero no todos los fiscales tienen un conocimiento

técnico actualizado sobre la materia. Por último, el octavo entrevistado explicó que aún se está en proceso de aprendizaje de estas nuevas formas de adquisición de prueba digital. La Academia de la Magistratura, las universidades y los colegios profesionales, cada vez ofrecen más cursos sobre la evidencia digital, incluso sobre el impacto de la inteligencia artificial en la comisión de delitos.

Por otro lado, respecto a la pregunta ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación? El primer entrevistado expuso que sí, mientras que el segundo solo mencionó que no hasta el momento. El tercer entrevistado explicó que una dificultad es la utilización de cuentas de personas iletradas que son captadas para crear estas cuentas y dificulta la identidad de quien usan realmente estas cuentas. Asimismo, el cuarto entrevistado indicó que hubo casos en los cuales, el proceso judicial ha terminado en absoluciones debido a que no se ha preservado de manera correcta las pruebas digitales dentro de una investigación preparatoria.

El quinto y sexto entrevistado mencionaron que no, mientras que el séptimo y octavo explicaron que sí, el séptimo expuso que por ejemplo, cuando no se asegura la cadena de custodia o cuando no se logra sustentar la autenticidad del contenido digital, se debilita el caso y a veces no se puede continuar con la investigación; mientras que el octavo explicó que a pesar de los esfuerzos de las autoridades para identificar a un usuario de criptomoneda involucrado en una estafa, no fue posible ubicar al titular de la cuenta debido al uso de seudónimos y la falta de coordinación con los servidores de alcance global.

Finalmente, respecto a la pregunta ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales? El primer entrevistado mencionó que una medida sería la implementación de fiscalías especializadas en ciberdelincuencia a nivel nacional con las herramientas tecnológicas adecuadas. El segundo expresó sobre la ampliación de recursos para la adquisición de mejores equipos informáticos,

y contratación de personal especializado (ingenieros informáticos) en cada distrito fiscal, que puedan realizar asesorías o acompañamiento en las investigaciones. El tercer entrevistado explicó que una mayor capacitación en las entidades, así como legislación para entidades bancarias o de tesorería. Por otro lado, el cuarto entrevistado explicó que de la misma manera una medida sería una constante capacitación para los fiscales y personal administrativo del Ministerio Público, se requiere la elaboración de un protocolo de actuación donde se fije los lineamientos de actuación para este tipo de casos de delitos informáticos.

A su vez, el quinto entrevistado mencionó que sobre en principio, una capacitación masiva en lo que es prueba digital y, segundo, una modificación del Código Procesal Penal para implementar de forma expresa la prueba digital. El sexto entrevistado explicó hacer un énfasis en realizar capacitaciones tanto para los fiscales, personal administrativo y demás entidades a las cuales se les solicita información para obtener estas pruebas. Por otro lado, el séptimo explicó que primero, una capacitación técnica obligatoria para fiscales y asistentes; segundo, mayor inversión en el área de pericias digitales y personal especializado. Y, tercero, establecer protocolos agiles de cooperación con entidades bancarias y plataformas tecnológicas. Por último, el octavo mencionó como medidas fortalecer la unidad de peritajes digitales de la PNP y del Ministerio Público, establecer mecanismos de coordinación con las unidades que contienen información de los titulares de los teléfonos celulares, establecer mecanismos de identificación idónea de los titulares de las cuentas de redes sociales.

V. DISCUSIÓN DE RESULTADOS

En cumplimiento del objetivo de analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024, los resultados obtenidos revelan que dicha evidencia no solo tiene un carácter relevante, sino que su papel se torna imprescindible para la reconstrucción de los hechos, la identificación de los autores y la formalización del proceso penal; ello se observa tanto en la percepción de los fiscales como en la experiencia de los peritos entrevistados. La prueba digital, en ese sentido, se convierte en el elemento central de las diligencias preliminares y posteriores, especialmente en contextos donde no existen testigos ni pruebas materiales tradicionales; es decir, cuando la naturaleza clandestina del delito, ejecutado mediante herramientas tecnológicas, impide contar con otras formas de evidencia. Así, los entrevistados señalan que, sin la obtención, validación y análisis técnico de esta prueba, resultaría prácticamente inviable sostener una investigación con fundamento jurídico sólido; por ende, la prueba digital no solo tiene carácter indiciario, sino que muchas veces constituye la única vía de esclarecimiento penal disponible, lo que refuerza su valor determinante en la configuración del proceso penal actual.

En relación directa con estos hallazgos, resulta pertinente contrastarlos con la investigación realizada por Salas y Romero (2024), quienes abordaron el modo en que se incorpora la prueba digital en los procesos por fraude informático en Lima Norte; si bien reconocen que la prueba digital puede lograr eficacia procesal, también advierten que ello solo es posible cuando su obtención se realiza mediante pericia técnica especializada y con sujeción estricta a criterios de utilidad, pertinencia y conducencia. En ese sentido, los resultados de esta investigación confirman lo señalado por estos autores, al evidenciar que los fiscales valoran la prueba digital como determinante, siempre que haya sido obtenida bajo un marco técnico y jurídico riguroso; sin embargo, se advierte un matiz relevante: mientras que Salas

y Romero (2024) subrayan la ausencia de lineamientos uniformes y la limitada capacitación como principales obstáculos, los entrevistados en esta investigación centran su preocupación en la dependencia exclusiva de esta prueba para sostener el caso, lo cual, más allá de la forma en que se obtiene, condiciona todo el desarrollo procesal y coloca al fiscal en una posición de alta dependencia del peritaje informático, configurando un panorama donde la carencia de otros elementos de convicción intensifica la exigencia de rigor probatorio sobre lo digital.

Asimismo, se encuentra una correspondencia sustancial con los planteamientos de Portugal (2023), quien señaló que, aunque la prueba digital es formalmente admisible, su eficacia probatoria depende de cómo se recolecta, presenta y preserva; esta afirmación guarda una relación directa con la percepción de los operadores jurídicos entrevistados, quienes indicaron que la sola existencia de una evidencia digital no garantiza su impacto en el proceso penal, sino que dicho impacto está mediado por procedimientos técnicos, como la cadena de custodia, la conservación del hash, la trazabilidad del origen de los datos y la correcta elaboración del informe pericial. No obstante, un punto de distinción importante se advierte: mientras que Portugal enfoca su análisis en la necesidad de contar con regulación clara y criterios uniformes, esta investigación encuentra que, incluso en presencia de criterios internos relativamente definidos por la propia Fiscalía, la eficacia de la prueba digital continúa siendo desigual; esto ocurre porque no todos los fiscales poseen los conocimientos necesarios para interpretar adecuadamente los informes técnicos, ni cuentan con personal especializado de manera constante, lo que reduce el impacto de la prueba en etapas claves del proceso, como la formalización de la denuncia, la solicitud de diligencias preliminares o la sustentación de la acusación ante el juez.

En tercer término, resulta pertinente incorporar el análisis de Estrada (2024), quien expone que la impunidad en los delitos informáticos se explica, entre otras razones, por la falta de

especialización técnica del personal fiscal y por la debilidad del trabajo pericial, lo que conduce al archivamiento de los casos. Esta conclusión encuentra respaldo en los resultados del presente estudio, en la medida en que los entrevistados relatan, desde su experiencia directa, que cuando no se cuenta con una intervención especializada en tecnología digital o cuando el soporte informático no es sólido ni verificable, el Ministerio Público tiende a cerrar el caso por insuficiencia probatoria; sin embargo, esta investigación aporta un nivel adicional de especificidad, al señalar que no solo la debilidad técnica es causa de impunidad, sino también la inadecuada articulación entre fiscales y peritos, pues en varias ocasiones se describen situaciones en las que los informes son presentados fuera de los plazos procesales o con un lenguaje técnico incomprensible para el fiscal a cargo. Este hallazgo refuerza la tesis de que la prueba digital, pese a su relevancia teórica, no logra traducirse automáticamente en eficacia práctica si no se cuenta con condiciones institucionales que garanticen su tratamiento oportuno, comprensible y jurídicamente válido.

Ahora, de acuerdo con el primer objetivo específico, consistió en describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte durante el año 2024; al respecto, los resultados permiten observar que la evidencia digital más recurrente en dichos procesos corresponde a registros financieros y comunicaciones electrónicas, tales como transferencias bancarias, estados de cuenta, correos electrónicos, mensajes y capturas de pantalla; adicionalmente, se identificó la utilización complementaria de dispositivos electrónicos y grabaciones de videovigilancia. De igual modo, en relación con el procedimiento de incorporación de esta evidencia, se determinó que existe una secuencia metodológica sostenida sobre la garantía de la cadena de custodia y el soporte técnico forense, donde la recolección, extracción y formalización documental de la prueba se realiza bajo parámetros fiscales específicos; sin

embargo, se advirtió una percepción fragmentada respecto a la existencia y conocimiento de lineamientos normativos del Ministerio Público, pues algunos operadores manifiestan conocer guías y reglamentos, mientras otros refieren no haber accedido a directrices claras, lo que revela una implementación normativa aún insuficiente o de baja difusión.

En comparación con el estudio desarrollado por Salas y Romero (2024), quienes identificaron que la prueba digital únicamente alcanza eficacia procesal si se obtiene mediante pericia técnica especializada y bajo criterios de pertinencia, utilidad y conducencia; los hallazgos de esta investigación corroboran dicha posición, en tanto los fiscales entrevistados reconocen que, si bien se logra recuperar evidencia electrónica de valor incriminatorio, esta solo puede integrarse válidamente a la carpeta fiscal si es sometida a procedimientos técnicos rigurosos, incluyendo peritajes informáticos, actas de incautación y documentación de respaldo. Sin embargo, mientras en el estudio de Salas y Romero se enfatiza la ausencia de lineamientos uniformes como el principal obstáculo en la valoración judicial, en el presente caso, se identifica un problema más inmediato: la existencia de protocolos poco difundidos entre fiscales de Lima Norte; es decir, el problema no es tanto la inexistencia de normas, sino su conocimiento limitado dentro del propio Ministerio Público. Por tanto, el contraste evidencia que el desafío institucional no recae únicamente en el diseño normativo, sino en su implementación efectiva y continua capacitación del personal.

A su vez, lo encontrado en esta investigación también guarda estrecha relación con lo reportado por Portugal (2023), quien concluyó que la eficacia de la evidencia digital en el proceso penal depende no de su mera admisibilidad, sino del modo en que es recolectada, presentada y conservada. En esta línea, los fiscales entrevistados refieren que el procedimiento habitual implica una recolección en campo mediante diligencias fiscales o incautaciones, seguido por una etapa de extracción técnica respaldada por informes

periciales, para finalmente integrarla a la carpeta fiscal a través de actas documentadas. Tal secuencia refleja el cumplimiento parcial del estándar señalado por Portugal; sin embargo, se debe advertir que, en muchos casos, esta actuación carece de uniformidad metodológica, lo cual genera disparidades en la calidad probatoria, especialmente cuando intervienen fiscales con menor especialización en ciberdelincuencia. En ese sentido, si bien existe una práctica operativa reconocible, esta aún no responde a un modelo homogéneo ni articulado institucionalmente; lo cual, en línea con Portugal, exige una regulación más clara y obligatoria sobre la actuación fiscal frente a evidencia digital.

Por otro lado, los resultados obtenidos también coinciden con las advertencias formuladas por Estrada (2024), quien explicó que la falta de capacitación técnica del personal fiscal y la deficiencia en la labor pericial representan factores críticos en el archivamiento de casos de fraude informático. Aunque en el presente estudio los fiscales entrevistados reconocen disponer de procedimientos operativos para integrar la prueba digital, también manifiestan que, en ausencia de peritos capacitados o herramientas tecnológicas adecuadas, muchas diligencias probatorias se tornan ineficaces o inconclusas; especialmente cuando la información se encuentra encriptada o distribuida en plataformas digitales transnacionales. Así, el proceso de incorporación de prueba se ve interrumpido no solo por fallas procedimentales, sino también por limitaciones estructurales que impiden un tratamiento técnico adecuado. Estrada (2024) señala que esta falta de especialización institucional favorece la impunidad, lo cual se refleja en el presente trabajo al constatar que la actuación probatoria, aun cuando se inicie con diligencia, no siempre concluye con evidencias sólidas, precisamente por la escasa infraestructura digital y pericial en sedes fiscales locales.

En suma, los hallazgos de esta investigación reafirman las preocupaciones detectadas en estudios previos: la incorporación de prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, si bien responde a un protocolo

técnico parcialmente implementado, sigue estando condicionada por variables como la capacitación del personal, la existencia, la difusión de lineamientos normativos y el acceso a soporte pericial especializado. Por consiguiente, resulta urgente articular una respuesta institucional que no solo elabore más normas o guías, sino que asegure su implementación operativa, garantizando así que la evidencia digital sea incorporada de forma eficaz, válida y conforme a los principios del debido proceso penal.

Por último, según el segundo objetivo específico se logró identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, específicamente en la Fiscalía Penal Provincial de Lima Norte, durante el año 2024; en función de dicho objetivo, los resultados obtenidos reflejan que las principales dificultades enfrentadas se concentran en tres niveles claramente diferenciables: en el aspecto técnico, la complejidad inherente de los metadatos, las direcciones IP y las brechas en infraestructura digital; en el plano normativo, la rigidez del marco legal vigente, representado por la Ley N.º 30096 y la Ley N.º 32314, que no contempla herramientas procesales eficaces ni protocolos operativos claros; y en el ámbito institucional, la falta de personal capacitado, la demora en la obtención de información de entidades privadas, la inexistencia de fiscalías especializadas en delitos informáticos en diversas jurisdicciones y una limitada coordinación nacional e internacional. Todo ello repercute negativamente en la oportunidad, confiabilidad y legalidad de la prueba digital; en consecuencia, su tratamiento deficiente puede devenir en el archivo del caso o en la imposibilidad de formalizar la investigación preparatoria.

Al contrastar estos hallazgos con lo expuesto por Estrada (2024), se corrobora que la falta de especialización técnica y la debilidad institucional son componentes que erosionan el rol del Ministerio Público frente a la ciberdelincuencia; el autor, desde un enfoque jurídico-analítico centrado en operadores de justicia, señala que la deficiente labor pericial, junto

con la escasa preparación del personal fiscal, impide la identificación de los autores de delitos informáticos; en la misma línea, los testimonios recabados en esta investigación evidencian que la ausencia de conocimientos técnicos no solo retrasa la investigación, sino que compromete la validez misma de la prueba; por tanto, la consecuencia directa, tanto en el trabajo de campo como en el análisis doctrinario, es el archivamiento prematuro de los casos; en ese sentido, la impunidad no se presenta como un fenómeno aislado, sino como el resultado lógico de una estructura institucional que no ha priorizado la cibercriminalidad ni ha dotado de medios adecuados a los fiscales ordinarios.

Por otro lado, en lo que respecta a la dimensión normativa, los hallazgos encontrados permiten una correspondencia precisa con el análisis realizado por Carranza y Hernández (2023), quienes, al evaluar la Ley N.º 30096, advierten vacíos significativos en cuanto a la autenticidad, custodia y valoración de la prueba digital; estos elementos, también identificados en la presente investigación, muestran cómo la falta de protocolos específicos genera interpretaciones dispares entre operadores judiciales y obstaculiza el ejercicio pleno de la función fiscal; en los relatos de los fiscales entrevistados, se evidencia que, aun cuando se cuenta con dispositivos legales, su alcance resulta insuficiente frente a los desafíos tecnológicos contemporáneos; la inexistencia de procedimientos ágiles para el intercambio de información con plataformas digitales, la carencia de estándares en la preservación de evidencia electrónica y la ausencia de fiscalías especializadas con competencia transversal son factores que se reiteran en ambos estudios; de allí que el fortalecimiento normativo no deba limitarse a la promulgación de nuevas leyes, sino a la generación de reglamentos operativos que integren componentes técnicos, de ciberseguridad y de actuación interinstitucional.

La investigación de Gómez (2022), centrada en evaluar la eficacia de la prueba digital dentro del proceso penal por delitos informáticos, también guarda una relación estrecha con

los resultados obtenidos; en su estudio, se revela que la mayoría de los fiscales y jueces entrevistados reconocen tanto el valor probatorio de la evidencia electrónica como sus limitaciones prácticas derivadas de una insuficiente formación técnica; en ese sentido, los hallazgos de la presente investigación permiten afianzar esta relación causal: la eficacia de la prueba digital no está determinada únicamente por su existencia o su contenido, sino por la capacidad operativa del Ministerio Público para gestionarla, interpretarla y defenderla en sede judicial; asimismo, Gómez (2022), subraya la falta de protocolos estandarizados como un punto crítico que impide la uniformidad en el tratamiento de este tipo de pruebas; esta ausencia normativa también fue identificada en el trabajo de campo, donde fiscales entrevistados manifestaron incertidumbre respecto a cómo preservar o analizar adecuadamente la evidencia extraída de redes sociales, correos electrónicos o bases de datos intervenidas, lo cual puede traducirse en nulidades procesales.

Desde el plano internacional, el estudio de Betrán (2024), que aborda la compatibilidad de la prueba digital con el debido proceso penal en el sistema español, proporciona un marco útil para interpretar los riesgos asociados a una gestión inadecuada de la cadena de custodia; sus hallazgos confirman que, sin peritajes técnicos rigurosos y una trazabilidad comprobable de la prueba electrónica, se compromete tanto la admisibilidad como la legitimidad del proceso; en la misma dirección, los testimonios recogidos en Lima Norte evidencian fallas en la cadena de custodia, pérdida de contenido digital y limitaciones para autenticar archivos electrónicos, especialmente en casos donde los usuarios emplean perfiles anónimos o sistemas de cifrado; de esta manera, la problemática local no es aislada ni inédita, sino parte de una tendencia estructural en los sistemas penales que no han logrado adecuarse completamente a la naturaleza volátil, mutable y transnacional de la evidencia digital.

Por último, la investigación desarrollada por Fernandes (2019) en Brasil refuerza la tesis de que la eficacia de la prueba digital no puede entenderse sin considerar las condiciones materiales de trabajo del Ministerio Público; al identificar el déficit de laboratorios forenses, la escasa capacitación del personal y la falta de inversión como elementos limitantes, el autor configura un panorama que guarda similitud con el contexto limeño; en el estudio presente, la mayoría de los fiscales entrevistados hizo referencia a la inexistencia de equipos tecnológicos adecuados, a la dependencia de peritos externos y a la escasa coordinación con plataformas digitales; por ello, tanto en Brasil como en Perú, la eficacia de la prueba digital no depende únicamente de la voluntad fiscal, sino de una estructura institucional con capacidades técnicas suficientes, personal entrenado y recursos sostenibles que permitan enfrentar la sofisticación de los delitos informáticos.

En suma, los resultados obtenidos en la Fiscalía Penal Provincial de Lima Norte permiten establecer una coherencia sustantiva con los antecedentes seleccionados; todos coinciden en que la prueba digital enfrenta obstáculos normativos, técnicos e institucionales que afectan su eficacia procesal; además, se corrobora que la capacitación continua del personal, el fortalecimiento de las fiscalías especializadas y la generación de protocolos técnicos son condiciones necesarias para garantizar una actuación fiscal efectiva frente a la ciberdelincuencia.

VI. CONCLUSIONES

6.1 Se concluye que la prueba digital influye de manera decisiva en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024, en tanto que representa el principal, y en muchos casos el único, medio para reconstruir los hechos, identificar al presunto responsable y sustentar jurídicamente las diligencias fiscales; sin embargo, su eficacia no depende únicamente de su existencia o admisibilidad formal, sino del modo en que se obtiene, preserva, interpreta y presenta dentro del expediente penal. Los hallazgos muestran que, si bien el personal fiscal reconoce su importancia, también enfrenta limitaciones técnicas que dificultan su correcta valoración procesal; ello conlleva que la prueba digital, lejos de ser un recurso automáticamente útil, se convierta en un componente complejo que requiere intervención especializada, coordinación interinstitucional y comprensión jurídica por parte del fiscal. Estas condiciones determinan que su influencia en la investigación no sea uniforme ni garantizada, sino condicionada a factores operativos e institucionales cuya ausencia puede obstaculizar el avance o sustento del caso. Por tanto, la relevancia de esta prueba no radica solo en su potencial probatorio, sino en la capacidad del sistema penal para integrarla eficazmente en el proceso de investigación.

6.2 Se concluye que la incorporación de la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte durante el año 2024 se realiza mediante un procedimiento técnico que privilegia la cadena de custodia, la intervención pericial y la documentación formal en actas fiscales; sin embargo, dicha actuación se ve limitada por el conocimiento parcial de los lineamientos institucionales que orientan su tratamiento, lo que afecta la consistencia metodológica entre investigaciones. Aunque existen esfuerzos por asegurar la validez probatoria de registros financieros, comunicaciones electrónicas y dispositivos tecnológicos, la

eficacia de su incorporación depende del nivel de especialización del fiscal a cargo, así como de la disponibilidad de recursos técnicos. Esto implica que, en ausencia de criterios uniformes aplicados de forma constante, la prueba digital puede perder fuerza en su función demostrativa, lo cual compromete la capacidad del Ministerio Público para sustentar la responsabilidad penal en contextos de criminalidad informática cada vez más complejos.

6.3 Se concluye que la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal por delitos de fraude informático, en la Fiscalía Penal Provincial de Lima Norte en 2024, se ve limitada por la combinación de tres factores críticos: en primer lugar, la insuficiencia normativa, dado que la Ley N.º 30096 y la Ley N.º 32314 no contemplan mecanismos ágiles ni procedimientos técnicos estandarizados para asegurar la integridad de la evidencia digital; en segundo lugar, la limitada capacitación del personal fiscal no especializado, lo cual restringe la adecuada recolección, análisis y sustentación de esta prueba ante la judicatura; en tercer lugar, la carencia de recursos tecnológicos actualizados, así como la falta de coordinación efectiva con entidades privadas e internacionales que poseen datos clave para la investigación. Estos factores no operan de forma aislada, sino que interactúan entre sí, debilitando la capacidad institucional del Ministerio Público para enfrentar la sofisticación de los fraudes informáticos. Como implicancia, se observa un riesgo latente de archivamiento prematuro de casos y de vulneración del debido proceso por deficiencias en la cadena de custodia y en la valoración de la evidencia digital, lo cual compromete no solo la eficacia de la acción penal, sino también la credibilidad del sistema de justicia frente a este tipo de criminalidad.

VII. RECOMENDACIONES

7.1 Establecer, con carácter obligatorio, un protocolo interno en la Fiscalía Penal Provincial de Lima Norte que disponga la intervención inmediata de peritos informáticos especializados desde la etapa preliminar de cada investigación por fraude informático, debiendo incluir lineamientos claros sobre preservación de la evidencia digital, redacción técnica accesible para el fiscal, y plazos perentorios de entrega, a fin de garantizar que la prueba digital pueda ser utilizada con eficacia procesal desde los primeros actos de investigación.

7.2 Implementar de manera obligatoria un plan de capacitación fiscal semestral, focalizado en el tratamiento técnico de la evidencia digital en delitos de fraude informático, dirigido específicamente al personal de la Fiscalía Penal Provincial de Lima Norte, que incluya el manejo forense de datos, el uso adecuado de herramientas digitales y la correcta aplicación de los lineamientos internos existentes, con el fin de reducir la variabilidad en la recolección y valoración de este tipo de prueba.

7.3 Se recomienda implementar una unidad técnica de soporte digital permanente dentro de la Fiscalía Penal Provincial de Lima Norte, conformada por peritos en informática forense y especialistas legales en delitos informáticos, con funciones específicas de asesoría inmediata al fiscal de turno, análisis técnico de evidencias electrónicas y supervisión directa de la cadena de custodia digital; esta unidad debe contar con protocolos internos aprobados por el Ministerio Público y con infraestructura tecnológica básica para realizar peritajes preliminares, lo que permitiría reducir la dependencia externa, evitar dilaciones en la formalización de investigaciones y garantizar la integridad procesal de la prueba digital desde su incautación hasta su presentación en juicio.

VIII. REFERENCIAS

Aragoneses Martínez, S., Hinojosa Segovia, R., Muerza Esparza, J. J., de la Oliva Santos, A., y Tomé García, J. (2003). *Derecho procesal penal* (6.ª ed.). Centro de Estudios Ramón Areces

Bernal, M. (2017). *Fiscalía y nuevas tecnologías: desafíos del Ministerio Público frente al cibercrimen*. Lima: Jurídica.

Betrán Franco, Y. (2024). *La valoración de la prueba digital en un caso de delito de coacciones… y revelación de secretos* [Trabajo Fin de Máster, Universidad de Zaragoza]. Zaguán (Repositorio UNIZAR).

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. ABC-CLIO.

Consejo de Europa. (2001). *Convenio de Budapest*

Decreto Legislativo N° 957. Decreto legislativo que aprobó el Nuevo Código Procesal Penal. (22 de julio de 2004)

Delgado Martín, J. (2013). *La prueba electrónica en el proceso penal.* Diario La Ley.

Devis Echandia, H. (2012). *Teoría general de la prueba judicial.* (6° ed.) Editorial Temis.

El Peruano. (2021, junio 2). *Ciberdelitos en el Perú: se elevan denuncias de fraude informático y suplantación de identidad*. https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad

Estrada Salvador Ramírez. (2024). *La impunidad en los delitos informáticos: una problemática de poco interés para legisladores, jueces y fiscales. Ius Vocatio, Corte Superior de Justicia de Huánuco.* https://revistas.pj.gob.pe/revista/index.php/iusVocatio/article/view/928

Fernandes, A. J. F. (2019). *A problemática da utilização da prova digital no processo penal brasileiro diante da ausência de regulamentação* [Trabalho de Conclusão de Curso (graduação em Direito), Universidade Federal de Santa Catarina]. Repositório Institucional da UFSC.

Gallegos Osorio, S. A. (2022). *La evidencia digital y laos delitos informáticos en el Sistema Jurídico Peruano, 2020*

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill.

Ley N° 30096. Ley de delitos informáticos (22 de octubre de 2013). Diario Oficial El Peruano.

Mendoza Ayma, F. (2019). *Aproximaciones a la prueba digital.* Obtenido de https://lpderecho.pe/aproximaciones-prueba-digital-francisco-celis-mendoza-ayma/

Mendoza Prado, M. de L. (2024) *Interpretación y Desafíos de la Evidencia Digital en la Investigación Criminal.* Código Científico Revista De Investigación.

Mengoa Valdivia , M. (2021). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú.*

Ministerio Público – Fiscalía de la Nación (15 de junio de 2006). *Reglamento de cadena de custodia (Resolución de la Fiscalía de la Nación N° 729-2006-MP-FN).*

Ministerio Público – Gerencia General (11 de agosto de 2020). *Guía de análisis digital forense (RGG N°. 000365-2020).*

Neyra Flores, J. A. (2024). *Temas de razonamiento probatorio penal: la práctica y valoración de la prueba digital en el proceso penal peruano* [Documento de trabajo]. Universidad de San Martín de Porres. https://hdl.handle.net/20.500.12727/17014

Orrego Acuña , J. (2019). *Teoría de la Prueba.* Obtenido de https://www.juanandresorrego.cl/apuntes/teor%C3%ADa-de-la-prueba/

Paredes, M. (2020). *Cadena de custodia y prueba digital en el proceso penal peruano*. Lima: Grijley.

Piza Burgos, N. D., Amaiquema Marquez, F. A., y Beltrán Baquerizo, G. E. (2019). *Métodos y técnicas en la investigación cualitativa. Algunas precisiones necesarias.* Revista Conrado.

Porras Espejo, P. A. (2023). *La incorporación de la prueba digital en el proceso penal colombiano [Tesis de especialización*, Universidad Libre (Seccional Bogotá)]. UniLibre Repository. https://hdl.handle.net/10901/29366

Portugal Román, J. (2023). *Delitos informáticos y la evidencia digital en el proceso penal peruano* [Tesis de licenciatura, Universidad Privada San Carlos]. https://repositorio.upsc.edu.pe/handle/UPSC/775

Ramos Núñez, C. (2015). *Manual de Derecho Penal Informático*. Lima: Palestra.

Resolución Ministerial N°. 848-2019-IN, Manual de evidencia digital. (12 de junio de 2019)

Salas Camacho, F., y Romero Soto, K. (2024). *La demostración de evidencia digital en delitos de fraude informático en Lima Norte, Perú* [Tesis de licenciatura, Universidad Tecnológica del Perú]. https://alicia.concytec.gob.pe/vufind/Record/UTPD_f806ca150d8064ac398b293f02d85a47

Sanz-Magallón Delhaize, G. (2018). *La prueba electrónica y sus diferentes tipos: Tratamiento procesal y consideraciones jurisprudenciales* (Trabajo académico, Facultad de Derecho, Universidad Pontificia Comillas).

Silva Sánchez, J. (2019). *Derecho penal de la sociedad digital*. Barcelona: Atelier.

Solanke, A. A. (2022). *Digital forensics AI: On practicality, optimality, and interpretability of digital evidence mining techni*ques [Doctoral dissertation, Université du Luxembourg]. ORBilu (University of Luxembourg Repository).

Téllez Valdés, J. (2003). *Derecho informático* (3.ª ed.). McGraw-Hill.

Tribunal Europeo de Derechos Humanos. (2009). *Bykov v. Russia*, Application no. 4378/02.

Vázquez, C. (2018). *La prueba digital y sus límites en el proceso penal*. Buenos Aires: Hammurabi.

Villalobos, J. (2017). *Prueba digital y proceso penal*. Fondo Editorial Jurídico.

IX. ANEXOS

Anexo A: MATRIZ DE CATEGORÍA
TÍTULO: *La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024*

PROBLEMAS	**OBJETIVOS**	**CATEGORIA**	**METODOLOGÍA**
Problema general	**Objetivo General**		
¿De qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024?	Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.	**<u>Categorías:</u>** - Incorporación de la prueba - Factores que afectan su eficacia **<u>Subcategoría</u>:** - Tipo de evidencia digital - Limitaciones técnicas y normativas, y capacitación fiscal	**Enfoque:** - **C**ualitativo **Diseño:** - No experimental **Tipo de investigación:** - Básica **Nivel de investigación:** - Descriptivo **Población:** Fiscalía Provincial Penal de Lima Norte. **Participantes:** Fiscales expertos en Derecho Penal. **Recolección y análisis de datos** **Técnicas:** Entrevista **Instrumento:** Guía de entrevista
Problemas específicos	**Objetivos Específicos**		
¿Cómo se incorpora la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte en 2024?	Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.		
¿Cuáles son los factores que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal por delitos de fraude informático?	Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal.		

Anexo B: Instrumento de recolección de datos

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos:

Cargo:

Institución:

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

   _____

   _____

   _____

2. ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?

   _____

   _____

   _____

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

3. ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?

4. ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?

5. ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

6. ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?

7. ¿Considera que el marco normativo vigente (como la Ley N.º 30096 o la Ley N.º 32314) es suficiente para sustentar su actuación fiscal en estos casos?

8. ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba?

_____

_____

_____

9. ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?

_____

_____

_____

10. ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?

_____

_____

_____

Anexo C: Validación del instrumento
Entrevistas

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos: Cristhian Junior Lozano Valverde

Cargo: Fiscal Adjunto Provincial

Institución: Ministerio Público

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

   Es fundamental ya que, en la actualidad la criminalidad se ha expandido a través de los sistemas informáticos.

2. ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?

   Es determinante, ya que te permite identificar la ubicación, el equipo que utilizó para el hecho ilícito e individualizar al autor o coautores.

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

3. ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?

   Las transferencias bancarias que se realizan al introducir datos personales del titular de una cuenta y así poder disponer y generar un beneficio económico.

4. ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?

A través del requerimiento del levantamiento de secreto de las comunicaciones y/o bancario.

5. ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?

   Si.

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

6. ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?
   La demora en recibir la información por parte de las entidades privadas (bancarias o aplicativos).
7. ¿Considera que el marco normativo vigente (como la Ley N.° 30096 o la Ley N.° 32314) es suficiente para sustentar su actuación fiscal en estos casos?
   Dicha ley como el código penal, busca la protección de los bienes jurídicos tutelados, pero no es suficiente porque se requiere un protocolo y un procedimiento célere que permita la obtención de información rápida.
8. ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba?

   Dependiendo en la especialidad que se desempeñen, los fiscales y personal administrativo que ven todos los delitos no tienen el conocimiento especializado para realzar un trabajo estratégico a diferencia de los fiscales especializados en la materia que cuenta con el conocimiento y las herramientas, es importante realizar esta distinción porque no todos los distritos fiscales a nivel nacional no cuentan con una fiscalía especializada en ciberdelincuencia, lo cual, debe ser prioridad para el estado y la Fiscalía de la Nación para su implementación integral.

9. ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?

Si.

10. ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?

La implementación de fiscalías especializadas en ciberdelincuencia a nivel nacional con las herramientas tecnológicas adecuadas.

Cristhian Junior Lozano Valverde
DNI N.° 47091932

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos: Shirley Stefani Requejo Fernández

Cargo: Fiscal Provincial

Institución: Ministerio Público

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

   Es relevante la información digital extraída de las aplicaciones de las entidades bancarias, pues comúnmente este tipo de delito se comete a través de las llamadas "bancas digitales".

2. ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?

   Sí, justamente con el reporte extraído por las entidades bancarias que registra los movimientos no autorizados en plataformas digitales es que se llama a la ruta de las transacciones fraudulentas, logrando identificarse a los autores.

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

3. ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?

En casos en general, con mayor frecuencia se presentan los registros fílmicos y otros medios audiovisuales.

4. ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?

Si el soporte es un USB, memoria, o CD, se incorpora mediante la cadena de custodia, y luego se introduce como medio probatorio a través de la preservación que se realiza generalmente mediante actas.

5. ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?

Desconozco si existe algún lineamiento específico.

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

6. ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?

Suele suceder que los equipos informáticos no cuentan con las características para soportar la reproducción de ciertas evidencias digitales, ya sea por problemas de software o hardware.

7. ¿Considera que el marco normativo vigente (como la Ley N.º 30096 o la Ley N.º 32314) es suficiente para sustentar su actuación fiscal en estos casos?

No es suficiente, además del marco normativo se requiere de mayores recursos, tanto humano como material para afrontar una investigación por delitos informáticos, es por ello que se deben crear fiscalías especializadas en ciberdelincuencia en el distrito fiscal de Lima Norte.

8. ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación

adecuada sobre este tipo de prueba?

No todos los fiscales estamos debidamente capacitados, pues la investigación de delitos informáticos requiere de conocimientos especializados, es por lo que resulta necesario que se amplíen las unidades de ciberdelincuencia del Ministerio Público a otros distritos fiscales además de Lima Centro.

9. ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?

No hasta el momento.

10. ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?

Ampliación de recursos para la adquisición de mejores equipos informáticos, y contratación de personal especializado (ingenieros informáticos) en cada distrito fiscal, que puedan realizar asesorías o acompañamiento en las investigaciones.

SHIRLEY STEFANI REQUEJO FERNANDEZ
FISCAL PROVINCIAL PENAL (T)
Primer Despacho
3° Fiscalía Provincial Penal Corporativa
Distrito Fiscal de Lima Norte

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos: JOSÉ RAÚL MINOSTROZA ESPINOZA

Cargo: FISCAL ADJUNTO PROVINCIAL PROVISIONAL

Institución: MINISTERIO PÚBLICO

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

   LA PRUEBA DIGITAL PARA ESTE TIPO DE DELITOS, RESULTA LO MÁS IDÓNEA EN LA INVESTIGACIÓN POR LA MISMA FORMA EN QUE SE COMETEN ESTOS DELITOS

2. ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?

   POR SU NATURALEZA DELICTIVA, SÍ RESULTA DETERMINANTE, PORQUE ES MUY DIFÍCIL UNA PRUEBA DOCUMENTAL (MATERIAL). SINO LA PRUEBA DIGITAL PERMANECE PENDIENTE HASTA SU EXTRACCIÓN OFICIAL

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

3. ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?

LOS MÁS COMUNES SON LOS MOVIMIENTOS DE ESTADOS DE CUENTA, LA EXTRACCIÓN PROPIA DE INFORMACIÓN DE APLICATIVOS BANCARIOS O MONEDERO DIGITAL EN LOS CELULARES.

4. ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?

LA MÁS RECURRENTE ES LA DILIGENCIA DE EXTRACCIÓN DIGITAL DE INFORMACIÓN DE UN EQUIPO CELULAR. OTRO ES LA EXTRACCIÓN DE INFORMACIÓN DE CORREOS ELECTRÓNICOS, ETC.

5. ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?

ESPECÍFICAMENTE NO EXISTE UN LINEAMIENTO PARA EL TRATAMIENTO DE PRUEBA DIGITAL, SIN EMBARGO, SE TRATA DE ADAPTAR LOS ACTOS DE INVESTIGACIÓN TRADICIONALES.

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

6. ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?

LO PRIMERO ES LA FALTA DE COLABORACIÓN DE LOS INVESTIGADOS, INCLUSO DE LA PARTE AGRAVIADA, LO QUE NOS LLEVA A SOLICITAR LOS LEVANTAMIENTOS, QUE DEMORAN EN SU RESPUESTA.

7. ¿Considera que el marco normativo vigente (como la Ley N.° 30096 o la Ley N.° 32314) es suficiente para sustentar su actuación fiscal en estos casos?

TODAVÍA DEBERÍA DEFINIRSE MEJOR DICHAS NORMATIVAS.

8. ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba?

TRATÁNDOSE DE DELITOS "MODERNOS", AUN ES POCA LA CAPACITACIÓN PARA EL TRATAMIENTO DE ESTE TIPO DE PRUEBAS.

9. ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?

UNA DIFICULTAD ES LA UTILIZACIÓN DE CUENTAS (CLONADAS POR EJEMPLO) DE PERSONAS JURADAS QUE SON CAPTADAS PARA CREAR ESAS CUENTAS, Y DIFICULTA LA IDENTIFICACIÓN DE QUIENES SON REALMENTE ESAS CUENTAS.

10. ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?

MAYOR CAPACITACIÓN EN LAS ENTIDADES, ASÍ COMO LEGISLACIÓN PARA ENTIDADES BANCARIAS O DE TELEFONÍA, Y AGILICEN LOS TRAMITES DE LEVANTAMIENTOS.

JOSÉ RAUL HINOSTROZA ESPINOZA
FISCAL ADJUNTO PROVINCIAL
Quinta Fiscalía Provincial Penal Corporativa
Cuarto Despacho - D. F. de Lima Norte

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos: Jorge Luis Porras Rosales

Cargo: Fiscal Adjunto Provincial

Institución: Ministerio Público

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

   Tiene relevancia, porque generalmente en este tipo de delitos las personas investigadas captan a las víctimas a través de correos electrónicos, mensajes de whatsaap, mensajes de texto, siendo que las víctimas solamente cuentan con ese tipo de evidencias al momento de formular su denuncia.

2. ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?

   Si es determinante para resolver este tipo de casos, ya que a través de estos medios de prueba se puede llegar a identificar a las personas que envían los mensajes de correo electrónico, whatsaap u otros a sus víctimas.

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

3. ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que

usted investiga?

Generalmente los denunciantes presentan las capturas de pantalla de sus teléfonos celulares, donde reciben los mensajes por whatsaap, asimismo presentan las impresiones de los correos electrónicos que reciben de estas personas o de las entidades bancarias comunicándoles a las personas los movimientos de dinero de su cuenta bancaria.

4. ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?

Preservar la evidencia digital (copia de los videos de seguridad, captura de pantalla, identificar direcciones web. URL e ID de redes sociales, preservación de cuentas de redes sociales, captura de información volatil entre otros).

5. ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?

No se cuenta de manera formal con un protocolo de actuación para este tipo de investigaciones.

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

6. ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?

No existe un protocolo de actuación para este tipo de casos, cada despacho fiscal investiga estos casos según su criterio.

7. ¿Considera que el marco normativo vigente (como la Ley N.° 30096 o la Ley N.° 32314) es suficiente para sustentar su actuación fiscal en estos casos?

No es suficiente ya que es necesario contar con un protocolo de actuación para este tipo de casos ya que en el distrito fiscal de lima norte no se cuenta con una fiscalia especializada en la materia, asimismo en lima norte no se cuenta con una unidad especializada en ciberdelincuencia.

8. ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba?

Los Fiscales y personal del Ministerio Publico no cuentan actualmente con la capacitación adecuada para este tipo de investigaciones.

9. ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?

Efectivamente hubo casos en los cuales el proceso judicial ha terminado en absoluciones debido a que no se ha preservado de manera correcta las pruebas digitales dentro de una investigación preparatoria.

10. ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?

Se requiere constante capacitación para los fiscales y personal administrativo del Ministerio Público, se requiere la elaboración de un protocolo de actuación donde se fije los lineamientos de actuación para este tipo de casos de delitos informáticos.

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos: Irving Poul Bustillos Villalta

Cargo: Fiscal Adjunto Provincial Penal

Institución: Ministerio Público

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

   La prueba digital es relevante en la investigación del delito de fraude informático pues cuenta es un delito que se comete en clandestinidad y con el uso de Tecnologías de información

2. ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?

   Si ha sido determinante pues constituye una de las pruebas más idóneas para resolver este tipo de casos.

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

3. ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?

Se presenta por ejemplo estados de cuenta bancarios, capturas de mensajes de texto donde se comenta sobre la operación realizada, capturas de Transferencias dinerarias.

4. ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?

En principio se requiere de forma documentada y luego de ser posible se revisa la fuente de prueba, es decir de donde proviene

5. ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?

El Ministerio Público como órgano constitucionalmente autónomo se encuentra sujeto a lo regulado en el C.P.P respecto al Tratamiento de la prueba en general.

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

6. ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?

En algunos casos se requieren direcciones IP o metadatos, que por lo general resulta ser una información compleja en su entendimiento

7. ¿Considera que el marco normativo vigente (como la Ley N.° 30096 o la Ley N.° 32314) es suficiente para sustentar su actuación fiscal en estos casos?

Considero que el marco normativo se encuentra en desarrollo y en constante cambio al avance tecnológico

8. ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba?

No pues si bien se creó hace un Tiempo las Fiscalías de Ciberdelincuencia hasta el momento no he visto reflejado su apoyo.

9. ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?

No hasta el momento.

10. ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?

En primer lugar una capacitación mayor en lo que es prueba digital y segundo quizas una modificación del C.P.P. para implementar de forma expresa la prueba digital.

IRVING POOL BUSTILLOS VILLALTA
FISCAL ADJUNTO PROVINCIAL
CUARTO DESPACHO
5ta. Fisc. Prov. Penal Corporativa
Distrito Fiscal de Lima Norte

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos: Elva Beneranda Cruz Mendez

Cargo: Fiscal Adjunta Provincial

Institución: Ministerio Público

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

   Considero que es central y determinante, ya que esto va a permitir reconstruir hechos con registros técnicos (transferencias, correos electrónicos y entre otros).

2. ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?

   Sí, en algunos casos estos han sido de mucha ayuda para poder reconstruir los hechos y poder lograr en algunos casos la identificación de los investigados y hasta la formalización de la investigación preparatoria.

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

3. ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?

   En su mayoría son los registros bancarios (movimientos, IP). Correos electrónicos, capturas de pantallas o la información que se puede extraer de un aparto electrónico.

ELVA BENERANDA CRUZ MENDEZ
FISCAL ADJUNTA PROVINCIAL
9° FISCALÍA PROVINCIAL PENAL CORPORATIVA
2° DESPACHO - DISTRITO FISCAL

4. ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?

   Los agraviados suelen remitir estas pruebas y estas son aseguradas en una cadena de custodia; también son mediante los requerimientos a bancos o empresas telefónicas para solicitar esa información y luego de ello ser incorporada a la carpeta fiscal. 3)

5. ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?

Existe el Reglamento de Cadena de Custodia del MP; Manual para el Recojo de Evidencia Digital (RM 848-2019-IN); lineamientos y guías de la Unidad Fiscal Especializada en Ciberdelincuencia.

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

6. ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?

   La falta de capacitación sobre los delitos informáticos, la demora en las respuestas de las entidades e inclusos de las partes agraviadas, y la brechas de equipamiento y peritaje.

7. ¿Considera que el marco normativo vigente (como la Ley N.° 30096 o la Ley N.° 32314) es suficiente para sustentar su actuación fiscal en estos casos?

No creo que sea suficiente, ya que se necesita un procedimiento más célere para la obtención de pruebas, además de ello, no en todos los casos se pueden adecuar a los nuevos delitos informáticos.

8. ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba?

ELVA BENERANDA CRUZ MENDEZ
FISCAL ADJUNTA PROVINCIAL
8° FISCALIA PROVINCIAL PENAL CORPORATIVA
2° DESPACHO - DISTRITO FISCAL DE LIMA NORTE

Es claro que al ser una fiscalía que ve delitos comunes y no una especializada, se requiere de una mayor capacitación para este tipo de delitos y así poder sacarle un mejor provecho a este tipo de pruebas digitales.

9. ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?

   Hasta la fecha no.

10. ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?

    Hacer un énfasis en realizar capacitaciones tanto para los fiscales, personal administrativo y demás entidades a las cuales se les solicita información para poder obtener estas pruebas.

ELVA BENERANDA CRUZ MENDEZ
FISCAL ADJUNTA PROVINCIAL
8° FISCALIA PROVINCIAL PENAL CORPORATIVA
2° DESPACHO - DISTRITO FISCAL DE LIMA NORTE

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos: Carlos Daniel Cabrel Rios

Cargo: Fiscal Adjunto Provincial

Institución: Ministerio Publico

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. **¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?**

   Es fundamental. En los delitos de fraude informático, la prueba digital no solo constituye el principal medio probatorio, sino que muchas veces es la única forma de evidenciar el modus operandi del investigado. Desde correos electrónicos, direcciones IP, transferencias bancarias virtuales, hasta el rastreo de dispositivos electrónicos, todo cobra valor probatorio.

2. **¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?**

   Sí, en la mayoría de los casos es determinante. En varios procesos, el acceso a registros de servidores, chats de WhatsApp o movimientos bancarios en línea han permitido reconstruir los hechos con precisión y lograr la formalización de la investigación preparatoria o incluso sentencias condenatorias.

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

3. **¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?**

   Principalmente registros de operaciones bancarias, capturas de pantalla, correos electrónicos, mensajes de redes sociales y archivos extraídos de celulares o computadoras mediante peritajes informáticos.

4. **¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?**

   Primero, se solicita su obtención mediante una diligencia fiscal, como una incautación o levantamiento del secreto de las comunicaciones. Luego, se incorpora el informe técnico del perito de informática forense, que da cuenta del contenido y de la cadena de custodia. Todo se registra formalmente en la carpeta fiscal.

5. **¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?**

   Sí, existe un Manual de Actuación Fiscal para Delitos Informáticos, y también lineamientos del Equipo Especializado en Ciberdelincuencia del Ministerio Público. Sin embargo, aún se requiere una mayor difusión y actualización de estos documentos para todos los despachos fiscales.

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

6. **¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?**

Hay varias: la falta de personal especializado, la demora en obtener información de proveedores de servicios digitales, y en algunos casos, la imposibilidad de acceder a datos alojados en el extranjero. También hay brechas tecnológicas entre el accionar delictivo y la capacidad investigativa.

7. **¿Considera que el marco normativo vigente (como la Ley N.° 30096 o la Ley N.° 32314) es suficiente para sustentar su actuación fiscal en estos casos?**
   Es un marco importante, pero necesita ajustes. La Ley N.° 30096 tipifica bien los delitos informáticos, pero no siempre se adecúa a los nuevos escenarios tecnológicos. Asimismo, se requiere fortalecer los mecanismos internacionales de cooperación para la obtención de prueba digital en el extranjero.
8. **¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba?**

   En general, no. Hay una clara necesidad de capacitación constante. Algunos despachos reciben apoyo del Equipo de Ciberdelincuencia, pero no todos los fiscales tienen un conocimiento técnico actualizado sobre la materia.

9. **¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?**

   Sí, ha ocurrido. Por ejemplo, cuando no se asegura la cadena de custodia o cuando no se logra sustentar la autenticidad del contenido digital, se debilita el caso y a veces no se puede continuar con la investigación.

10. **¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?**
    Primero, una capacitación técnica obligatoria para fiscales y asistentes. Segundo, mayor inversión en el área de pericias digitales y personal especializado. Y tercero, establecer protocolos ágiles de cooperación con entidades bancarias y plataformas tecnológicas.

CARLOS DANIEL CABREL RIOS
Fiscal Adjunto Provincial (P)
Cuarto Despacho
6to. Fiscalía Provincial Penal Corporativo
Distrito Fiscal de Lima Norte

GUÍA DE ENTREVISTA A EXPERTOS

Título: La prueba digital y su influencia en el delito de Fraude Informático en la Fiscalía Penal Provincial de Lima Norte, 2024

Nombre y apellidos: Karina Noemí Dávalos Navarro

Cargo: Fiscal Provincial

Institución: Ministerio Público

OBJETIVO GENERAL: Analizar de qué manera influye la prueba digital en el proceso de investigación del delito de fraude informático en la Fiscalía Penal Provincial de Lima Norte durante el año 2024.

1. ¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?

   Es muy relevante la prueba digital, ya que los delitos informáticos tienen relación con actos ilícitos que afectan los sistemas y datos informáticos que se cometen mediante el uso de tecnologías de la información o de la comunicación, por tanto, la prueba digital al ser una evidencia de carácter electrónica es el medio más idóneo para acreditar los hechos relacionados a los delitos informáticos.

2. ¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?

   Sí es muy importante pues la prueba digital tales como los correos, mensajes y audios a través de redes sociales, constituyen pruebas determinantes para la obtención de información corroborante de los delitos, ya que son el soporte a través de los cuales se concretizan estos delitos.

OE 1: Describir cómo se viene incorporando la prueba digital en los casos de fraude informático investigados por la Fiscalía Penal Provincial de Lima Norte, 2024.

KARINA NOEMI DAVALOS NAVARRO
FISCAL PROVINCIAL
5º FISCALIA PROVINCIAL
PENAL CORPORATIVA
CUARTO DESPACHO - D. F. LIMA NORTE

Escaneado con CamScanner

3. ¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?

   Los celulares y computadoras, que contienen información relacionada a mensajes y llamadas, almacenamiento o intercambio de información a través de redes sociales, las cámaras de videovigilancia públicos o privados.

4. ¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?

   Se debe proceder al aseguramiento de la escena del delito donde se encuentre la evidencia digital, antes del ingreso a la escena se debe coordinar con los peritos especializados para la forma de reconocer, identificar la evidencia digital relevante, para proceder a su adquisición y captura de la evidencia digital, luego se debe preservar la evidencia con la debida cadena de custodia.

5. ¿El Ministerio Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?

Si, contamos con el Manuel de Evidencia Digital además tenemos el Reglamento de la Cadena de Custodia de Elementos Materiales, Evidencias y Administración de Bienes Incautados, aprobado por la Resolución N° 729-2006-MP-FN. También se tiene el Manual para el recojo de la evidencia digital 2019, La guía de análisis digital forense aprobado mediante Resolución de la Gerencia General N° 000365-2020-MP-FN-GG y el Convenio de Budapest sobre el ciberdelito.

OE 2. Identificar los factores técnicos, normativos e institucionales que limitan la eficacia de la prueba digital en el esclarecimiento de los hechos durante la investigación fiscal, en Fiscalía Penal Provincial de Lima Norte, 2024.

KARINA NOEMI DAVALOS NAVARRO
FISCAL PROVINCIAL
5° FISCALIA PROVINCIAL
PENAL CORPORATIVA
CUARTO DESPACHO - D. F. LIMA NORTE

Escaneado con CamScanner

6. ¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraude informático?

La disponibilidad de peritos suficientes para la recolección de evidencia digital, sobre todo en los turnos fiscales, lo que genera un retraso en la obtención de la prueba digital.

La alta demanda de peritajes para el análisis de prueba digital, hace que se prioricen los casos emblemáticos, en desmedro de casos de menor relevancia pero que también requieren pruebas digitales.

La casi nula coordinación con otros países para identificar a los titulares de líneas telefónicas extranjeras.

La informalidad y facilidad con que se otorgan líneas telefónicas y se adquieren chips, permite la suplantación de identidad de personas, lo que dificulta identificar a la verdadera persona que adquiere la línea o servicio, ya que muchas veces se gestiona por medios virtuales donde no se deja rastro de la verdadera identidad.

7. ¿Considera que el marco normativo vigente (como la Ley N.° 30096 o la Ley N.° 32314) es suficiente para sustentar su actuación fiscal en estos casos?

Sí resulta suficiente por el momento, sin embargo, se ha incluido delitos comunes contra el Patrimonio, contra la Fe pública, entro otros, lo que me parece una técnica de legislación inadecuada, pues desnaturaliza lo que constituye propiamente el delito informático, que en mi criterio es el atentado contra los sistemas informáticos.

Ello por cuanto ahora cualquier delito común o especial se puede cometer a través de la informática y por ello ya se convertiría en un delito informático, lo que genera dificultad al momento de tipificar los delitos.

8. ¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitación adecuada sobre este tipo de prueba?

Aún estamos en proceso de aprendizaje de estas nuevas formas de adquisición de prueba digital. La Academia de la Magistratura, las universidades y los colegios

KARINA NOEMI DAVALOS NAVARRO
FISCAL PROVINCIAL
5° FISCALIA PROVINCIAL
PENAL CORPORATIVA
CUARTO DESPACHO - D. F. LIMA NORTE

Escaneado con CamScanner

profesionales cada vez ofrecen más cursos sobre la evidencia digital, incluso sobre el impacto de la Inteligencia Artificial en la comisión de delitos.

9. ¿Ha tenido casos en los que la deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?

Sí, por ejemplo, se ordenó la identificación de un usuario de una página de criptomonedas de un país extranjero que habría participado en una estaba en la compra de criptomonedas, sin embargo, a pesar que se hizo el patrullaje electrónico por parte de la unidad especializada de la Dirincri, de la Divindat, no se logró ubicar al titular de la cuenta, ello también fue generado, debido a que las cuentas se activan con seudónimos, lo que dificulta tener acceso al verdadero titular y la falta de coordinación con los servidores de estas cuentas que tienen alcance global, y es muy difícil contactas con el administrador de la cuenta para acceder a la información.

10. ¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?

. Fortalecer la unidad de peritajes digitales de la PNP y del Ministerio Público.

. Establecer mecanismos de coordinación con las unidades que contienen información de los titulares de los teléfonos celulares.

. Establecer mecanismos de identificación idónea de los titulares de las cuentas de redes sociales

. Adquirir dispositivos actualizados que permitan acceder de manera óptima a los dispositivos electrónicos para hacer un copiado de la información para la perennización y análisis correspondiente.

KARINA NOEMI DAVALOS NAVARRO
FISCAL PROVINCIAL
5° FISCALIA PROVINCIAL
PENAL CORPORATIVA
CUARTO DESPACHO - D. F. LIMA NORTE

Escaneado con CamScanner

Anexo D: Matriz de triangulación

Preguntas	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6	Experto 7	Experto 8	Conceptos identificados	Semejanzas	Diferencias	Interpretación
¿Qué tan relevante considera la prueba digital en el proceso de investigación del delito de fraude informático?	Es fundamental ya que, en la actualidad la criminalidad se ha expandido a través de los sistemas informáticos	Es relevante la información digital extraída de las aplicaciones de las entidades bancarias, pues comúnmente este tipo de delito se comete a través de las llamadas "bancas digitales".	La prueba digital para este tipo de delitos, resulta la más idónea en la investigación por la misma forma en que se comenten estos delitos.	Tiene relevancia, porque generalmente en este tipo de delitos las personas investigadas captan a las víctimas a través de correos electrónicos, mensajes de WhatsApp, mensaje de texto, siendo que las víctimas solamente cuentan con ese tipo de evidencias al momento de formular su denuncia.	La prueba digital es relevante en la investigación del delito de fraude informático, por cuanto es un delito que se comete en clandestinidad y con el uso de tecnología.	El entrevistado considera que es central y determinante, ya que esto va a permitir reconstruir hechos con registros técnicos (transferencias, correos electrónicos y entre otros).	Es fundamental. En los delitos de fraude informático, la prueba digital no solo constituye el principal medio probatorio, sino que muchas veces es la única forma de evidenciar el modus operandi del investigado. Desde correos electrónicos, direcciones IP, trasferencias bancarias	La prueba digital es relevante, ya que los delitos informáticos tienen relación con actos ilícitos que afectan los sistemas y datos informáticos que se comenten mediante el uso de tecnologías de la información o de la comunicación, por lo tanto, la prueba digital al ser una evidencia de carácter electrónica, es el medio más idóneo para acreditar los	Prueba digital Fraude informático Evidencia Investigación	Todas las respuestas coinciden en señalar que la prueba digital es fundamental o altamente relevante en la investigación del fraude informático. Esta percepción se basa en que el delito ocurre en entornos digitales, lo que convierte a este tipo de evidencia en el principal medio para esclarecer	Algunas respuestas brindan ejemplos concretos de pruebas digitales (como direcciones IP, rastreo de dispositivos o registros de transferencias). Una de las respuestas pone énfasis en que muchas veces las víctimas solo cuentan con pruebas digitales (como mensajes o correos)	La prueba digital es percibida como esencial y determinante en la investigación del delito de fraude informático, dado que este tipo de delito se comete íntegramente en entornos digitales, lo que convierte a las evidencias electrónicas en el principal medio probatorio disponible. Se destaca que estas pruebas no solo permiten

							virtuales, hasta el rastreo de dispositivos electrónicos, todo cobra valor probatorio.	hechos relacionados a los delitos informáticos.		los hechos. Existe consenso en que el fraude informático se comete mediante el uso de tecnologías, aplicaciones bancarias y plataformas digitales. Las respuestas coinciden en destacar que elementos como correos electrónicos, mensajes, transferencias y rastros tecnológicos tienen un alto	al momento de formular la denuncia. Algunas respuestas destacan que el fraude informático se comete en condiciones de clandestinidad, mientras otras enfatizan el uso habitual de plataformas bancarias y sistemas digitales como el medio principal del delito	identificar y vincular al sospechoso con el delito, sino también reconstruir los hechos mediante registros como transferencias, mensajes o rastros digitales. Asimismo, se subraya que en muchos casos, la única evidencia accesible para la víctima es de tipo digital, lo cual refuerza su valor en la etapa de denuncia y posterior investigación. Aunque las respuestas varían en

										valor probatorio.		grado de tecnicismo y profundidad, hay una coincidencia total en reconocer la relevancia de la prueba digital, tanto desde la perspectiva técnica como procesal.
¿Desde su experiencia, la prueba digital ha sido determinante para esclarecer los hechos en este tipo de delitos?	Es determinante, ya que te permite identificar la ubicación, el equipo que utilizó para el hecho ilícito e individualizar al autor o coautores.	Sí, justamente con el reporte extraído por las entidades bancarias que registra los movimientos no autorizados en plataformas digitales es que se llama a la ruta de las transacciones fraudulentas, logrando	Por su naturaleza delictiva, si resulta determinante, porque es muy difícil una prueba documental (material), sino la prueba digital permanece pendiente hasta su extracción oficial.	Si es determinante para resolver este tipo de casos, ya que, a través de estos medios de prueba, se puede llegar a identificar a las personas que envían los mensajes de correo electrónico, WhatsApp u otros a	Si es determinante, constituye una de las pruebas más idóneas para resolver este tipo de casos.	Si, en algunos casos estos han sido de mucha ayuda para poder reconstruir los hechos y poder lograr en algunos casos, la identificación de los investigados y hasta la formalización de la investigación preparatoria.	Si, en la mayoría de casos es determinante. En varios procesos, el acceso a registros de servidores, chats de WhatsApp o movimientos bancarios en línea, han permitido reconstruir los	Si es muy importante, ya que la prueba digital, tales como correos, mensajes y audios a través de redes sociales, constituyen pruebas determinantes para la obtención de información corroborante de los delitos, ya que son el soporte a	Identificación Ubicación Mensajes Transacciones	Las respuestas coinciden en señalar que la prueba digital es determinante para el esclarecimiento de delitos, especialmente aquellos relacionados con plataformas digitales y medios electrónicos. Todas	Las principales diferencias radican en el tipo específico de prueba digital resaltada: mientras algunos entrevistados destacan los movimientos bancarios y transacciones fraudulent	Desde la experiencia de los participantes, la prueba digital no solo es útil, sino crucial en delitos cometidos mediante medios tecnológicos. Su valor probatorio es altamente reconocido, ya que proporciona trazabilidad, respaldo y evidencia objetiva que

		identificarse a los autores.		sus víctimas.			hechos con precisión y lograr la formalización de la investigación preparatoria o incluso sentencias condenatorias.	través de los cuales se concretizan estos delitos.		destacan su capacidad para individualizar a los autores, reconstruir los hechos y respaldar legalmente los procesos de investigación. También se enfatiza que la información digital (mensajes, correos, registros bancarios) permanece como evidencia clave hasta ser oficialmente extraída.	as, otros hacen énfasis en mensajes de texto, correos electrónicos o chats. Asimismo, unos ponen el foco en la fase de identificación del autor, y otros en la formalización de la investigación preparatoria o incluso la obtención de sentencias condenatorias.	permite vincular hechos con responsables, especialmente en contextos donde la prueba física es inexistente o insuficiente. En consecuencia, se consolida como un pilar en las investigaciones modernas relacionadas con ciberdelitos y fraudes digitales.

¿Qué tipo de evidencia digital se presenta con mayor frecuencia en los casos que usted investiga?	Las transferencias bancarias que se realizan al introducir datos personales del titular de una cuenta y así poder disponer y generar un beneficio económico.	En casos en general, con mayor frecuencia se presentan los registros fílmicos y otros medios audiovisuales.	La más comunes son los movimientos de estados de cuenta, la extracción propia de información de aplicativos bancarios o monetario digital en los celulares	Generalmente los denunciantes presentan las capturas de pantalla de sus teléfonos celulares, donde reciben los mensajes por WhatsApp, asimismo, presentan las impresiones de los correos electrónicos que reciben de estas personas o de las entidades bancarias, comunicándoles a las personas los movimientos de dinero de su cuenta bancaria.	Se presenta, por ejemplo, estado de cuenta bancaria, captura de mensajes de texto donde se comunica sobre la operación realizada, capturas de transferencias dinerarios.	En su mayoría son los registros bancarios (movimientos, IP), correos electrónicos, capturas de pantallas o la información que se puede extraer de un aparato electrónico.	Principalmente registros de operaciones bancarias, captura de pantalla, correos electrónicos, mensajes de redes sociales y archivos extraídos de celulares o computadoras mediante peritajes informáticos.	Los celulares y computadoras, que contienen información relacionada a mensajes y llamadas, almacenamiento o intercambio de información a través de redes sociales, las cámaras de videovigilancia públicos o privados.	Registros Capturas Mensajes Correos	En las respuestas analizadas se identifica una fuerte coincidencia en la mención de evidencias vinculadas con información bancaria (como registros de transferencias, estados de cuenta y movimientos), así como el uso de capturas de pantalla provenientes de dispositivos móviles. También hay un patrón	Aunque todos coinciden en la presencia de evidencia digital, algunos enfatizan más la naturaleza bancaria (transferencias, IP, movimientos en aplicaciones financieras), mientras que otros destacan evidencia de comunicación, como mensajes y correos. También se diferencia en el nivel de profundidad:	La información recopilada sugiere que la evidencia digital más frecuente está directamente relacionada con los dispositivos personales (celulares y computadoras), destacando especialmente los elementos que estafan movimientos financieros o comunicaciones digitales. Esto indica que los delitos investigados suelen involucrar interacciones electrónicas documentad

										común en el uso de mensajes electrónicos o de redes sociales (WhatsApp, correos) y en la recolección de datos desde dispositivos electrónicos personales, como celulares o computadoras. En general, todos los encuestados coinciden en que la evidencia digital más común es la que puede extraerse directamente desde medios	algunos mencionan solamente tipos de documentos (capturas, correos), mientras otros detallan procedimientos técnicos como peritajes informáticos o recuperación de datos desde dispositivos. Por otro lado, no todos mencionan evidencia audiovisual o de videovigilancia, lo que sugiere diferencias en los	as, y que tanto víctimas como peritos recurren comúnmente a pruebas fácilmente accesibles y almacenables en medios digitales. La triangulación refuerza la importancia del manejo técnico y legal adecuado de esta evidencia en contextos judiciales o investigativos.

										electrónicos personales o plataformas digitales.	tipos de casos investigados.	
¿Cuál es el procedimiento habitual para incorporar la prueba digital a la carpeta fiscal?	A través del requerimiento del levantamiento de secreto de las comunicaciones y/o bancario.	Si el soporte es un USB, memoria, o CD, se incorpora mediante la cadena de custodia, y luego se introduce como medio probatorio a través de la preservación que se realiza generalmente mediante actas.	Las más recurrentes es la diligencia de extracción digital de información de un equipo celular. Otro es la extracción de información de correctos electrónicos, etc.	Preservar la evidencia digital (copia de los videos de seguridad, captura de pantalla, identificar dirección web, URL e ID de redes sociales, preservación de cuentas de redes sociales, captura de información volátil, entre otros).	En principio, se requiere de forma documental y luego, de ser posible, se revisa la fuente de prueba, es decir, de donde proviene.	Los agraviados suelen remitir estas pruebas y estas son aseguradas en una cadena de custodia. También son mediante los requerimientos a bancos o empresas telefónicas para solicitar esa información y luego de ello ser incorporada a la carpeta fiscal.	Primero, se solicita su obtención mediante una diligencia fiscal, como una incautación o levantamiento del secreto de las comunicaciones. Luego, se incorpora el informe técnico del perito de informática forense, que da cuenta del contenido y de la	Se debe proceder al aseguramiento de la escena del delito donde se encuentre la evidencia digital. Antes del ingreso a la escena, se debe coordinar con los peritos especializados para la forma de reconocer, identificar la evidencia digital relevante, para proceder a su adquisición y captura de la evidencia	Custodia Preservación Diligencia Evidencia	Todas las respuestas coinciden en que la incorporación de prueba digital a la carpeta fiscal requiere de procedimientos técnicos y legales que garanticen su validez, autenticidad y trazabilidad. Se enfatiza el uso de la cadena de custodia como mecanism	Las diferencias radican en el enfoque operativo o el momento específico del procedimiento que cada respuesta destaca. Algunas enfatizan el inicio del proceso mediante diligencias judiciales (como incautaciones o levantamiento del	La variedad de respuestas refleja que no existe un único procedimiento estandarizado, sino una serie de pasos adaptables según el tipo de prueba digital y el contexto del caso. Sin embargo, se puede interpretar que hay una estructura básica compartida: obtención legal de la prueba,

							cadena de custodia. Todo se registra formalmente en la carpeta fiscal.	digital, luego se debe preservar la evidencia con la debida cadena de custodia.		o fundamental para preservar la integridad de la evidencia digital, así como la intervención de peritos o diligencias fiscales como parte del proceso. Además, se señala que estas pruebas pueden provenir tanto de dispositivos físicos como de fuentes en línea (como redes sociales o correos electrónicos).	secreto de comunicaciones), mientras otras ponen el acento en la técnica de preservación (copias, capturas, actas). Asimismo, algunas respuestas hacen referencia explícita al rol del agraviado en el envío de pruebas o a la escena del delito como punto de inicio para la recolección.	intervención especializada, preservación técnica con cadena de custodia, y formalización en la carpeta fiscal. Esto sugiere un enfoque mixto entre lo jurídico y lo técnico, orientado a asegurar la admisibilidad de la prueba digital en el proceso penal.
¿El Ministerio	Sí	Desconozco	Específicamente no	No se cuenta de	El Ministerio	Existe el Reglamento de	Si, existe un	Si, se cuenta con el	Lineamientos	Las respuestas	Algunas respuestas	Aunque el Ministerio

Público cuenta con lineamientos que orienten el tratamiento de la prueba digital durante la investigación?			existe un lineamiento para el tratamiento de prueba digital; sin embargo, se trata de adoptar los actos de investigación.	manera formal con un protocolo de actuación para este tipo de investigaciones.	Público como órgano, constitucionalmente autónomo se encuentra sujeto a lo regulado en el Código Procesal Penal respecto al tratamiento de la prueba en general.	Cadena de Custodia del Ministerio Público, Manual para el recojo de evidencia Digital (RM 848-2019-IN), lineamientos y guías de la Unidad Fiscal Especializada en Ciberdelincuencia.	Manual de Actuación Fiscal para delitos informáticos, y también lineamiento del equipo especialista en ciberdelincuencia del Ministerio Público. Sin embargo, aún se requiere una mayor difusión y actualización de estos documentos para todos los despachos fiscales.	Manual de evidencia digital, además del Reglamento de la cadena de custodia de elementos materiales, evidencias y administración de bienes incautados, aprobado por la Resolución N° 729-2006-MP-FN.	Manuales Protocolo Prueba	coinciden en que sí existen documentos que orientan el tratamiento de la prueba digital, aunque con diferente nivel de conocimiento y aplicación entre los entrevistados. Se mencionan normativas como el Manual de evidencia digital, el Reglamento de cadena de custodia y guías específicas del Ministerio Público. Hay consenso	indican que sí existen lineamientos específicos y formales, mientras que otras mencionan que no hay un protocolo formal o que lo desconocen. También varía la percepción sobre la vigencia y difusión de estos documentos: algunos los reconocen como útiles pero poco difundidos o desactualizados, mientras	Público ha desarrollado ciertos lineamientos, manuales y reglamentos para el tratamiento de la prueba digital, existe una brecha entre la existencia normativa y su conocimiento o aplicación práctica. Esto revela una necesidad de mayor difusión, capacitación y actualización de los instrumentos existentes, así como de una uniformidad en la percepción y uso de estos

										en que hay esfuerzos normativos, aunque no todos los operadores los tienen plenamente identificados o implementados.	que otros dudan de su existencia o aplicabilidad directa en el contexto de prueba digital.	lineamientos entre los fiscales y operadores del sistema.
¿Cuáles son las principales dificultades que enfrenta al trabajar con prueba digital en casos de fraudes informático?	La demora en recibir la información por parte de las entidades privadas (bancarias o aplicativos).	Suele suceder que los equipos informáticos no cuentan con las características para soportar la reproducción de ciertas evidencias digitales, ya sea por problemas de software o hardware.	Lo primero es la falta de colaboración de los investigados, incluso de la parte agraviada, lo que nos lleva a solicitar los levantamientos que demoran en su respuesta.	No existe un protocolo de actuación para este tipo de casos, cada despacho fiscal investiga estos casos según su criterio	En algunos casos, se requieren direcciones IP o metadatos, que por lo general resulta ser una información compleja en su entendimiento.	La falta de capacitación sobre los delitos informáticos, la demora en las respuestas de las entidades e incluso de las partes agraviadas, y las brechas de equipamiento y peritaje.	Hay varias, la falta de personal especializado, la demora en obtener información de proveedores de servicio digitales y, en algunos casos, la imposibilidad de acceder a datos alojados	La disponibilidad de peritos suficientes para la recolección de evidencia digital, sobre todo en los turnos fiscales, lo que genera un retraso en la obtención de la prueba digital. La casi nula coordinación con otros países para identificar a los titulares	Demora Equipamiento Colaboración Capacitación	Todas las respuestas coinciden en señalar que existen obstáculos estructurales y técnicos para el tratamiento de la prueba digital en casos de fraude informático. En particular, se repite la demora	Las diferencias entre las respuestas radican en el énfasis que cada actor pone en los problemas específicos. Mientras algunos destacan más la limitación técnica o de equipamiento, otros hacen	Las dificultades en el manejo de prueba digital en casos de fraude informático revelan una combinación de carencias técnicas, organizativas y humanas dentro del sistema de justicia. La falta de equipamiento adecuado,

							en el extranjero. También hay brechas tecnológicas entre el accionar delictivo y la capacidad investigativa.	de líneas telefónicas extranjeras.		en la obtención de información, ya sea por parte de entidades privadas, proveedores digitales o incluso de los propios agraviados. También se menciona de forma reiterada la falta de preparación del personal, ya sea por la ausencia de capacitación o por la escasez de peritos especializados. La brecha tecnológic	hincapié en los problemas institucionales, como la falta de coordinación internacional o la ausencia de protocolos de actuación. También varía el enfoque en cuanto a la fuente de la demora: para unos, son las entidades privadas; para otros, los propios despachos fiscales o la falta de colaboración de los involucrados.	personal capacitado y protocolos estandarizados, sumada a la escasa cooperación de terceros (incluyendo empresas tecnológicas y víctimas), limita seriamente la capacidad del Estado para perseguir delitos informáticos de forma eficaz y oportuna. Esta situación evidencia la necesidad urgente de fortalecer capacidades institucionales y mejorar la articulación interinstitucional e internacional para hacer

										a y la inexistencia de protocolos claros son otros puntos en común que afectan directamente la eficacia de la investigación.		frente al creciente desafío del cibercrimen.
¿Considera que el marco normativo vigente (como la Ley N.º 30096 o la Ley N.º 32314) es suficiente para sustentar su actuación fiscal en estos casos?	Dicha ley como el código penal, busca la protección de los bienes jurídicos tutelados, pero no es suficiente porque se requiere un protocolo y un procedimiento célere que permita la obtención de	No es suficiente, además del marco normativo se requiere de mayores recursos, tanto humano como material para afrontar una investigación por delitos informáticos, es por ello que se deben crear	Todavía debería afinarse mejor dichas normativas.	No es suficiente, ya que es necesario contar con un protocolo de actuación para este tipo de casos, ya que en el distrito fiscal de Lima Norte no se cuenta con una fiscalía especializada en la materia.	El entrevistado considera que el marco normativo se encuentra en desarrollo y en constante cambio al avance tecnológico.	No es suficiente, ya que se necesita un procedimiento más célere para la obtención de pruebas, además de ello, no en todos los casos se pueden adecuar a los nuevos delitos informáticos.	Es un marco importante, pero necesita ajustes. La Ley N° 30096 tipifica bien los delitos informáticos, pero no siempre se adecua a los nuevos escenarios tecnológicos. Asimos, se	Si resulta suficiente por el momento; sin embargo, se ha incluido delitos comunes contra el Patrimonio, contra la fe pública, lo que parece una técnica de legislación inadecuada, ya que desnaturaliza lo que constituye	Normativa Protocolo Recursos Especialización	En general, las respuestas coinciden en que el marco normativo vigente (como la Ley N.º 30096 o la Ley N.º 32314) no es suficiente para sustentar adecuadamente la actuación fiscal	Las respuestas difieren en el grado de suficiencia que otorgan al marco normativo actual: mientras la mayoría considera que no es suficiente, uno de los entrevistados indica que sí lo es,	Las respuestas reflejan una percepción crítica y realista del marco normativo vigente, indicando que, si bien existen leyes que tipifican los delitos informáticos, estas resultan insuficientes ante los desafíos prácticos

	información rápida.	fiscalías especializadas en ciberdelincuencia en el distrito fiscal de Lima Norte.		Asimismo, en Lima Norte no se cuenta con una unidad especializada en ciberdelincuencia.			requiere fortalecer los mecanismos internacionales de cooperación para la obtención de prueba digital en el extranjero.	propiamente el delito informativo, que es un atentado contra los sistemas informáticos.		frente a delitos informáticos. Los participantes coinciden en la necesidad de protocolos claros, mayores recursos, y la especialización institucional (como fiscalías o unidades especializadas en ciberdelincuencia). Además, se señala la necesidad de una mayor celeridad en los procedimientos y ajustes normativos que	aunque con críticas a la técnica legislativa. Además, algunas opiniones ponen mayor énfasis en la necesidad de infraestructura institucional especializada, mientras que otras se centran en la necesidad de reformas legales o cooperación internacional. También hay quienes opinan que la ley está en	que enfrenta el Ministerio Público. La falta de protocolos, la lentitud en la obtención de pruebas, la ausencia de fiscalías especializadas y la necesidad de adaptar la normativa a nuevas formas delictivas evidencian una brecha entre la ley escrita y su aplicación efectiva. Esto sugiere la urgencia de una reforma integral que contemple tanto ajustes normativos como fortalecimiento

										respondan al dinamism o tecnológic o.	constante evolución, sugiriend o una visión más flexible del marco normativo .	institucional y técnico.
¿Cree que los fiscales y personal del Ministerio Público cuentan con la capacitació n adecuada sobre este tipo de prueba?	Dependien do en la especialida d que se desempeñe n, los fiscales y personal administrat ivo que ven todos los delitos no tienen el conocimie nto especializa do para realzar un trabajo estratégico a diferencia de los fiscales especializa dos en la materia	No todos los fiscales están debidament e capacitados , la investigaci ón de delitos informático s requiere de conocimien tos especializa dos, es por lo que resulta necesario que se amplíen las unidades de ciberdelinc uencia del Ministerio Público a	Tratándose de delitos “modernos” , aun es poca la capacitació n para el tratamiento de este tipo de pruebas	Los fiscales y personal del Ministro Público no cuentan actualmente con la capacitació n adecuada para este tipo de investigacio nes.	No, si bien se creó hace un tiempo las fiscalías de ciberdelincu encia, hasta el momento no se ha visto reflejado su apoyo.	Al ser una fiscalía que ve delitos comunes y no una fiscalía especializada, se requiere de una mayor capacitación para este tipo de delito y así poder sacarle un mejor provecho a este tipo de pruebas digitales.	En general no hay una clara necesidad de capacitaci ón constante. Algunos despachos reciben apoyo del equipo de ciberdelin cuencia, pero no todos los fiscales tienen un conocimie nto técnico actualizad o sobre la materia.	Aún se está en proceso de aprendizaje de estas nuevas formas de adquisición de prueba digital. La Academia de la Magistratura , las universidade s y los colegios profesionales , cada vez ofrecen más cursos sobre la evidencia digital, incluso sobre el impacto de la inteligencia artificial en	Capacitaci ón Fiscales Ciberdelinc uencia Conocimie nto	Todas las respuestas coinciden en señalar que la capacitaci ón actual es insuficient e para enfrentar adecuada mente la investigac ión de delitos informátic os y el manejo de pruebas digitales. Se reconoce que los conocimie ntos técnicos especializ	Algunas respuestas matizan la situación diferencia ndo entre fiscales especializ ados y no especializ ados, destacand o que los primeros sí tienen herramien tas y conocimie ntos adecuados . Otras respuestas remarcan que a pesar de la existencia de	Se puede interpretar que el Ministerio Público enfrenta un reto estructural en la formación continua y especializad a de su personal frente a la evolución tecnológica de los delitos. Aunque hay conciencia institucional sobre la necesidad de capacitar, las acciones implementa das no han

	que cuenta con el conocimiento y las herramientas	otros distritos fiscales además de Lima Centro.						la comisión de delitos.		ados son necesarios y que no todos los fiscales cuentan con ellos, aunque existen intentos de formación o apoyo en algunas unidades específicas, como las fiscalías de ciberdelincuencia.	fiscalías especializadas, no se percibe un impacto real. También hay quienes resaltan los esfuerzos de capacitación en curso, aunque aún sean incipientes o insuficientes, señalando el papel de instituciones como la Academia de la Magistratura o universidades.	alcanzado cobertura ni profundidad suficiente, generando una brecha entre la demanda del sistema penal y la preparación del recurso humano para afrontar la prueba digital y los delitos informáticos.
¿Ha tenido casos en los que la	Sí	No hasta el momento.	Una dificultad es la	Hubo casos en los cuales, el	No hasta el momento.	Hasta la fecha no.	Si, por ejemplo, cuando no	Sí, pero, a pesar de los esfuerzos de	Prueba Identidad	Las respuestas coinciden	Algunas respuestas señalan	Existe una percepción compartida

deficiente actuación respecto a la prueba digital haya influido en un archivo o en la imposibilidad de formalizar la investigación?			utilización de cuentas de personas iletradas que son captadas para crear estas cuentas y dificulta la identidad de quien usan realmente estas cuentas.	proceso judicial ha terminado en absoluciones debido a que no se ha preservado de manera correcta las pruebas digitales dentro de una investigación preparatoria.			se asegura la cadena de custodia o cuando no se logra sustentar la autenticidad del contenido digital, se debilita el caso y a veces no se puede continuar con la investigación.	las autoridades para identificar a un usuario de criptomoneda involucrado en una estafa, no fue posible ubicar al titular de la cuenta debido al uso de seudónimos y la falta de coordinación con los servidores de alcance global.	Custodia Investigación	en que existen riesgos reales para la investigación cuando no se manejan adecuadamente las pruebas digitales. Se repite la preocupación por la cadena de custodia, la autenticidad del contenido digital y la dificultad para identificar a los usuarios reales detrás de cuentas virtuales. Aunque algunos entrevistados aún	experiencias directas con consecuencias graves, como absoluciones por mala preservación de pruebas, mientras que otras indican que, hasta el momento, no han enfrentado ese tipo de situaciones. Además, algunas menciones se enfocan en aspectos técnicos (cadena de custodia), mientras que otras	sobre la fragilidad de la prueba digital como elemento clave en una investigación penal, especialmente si no se maneja correctamente. La evidencia digital, por su naturaleza técnica y su contexto global, presenta desafíos tanto en su obtención como en su validación, lo que puede comprometer la formalización de la investigación o favorecer la impunidad. Aunque no todos los

										no han tenido experiencias directas, reconocen el problema como potencial o han presenciado casos cercanos.	abordan obstáculos estructurales como el anonimato digital y la falta de cooperación internacional.	actores han vivido estas fallas, hay una conciencia latente sobre su impacto potencial.
¿Qué medidas considera prioritarias para fortalecer el uso eficaz de la prueba digital en las investigaciones fiscales?	La implementación de fiscalías especializadas en ciberdelincuencia a nivel nacional con las herramientas tecnológicas adecuadas.	Ampliación de recursos para la adquisición de mejores equipos informáticos, y contratación de personal especializado (ingenieros informáticos) en cada distrito fiscal, que puedan realizar asesorías o acompañamiento en	Una mayor capacitación en las entidades, así como legislación para entidades bancarias o de tesorería.	Se requiere constante capacitación para los fiscales y personal administrativo del Ministerio Público, se requiere la elaboración de un protocolo de actuación donde se fije los lineamientos de actuación para este tipo de casos de	En principio, una capacitación masiva en lo que es prueba digital y, segundo, una modificación del Código Procesal Penal para implementar de forma expresa la prueba digital.	Hacer un énfasis en realizar capacitaciones tanto para los fiscales, personal administrativo y demás entidades a las cuales se les solicita información para obtener estas pruebas.	Primero, una capacitación técnica obligatoria para fiscales y asistentes. Segundo, mayor inversión en el área de pericias digitales y personal especializado. Y, tercero, establecer protocolos agiles de cooperación con	- Fortalecer la unidad de peritajes digitales de la PNP y del Ministerio Público - Establecer mecanismos de coordinación con las unidades que contienen información de los titulares de los teléfonos celulares - Establecer mecanismos de identificación idónea de	Capacitación Protocolos Tecnología Especialistas	Todas las respuestas coinciden en que el fortalecimiento del uso de la prueba digital requiere una capacitación constante y técnica del personal fiscal y administrativo, así como la incorporación de personal	Las diferencias se presentan principalmente en el énfasis y el alcance de las propuestas. Algunas respuestas priorizan la creación de fiscalías especializadas o unidades específicas dentro	Las respuestas reflejan una visión compartida sobre la necesidad de modernizar y especializar el sistema fiscal frente a los desafíos del entorno digital. Se interpreta que los actores involucrados perciben un vacío tanto en

		las investigaciones.		delitos informáticos.			entidades bancarias y plataformas tecnológicas.	los titulares de las cuentas de redes sociales.		especializado en tecnologías de la información. Además, existe consenso en la necesidad de contar con protocolos claros para el manejo de evidencia digital, y se resalta la importancia de mejorar la infraestructura tecnológica y los recursos disponibles para las investigaciones.	del Ministerio Público o la Policía, mientras que otras hacen hincapié en la modificación normativa, como la actualización del Código Procesal Penal. También varía el enfoque sobre con quién debe establecerse coordinación: algunos mencionan entidades bancarias, otros plataformas tecnológicas o	capacidades técnicas como en regulación normativa y cooperación interinstitucional, lo cual obstaculiza el uso eficaz de la prueba digital. Por tanto, el fortalecimiento debe ser integral, incluyendo formación, normativa, infraestructura y colaboración estratégica.

											proveedores de servicios móviles.	