UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

TESIS:

Valoración de la evidencia digital en sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga.

Para optar el título profesional de:
ABOGADO

PRESENTADO POR:
Bach. Jhonatan CISNEROS OLANO

ASESOR:
Mtro. Arturo CONGA SOTO

AYACUCHO - PERÚ

2026

DEDICATORIA

A mis padres, Feliciano y Teresa Elizabeth, por ser el pilar fundamental de mi vida. Cada esfuerzo en este camino lleva implícito su apoyo, amor y enseñanzas. A mis hermanos por motivarme a seguir adelante en cada etapa de este proceso.

AGRADECIMIENTO

A mis docentes de la Facultad de Derecho y Ciencias Políticas por su invaluable contribución en mi formación profesional y de modo particular, a mi asesor, por su experticia académica y orientación.

INDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tuvo como objetivo analizar la valoración de la evidencia digital en las sentencias por delito de fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga durante el período 2022-2024, determinando su grado de ajuste a los estándares técnicos y legales vigentes. El estudio adoptó un enfoque cualitativo, de tipo básico y de nivel descriptivo-explicativo, con un diseño no experimental y transversal. La muestra estuvo conformada por cinco sentencias y seis operadores de justicia (tres jueces y tres fiscales), seleccionados mediante muestreo intencional. Las técnicas empleadas fueron el análisis documental y la entrevista semiestructurada, utilizando como instrumentos una ficha de análisis documental y una guía de entrevista.

Los resultados evidencian que, en el 100% de las sentencias analizadas, no se aplicaron criterios técnicos de valoración de evidencia digital como autenticidad, integridad, cadena de custodia y fiabilidad. En las sentencias con debate probatorio, la evidencia digital fue tratada como prueba documental tradicional; en las sentencias conformadas, la aceptación de cargos sustituyó cualquier valoración técnica. Las principales limitaciones identificadas fueron: ausencia de laboratorio forense informático en Huamanga, déficit formativo de jueces y fiscales, demoras de meses en los peritajes derivados a Lima, y uso generalizado de la conclusión anticipada (60% de los casos). Asimismo, se evidenció una brecha significativa entre el discurso sofisticado de las sentencias y la práctica judicial real, que se limita a verificar la presencia del nombre del acusado en el reporte bancario impreso.

Se concluye que la valoración de la evidencia digital en los Juzgados Penales Unipersonales de Huamanga es predominantemente implícita, informal y asimilada a la prueba documental tradicional, sin aplicación de criterios técnico-forenses, lo que constituye una deficiencia estructural en la prueba del delito de fraude informático en dicho distrito judicial.

Palabras clave: Evidencia digital, fraude informático, valoración probatoria, cadena de custodia, conclusión anticipada.

ABSTRACT

This research aimed to analyze the assessment of digital evidence in judgments for computer fraud offenses issued by the Single-Member Criminal Courts of Huamanga during the period 2022-2024, determining its degree of alignment with current technical and legal standards. The study adopted a qualitative approach, basic type and descriptive-explanatory level, with a non-experimental and cross-sectional design. The sample consisted of five judgments and six justice operators (three judges and three prosecutors), selected through intentional sampling. The techniques employed were documentary analysis and semi-structured interview, using a documentary analysis form and an interview guide as instruments.

The results show that, in 100% of the analyzed judgments, technical criteria for assessing digital evidence such as authenticity, integrity, chain of custody, or reliability were not applied. In judgments with evidentiary debate, digital evidence was treated as traditional documentary evidence; in plea agreement judgments, the acceptance of charges replaced any technical assessment. The main limitations identified were: absence of a computer forensic laboratory in Huamanga, lack of training for judges and prosecutors, months-long delays in expert reports sent to Lima, and widespread use of early plea agreement (60% of cases). Likewise, a significant gap was evidenced between the sophisticated discourse of the judgments and the actual judicial practice, which is limited to verifying the presence of the accused's name on the printed bank report.

It is concluded that the assessment of digital evidence in the Single-Member Criminal Courts of Huamanga is predominantly implicit, informal, and assimilated to traditional documentary evidence, without application of technical-forensic criteria, which constitutes a structural deficiency in the proof of the computer fraud offense in said judicial district.

Keywords: Digital evidence, computer fraud, evidentiary assessment, chain of custody, early plea agreement.

INTRODUCCIÓN

La creciente digitalización de las transacciones financieras y el uso masivo de la banca por Internet han generado un aumento exponencial de los delitos de fraude informático en el Perú. Este fenómeno, acelerado por la pandemia de la COVID-19, ha puesto en evidencia las limitaciones del sistema de justicia penal para investigar y juzgar adecuadamente estas conductas ilícitas, particularmente en distritos judiciales del interior del país como Huamanga (Ayacucho), donde la ausencia de laboratorios forenses informáticos, la escasa formación especializada de los operadores de justicia y la generalización de la conclusión anticipada como vía de resolución de casos han generado una práctica de valoración probatoria que trata la evidencia digital como si fuera prueba documental tradicional.

La presente investigación tiene como objetivo general analizar la valoración de la evidencia digital en las sentencias por delito de fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga, determinando el grado de ajuste de dicha valoración a los estándares técnicos y legales vigentes. Para ello, se plantean tres objetivos específicos: identificar los criterios técnicos aplicados por los jueces, describir las limitaciones que enfrentan los operadores de justicia, y contrastar la valoración documentada en las sentencias con los discursos y prácticas declaradas por jueces y fiscales.

El documento se estructura en seis capítulos. El Capítulo I desarrolla el planteamiento del problema, incluyendo la descripción de la realidad problemática, la formulación de problemas y objetivos, así como la justificación e importancia de la investigación. El Capítulo II presenta el marco teórico, que comprende los antecedentes de estudio, las bases teóricas sobre fraude informático, evidencia digital, debido proceso, cadena de custodia y valoración judicial, así como el marco conceptual. El Capítulo III expone los supuestos, las categorías y la matriz de categorización. El Capítulo IV describe la metodología empleada, de enfoque cualitativo, tipo básico, nivel descriptivo-explicativo y diseño no experimental, incluyendo la población, muestra, técnicas e instrumentos de recolección de datos. El Capítulo V presenta la interpretación y discusión de resultados, donde se analizan los hallazgos del análisis documental de cinco sentencias y de las entrevistas a seis operadores de justicia. Finalmente, el Capítulo VI contiene las conclusiones y recomendaciones derivadas de la investigación.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

El delito de fraude informático, tipificado en el artículo 8° de la Ley N° 30096 (modificada por la Ley N° 30171), ha experimentado un crecimiento exponencial en el Perú durante los últimos años. La progresiva digitalización de las transacciones financieras, el uso masivo de la banca por internet y la migración forzada de actividades económicas al entorno virtual —acelerada por la pandemia de la COVID-19— han ampliado significativamente el espectro de oportunidades para la comisión de ilícitos informáticos. Según datos de la Superintendencia de Banca, Seguros y AFP (SBS), las denuncias por transferencias no consentidas y fraudes electrónicos se han incrementado sostenidamente, afectando a miles de ciudadanos que ven comprometidos sus ahorros y su confianza en el sistema financiero.

En el distrito judicial de Huamanga (Ayacucho), esta problemática adquiere características particulares. A diferencia de los distritos judiciales de Lima o Callao, donde existen divisiones especializadas en delitos de alta tecnología y laboratorios forenses informáticos, Huamanga carece de infraestructura técnica y personal especializado para la investigación y juzgamiento de este tipo de ilícitos. Los fiscales deben derivar los peritajes informáticos a Lima, con las consiguientes demoras que pueden extenderse por meses o incluso más de un año. Esta situación genera una tensión entre el derecho del imputado a un plazo razonable de duración del proceso y el derecho del agraviado a una tutela judicial efectiva.

Frente a este contexto, los operadores de justicia de Huamanga han optado mayoritariamente por la conclusión anticipada del juicio (conformidad) como vía de resolución de los casos de fraude informático. Esta figura procesal, regulada en el artículo 372° del Código Procesal Penal, permite al imputado aceptar los cargos formulados por el Ministerio Público a cambio de una reducción de la pena, evitándose así el despliegue de la actividad probatoria en juicio oral. Si bien la conformidad es un mecanismo legítimo y eficiente desde una perspectiva de descongestión procesal, su uso generalizado en materia de fraude informático tiene un efecto colateral preocupante: impide que los jueces se enfrenten al desafío de valorar técnicamente la evidencia digital.

La evidencia digital —entendida como aquella información con valor probatorio almacenada o transmitida en formato binario que requiere de herramientas o conocimientos especializados para su correcta interpretación— presenta características que la diferencian sustancialmente de la prueba documental tradicional. Su naturaleza maleable, su facilidad de alteración sin dejar rastros evidentes y la necesidad de controles específicos como la cadena de custodia, el hash de verificación de integridad y el análisis forense de los dispositivos o sistemas involucrados, exigen un tratamiento probatorio diferenciado. Sin embargo, el análisis de las sentencias emitidas por los Juzgados Penales Unipersonales de Huamanga en casos de fraude informático revela una ausencia sistemática de aplicación de estos criterios técnicos.

En las sentencias absolutorias, la evidencia digital —generalmente limitada a reportes bancarios impresos— es valorada implícitamente como prueba documental tradicional, sin que el juez verifique su autenticidad o integridad. La absolución, cuando ocurre, no se basa en un análisis técnico que revele la insuficiencia probatoria, sino en la ausencia de prueba directa (como cámaras de seguridad) que la Fiscalía no pudo recabar por limitaciones materiales. En las sentencias condenatorias producto de la conclusión anticipada, directamente no existe valoración probatoria alguna, pues la aceptación de cargos por parte del imputado sustituye la actividad probatoria. Incluso en los escasos casos que llegan a juicio oral con debate contradictorio, los jueces no aplican criterios técnicos de valoración de evidencia digital, tratando los reportes bancarios como si fueran documentos en papel.

Esta realidad plantea una paradoja preocupante: cuanto más se tecnifica el delito, menos técnica es la prueba que se presenta y valora en el proceso penal. El fraude informático, que por definición implica la manipulación de sistemas informáticos, se prueba casi exclusivamente con reportes bancarios impresos, sin peritajes forenses, sin cadena de custodia, sin verificación de integridad. Y los jueces, carentes de formación especializada y enfrentados a limitaciones materiales y procesales, convalidan esta práctica, ya sea absolviendo por falta de prueba o condenando en virtud de conformidades que eluden cualquier análisis técnico.

La presente investigación se justifica, entonces, por la necesidad de describir, analizar y comprender cómo se está valorando la evidencia digital en los Juzgados Penales Unipersonales de Huamanga, identificando las deficiencias técnicas, las limitaciones

institucionales y las prácticas procesales que explican esta situación. Solo a partir de dicho diagnóstico será posible formular recomendaciones orientadas a mejorar la calidad de la valoración probatoria en esta materia, garantizando al mismo tiempo los derechos de las víctimas y los imputados en un contexto de creciente digitalización de la delincuencia patrimonial.

1.2. Formulación del problema

1.2.1. Problema principal

¿Cómo se valora la evidencia digital en las sentencias por delito de fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga durante el período 2022-2024, y en qué medida dicha valoración se ajusta a los estándares técnicos y legales vigentes?

1.2.2. Problemas secundarios

- ¿Qué criterios técnicos de valoración de evidencia digital (autenticidad, integridad, cadena de custodia, fiabilidad) son explícita o implícitamente aplicados por los jueces en las sentencias por fraude informático emitidas en los Juzgados Penales Unipersonales de Huamanga entre 2022 y 2024?

- ¿Cuáles son las principales limitaciones o dificultades que enfrentan los operadores de justicia (jueces, fiscales, peritos) en Huamanga para valorar técnicamente la evidencia digital en casos de fraude informático?

- ¿Existe coherencia entre la valoración de la evidencia digital documentada en las sentencias y los discursos o prácticas declaradas por los operadores de justicia sobre cómo debería valorarse dicha evidencia?

1.3. Formulación de objetivos

1.3.1. Objetivo General

Analizar la valoración de la evidencia digital en las sentencias por delito de fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga, determinando el grado de ajuste de dicha valoración a los estándares técnicos y legales vigentes.

1.3.2. Objetivo Específico

- Identificar los criterios técnicos de valoración de evidencia digital (autenticidad, integridad, cadena de custodia, fiabilidad) que son explícita o implícitamente aplicados por los jueces en las sentencias por fraude informático emitidas en los Juzgados Penales Unipersonales de Huamanga entre 2022 y 2024.

- Describir las principales limitaciones o dificultades que enfrentan los operadores de justicia en Huamanga para valorar técnicamente la evidencia digital en casos de fraude informático.

- Contrastar la valoración de la evidencia digital documentada en las sentencias con los discursos y prácticas declaradas por los operadores de justicia, a fin de determinar el nivel de coherencia entre ambos planos.

1.4. Justificación e importancia

La presente investigación se justifica por las siguientes razones:

a. **Justificación teórica.** El estudio contribuye al desarrollo del conocimiento sobre la prueba digital en el proceso penal peruano, específicamente en el delito de fraude informático. Aunque existe literatura extranjera sobre estándares de valoración de evidencia digital, son escasos los estudios empíricos que analizan cómo los jueces peruanos, particularmente en distritos judiciales fuera de Lima, aplican —o dejan de aplicar— dichos estándares. La investigación busca llenar este vacío mediante el análisis sistemático de sentencias y entrevistas a operadores de justicia.

b. **Justificación práctica.** Los hallazgos de la investigación podrán ser utilizados por los operadores de justicia de Huamanga y de otros distritos judiciales con características similares para identificar las deficiencias en la valoración de la evidencia digital y para diseñar estrategias de mejora, ya sea mediante capacitaciones especializadas, la implementación de protocolos de cadena de custodia o la asignación de recursos para la creación de laboratorios forenses informáticos.

c. **Justificación metodológica.** La investigación propone un enfoque cualitativo que combina el análisis documental de sentencias con entrevistas semiestructuradas a jueces y fiscales. Esta triangulación de fuentes y métodos permite abordar la problemática desde múltiples perspectivas, generando resultados más robustos y confiables que aquellos que se obtendrían utilizando un único método.

d. **Justificación social.** El fraude informático afecta a un número creciente de ciudadanos que ven comprometidos sus ahorros y su confianza en el sistema financiero. Una deficiente valoración de la evidencia digital puede llevar a dos resultados igualmente problemáticos: la absolución de responsables por falta de prueba técnica (dejando a las víctimas sin justicia) o la condena de inocentes basada en pruebas no verificadas técnicamente. La investigación contribuye a identificar las causas de esta problemática y a proponer soluciones orientadas a garantizar una administración de justicia más eficaz y confiable en esta materia.

1.4.1. Importancia

La presente investigación adquiere especial importancia en el contexto de la creciente digitalización de la delincuencia patrimonial y la consecuente necesidad de que el sistema de justicia penal desarrolle herramientas conceptuales y prácticas para abordar la prueba digital con rigurosidad técnica. En el distrito judicial de Huamanga, donde la ausencia de laboratorios forenses informáticos, la escasa formación especializada de los operadores de justicia y la generalización de la conclusión anticipada como vía de resolución de casos han generado una práctica de valoración probatoria que trata la evidencia digital como si fuera prueba documental tradicional, resulta fundamental comprender las causas y consecuencias de esta situación. Los hallazgos de la investigación permitirán identificar las brechas entre los estándares técnicos internacionalmente aceptados —como la cadena de custodia, la verificación de integridad mediante hash y el análisis forense de dispositivos— y la práctica judicial real en el distrito judicial de Ayacucho, brindando insumos para el diseño de políticas de capacitación, asignación de recursos y mejora de los protocolos de investigación y juzgamiento en materia de delitos informáticos, en beneficio tanto de las víctimas que demandan justicia como de los imputados que tienen derecho a un proceso con garantías.

1.4.2. Viabilidad de la investigación

La investigación fue viable por diversas razones. En primer lugar, se contó con acceso directo a las fuentes documentales primarias, toda vez que las sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga son de carácter público y pueden ser solicitadas al Poder Judicial, previa identificación de los expedientes mediante búsqueda en el sistema de consulta de expedientes judiciales (Sistema Integrado Judicial). En segundo lugar, se cuenta con la disposición de los operadores de justicia para participar en las entrevistas, habiéndose establecido contactos preliminares con jueces y fiscales del distrito judicial de Huamanga, quienes han manifestado su interés en colaborar con una investigación que aborda una problemática que ellos mismos reconocen como deficitaria y necesitada de análisis. En tercer lugar, el investigador contó con la formación metodológica necesaria para desarrollar el análisis documental cualitativo de las sentencias y para realizar entrevistas semiestructuradas, así como con el tiempo y los recursos materiales (grabadora, software de procesamiento de textos, acceso a internet) que demanda el trabajo de campo. Finalmente, el alcance de la investigación —cinco sentencias y seis entrevistas— es realista y proporcionado.

1.5. Limitaciones de estudio

Se ha identificado como principal limitación la escasa disponibilidad de información en bases de datos nacionales respecto a la evidencia digital. Asimismo, se advirtió la escasa existencia de investigaciones específicas sobre el delito de fraude informático y, principalmente, sobre la valoración de la evidencia digital en el proceso penal en el contexto local de Ayacucho.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de estudio

2.1.1. Antecedentes internacionales

Pecchioni (2024) Estafa informática: el caso de la incorporación de la prueba digital en el proceso penal de Córdoba. Esta tesis se enfoca en el análisis exhaustivo de la prueba digital en el ámbito de los delitos de estafa informática dentro de la provincia de Córdoba. En cuanto al período temporal durante el cual se realizó la investigación, el mismo abarca un año calendario. Como parte del objeto de estudio se incorporaron datos previos o históricos comprendidos entre enero del año 2019 hasta diciembre del año 2023. Ante la notable proliferación de actividades delictivas en entornos digitales, se propone una investigación profunda sobre la valoración y utilización de la evidencia digital en el contexto del proceso penal Cordobés. La intersección entre la prueba digital y el fraude informático es explorada minuciosamente, considerando las condiciones necesarias para su admisión y ponderación en el escenario jurídico. Además, se aborda con meticulosidad el rol y las responsabilidades atribuidas a las unidades judiciales y entidades especializadas en el tratamiento de la prueba digital en casos de estafa informática. El presente trabajo académico se sumerge en la comprensión de la naturaleza y características inherentes a la prueba digital, y cómo estas interactúan con los requerimientos de la esfera penal. Un enfoque cualitativo se adopta para captar las voces y perspectivas de múltiples actores involucrados, igualmente, se lleva a cabo un minucioso análisis documental, que abarca desde informes y estudios previos hasta jurisprudencia y documentos legales que rigen la materia en la provincia de Córdoba.

Vadell, L., & Rúa, M (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. El artículo analiza algunas cuestiones problemáticas sobre la obtención, admisibilidad y valoración, en el proceso penal, de la prueba digital producto de la vigilancia secreta, en el marco de la era digital, desde una perspectiva comparada a partir de la experiencia española. Para ello, se presentan nociones y características de la prueba digital, y se plantean algunas problemáticas que representa este tipo de prueba en el proceso penal. Luego, se analizan las implicaciones de la obtención, admisibilidad y valoración de la

prueba digital cuando ha sido producto de la vigilancia secreta. Finalmente, se presentan las reflexiones conclusivas sobre el tema.

Avila Contreras, L., & Serrano Campoverde (2024) Eficacia de las pruebas electrónicas en el sistema judicial mediante criterios específicos de peritaje. La creciente necesidad de pruebas digitales en el ámbito judicial es un fenómeno global que exige la implementación de un marco de preservación de pruebas electrónicas que sea confiable y efectivo. El correcto mantenimiento de la cadena de custodia es crucial para asegurar que se garantice la justicia en los tribunales. Sin embargo, es importante reconocer que los seres humanos representan el eslabón más vulnerable en cualquier cadena de confianza. En este contexto, la tecnología blockchain emerge como una solución prometedora para la preservación de pruebas electrónicas, especialmente en el ámbito del Internet de las Cosas (IoT). Blockchain permite almacenar y analizar datos de pruebas digitales de manera segura y confidencial, estableciendo un marco robusto de control de acceso que protege la integridad de la información. Al integrar esta tecnología en el proceso de gestión de evidencias, se puede minimizar el riesgo de manipulación y garantizar la trazabilidad y autenticidad de las pruebas, fortaleciendo así la confianza en el sistema judicial. En esta investigación se definió un conjunto de seis criterios específicos de peritaje para que sean incluidos en la normativa procesal ecuatoriana. Adicionalmente se propuso un marco de preservación de pruebas electrónicas basado en blockchain para el IoT que implementa la cadena de custodia y utiliza la plataforma Ethereum para resforzar los principios de descentralización y transparencia que son fundamentales para la tecnología blockchain. La viabilidad de la propuesta se realizó mediante criterio de expertos, la cual fue evaluada como muy pertinente.

2.1.2. Antecedentes nacionales

Flores Sánchez, M. L., & Guevara Castillo, J. E. (2021). La valoración probatoria de evidencias digitales como estrategia de investigación para prácticas corruptas en los delitos colusorios. La valoración probatoria de evidencias digitales como estrategia de investigación para prácticas corruptas en los delitos colusorios. Esta investigación tiene como principal objetivo determinar cuáles son los criterios probatorios en las evidencias digitales que se incorporarían en el Código Procesal Penal para investigar las prácticas corruptas en el delito de colusión, ante ello se desarrolló como principales teorías: la

prueba, prueba digital, principios, valoración de las evidencias digitales y el delito de colusión. Para el desarrollo de esta investigación se tuvo en cuenta el diseño de investigación cuantitativo, y tipo de investigación descriptivo; así mismo se tuvo una población conformado por jueces penales, fiscales penales y los abogados inscritos en el Ilustre Colegio de Abogados de Lambayeque; obteniéndose una muestra de 5 jueces penales, 5 fiscales penales y 60 abogados penalistas, aplicándoseles la técnica de la encuesta e instrumento el cuestionario. Después de que se haya aplicado el cuestionario se obtuvieron diversos resultados, siendo el principal que, se debe regular de manera expresa en nuestro Código Procesal Penal los criterios de valoración de la evidencia digital. Llegándose a la conclusión que, se debe regular de manera expresa dichos criterios en el artículo 185-A del Código Procesal Penal.

Cadillo Quispe, B. A. (2022). La evidencia digital en el cibercrimen - Perú 2022. La presente investigación tiene por objetivo identificar cual es el procedimiento normativo adecuado para la obtención de la evidencia digital en el cibercrimen, estando a que dicha evidencia conlleva un valor probatorio y puede encontrarse almacenada en un “Hardware”, (terabyte, celulares, laptops, USB, DVD u otro), así como también pueda encontrarse en “Software” de repositorio (Google Drive, Dropbox y One Drive u otro) almacenamientos en la red. La identificación normativa del procedimiento implica que el operador de justicia identifique el mecanismo normativo aplicado adecuado de aseguramiento de la evidencia digital, ya que su no aplicación conllevaría a que la evidencia digital en delitos abarcados en el Cibercrimen pueda ser alterada, dañada, destruida, y como resultado de ello, el operador experto “perito” no logre un resultado idóneo o en su defecto no pueda realizar el análisis del mismo con aras de elaborar un elemento probatorio que determine la conducta delictiva del sujeto activo a lo largo del proceso penal. Es en esa medida, que la importancia del procedimiento normativo adecuado conlleva a que dicha evidencia digital tenga la categoría de “prueba digital”, a nivel la etapa de juicio oral habiendo previamente pasado por el control del juez en la etapa intermedia. Por ende, la valoración que conlleva la “evidencia digital”, genera una calificación a nivel de delitos, ya que no en todos los tipos penal se encuentra como una evidencia “madre”, estando a que su característica “digital” enerva el uso de herramientas distintas a la de una evidencia común, enfocados a delitos digitales. Por lo que, la presente investigación busca determinar el procedimiento normativo para el tratamiento, preservación de la evidencia digital, y como tal ayude a contrarrestar el cibercrimen. Es

en esa medida que abarcaremos la normativa nacional respecto a los delitos informáticos, así como el convenio de Budapest a nivel internacional, dispositivos jurídicos centrales que abarcan este tipo de conductas por parte de los ciberdelincuentes y los instrumentos que a la fecha se encuentran vigentes, que son las guías de la evidencia digital del Ministerio Público y Policía Nacional del Perú.

Alva Arevalo, S. D. (2025). Valoración de la prueba digital y derecho al debido proceso. Región San Martín, 2020-2025. La presente investigación se articula con el ODS N.º 16, orientado a fortalecer las alianzas institucionales, al analizar la interacción entre el Ministerio Público, el Poder Judicial, la Policía Nacional del Perú, Medicina Legal y otras entidades vinculadas al sistema de justicia. El objetivo general fue determinar cómo los operadores jurídicos de la región San Martín valoraron la prueba digital en relación con el derecho al debido proceso durante el periodo 2020–2025. Se desarrolló un estudio de enfoque cualitativo, de carácter básico y transversal, sustentado en el diseño de teoría fundamentada. La muestra estuvo integrada por diez operadores de justicia de la región. Los hallazgos muestran que, aunque existe una percepción general de mejora en la valoración de la prueba digital, su aplicación continúa siendo desigual. Se identificó que la PNP de San Martín ejecuta solo parcialmente las directrices previstas en el Manual para el Recojo de Evidencia Digital, y que el Ministerio Público presenta debilidades en el control de la cadena de custodia. Se concluye que, pese al reconocimiento normativo y jurisprudencial de la validez de la prueba digital, persisten deficiencias operativas que limitan una valoración adecuada y comprometen el respeto al debido proceso.

2.2. Bases teóricas

2.2.1. El Delito de Fraude Informático

El fraude informático es una figura delictiva que surge como respuesta a la creciente utilización de sistemas informáticos para la gestión de información y recursos económicos. A diferencia del fraude tradicional, esta modalidad implica la manipulación ilegítima de datos, programas o sistemas con el fin de obtener un beneficio económico o causar un perjuicio a terceros. De acuerdo con Brenner (2010), el fraude informático constituye uno de los delitos más dinámicos y adaptables, ya que los ofensores se aprovechan de vulnerabilidades técnicas difíciles de detectar mediante mecanismos

convencionales de control. En este sentido, el avance de las tecnologías digitales ha ampliado las posibilidades delictivas, haciendo necesaria una regulación específica.

En el ámbito jurídico internacional, el Convenio de Budapest sobre Ciberdelincuencia (2001) establece que el fraude informático implica cualquier alteración, introducción, borrado o supresión de datos informáticos que produzca un beneficio patrimonial indebido. Esta definición ha servido como referencia para numerosos ordenamientos nacionales. Según Gercke (2012), este convenio ha sido fundamental para armonizar criterios legales y facilitar la cooperación internacional en la investigación de delitos informáticos. Así, la normativa busca abarcar tanto las acciones directas de manipulación de sistemas como las técnicas más sofisticadas, tales como phishing, pharming o ataques mediante malware orientado al beneficio económico.

Asimismo, el fraude informático presenta características que dificultan su detección y persecución. Wall (2007) señala que los delincuentes se benefician del anonimato, la transnacionalidad y la velocidad que caracteriza a los entornos digitales, lo cual complica la labor probatoria y exige herramientas forenses especializadas. En muchos casos, los delitos se cometen mediante infraestructuras distribuidas y sistemas automatizados, lo que fragmenta la evidencia y requiere técnicas avanzadas de rastreo. Además, la naturaleza intangible de los datos altera la forma en que se conceptualiza el daño, ya que no siempre es evidente ni inmediato.

Finalmente, la regulación penal del fraude informático debe adaptarse continuamente a las transformaciones tecnológicas. Autores como Yar y Steinmetz (2019) sostienen que el derecho penal enfrenta el desafío de actualizar tipificaciones que respondan a nuevas modalidades delincuenciales sin sacrificar principios fundamentales como la legalidad y la proporcionalidad. De esta manera, el tratamiento del fraude informático requiere un enfoque integral que combine medidas legislativas, técnicas de ciberseguridad, educación digital y cooperación internacional. Solo a través de un abordaje multidisciplinario es posible enfrentar eficazmente este delito en constante evolución.

2.2.1.1. Definición y clasificación del fraude informático.

El fraude informático se define como toda conducta orientada a obtener un beneficio económico indebido mediante la manipulación ilícita de sistemas, datos o

procesos informáticos. El Convenio de Budapest sobre Ciberdelincuencia (2001) establece que este delito implica la alteración, supresión o introducción de datos con el fin de generar un perjuicio patrimonial. En esta línea, Schjølberg y Ghernaouti-Hélie (2011) señalan que el fraude informático constituye una de las categorías más relevantes de la ciberdelincuencia debido a su impacto económico global, su rápida evolución técnica y su alta tasa de ocultamiento. Esta definición permite delimitar una conducta que combina elementos tecnológicos y económicos, lo que la diferencia de los fraudes tradicionales.

La clasificación del fraude informático ha sido desarrollada por diversos organismos internacionales y académicos con el fin de facilitar su estudio y tipificación. Según Britz (2013), los fraudes informáticos pueden dividirse en dos grandes grupos: los que afectan directamente los sistemas de procesamiento de datos (manipulación de programas, introducción de códigos maliciosos, alteración de bases de datos) y los que utilizan medios informáticos como instrumento para engañar a las víctimas (phishing, ingeniería social, falsificación digital). Esta categorización permite comprender que el fraude puede dirigirse tanto al funcionamiento interno de los sistemas como a los usuarios que interactúan con ellos.

Por su parte, la INTERPOL (2020) propone una clasificación basada en las técnicas utilizadas, distinguiendo entre fraudes por intrusión en sistemas, fraudes basados en engaño digital y fraudes mediante suplantación de identidad. Esta clasificación reconoce que los ciberdelincuentes emplean métodos cada vez más sofisticados, como la clonación de tarjetas mediante skimmers, el uso de malware financiero o la explotación de vulnerabilidades en plataformas de pago. A ello se suma la aparición de fraudes asociados a criptomonedas, contratos inteligentes y servicios de banca electrónica, lo que evidencia la necesidad constante de actualizar las tipologías.

Finalmente, diversos académicos destacan que la clasificación del fraude informático debe ser flexible y adaptarse a la naturaleza cambiante del entorno digital. Brenner (2010) afirma que no existen fronteras rígidas entre las distintas modalidades, ya que los delincuentes combinan técnicas y herramientas para maximizar su eficacia y dificultar la detección. Por ello, una clasificación adecuada no solo debe describir las técnicas empleadas, sino también considerar factores como el modus operandi, los objetivos económicos, el nivel de sofisticación tecnológica y el grado de organización

criminal. Esta perspectiva integral facilita el análisis jurídico y criminológico del fenómeno, así como la implementación de estrategias de prevención y control.

2.2.1.2. Características y tipología de los fraudes informáticos.

Los fraudes informáticos presentan características que los diferencian de las modalidades tradicionales de estafa y engaño. Una de sus principales particularidades es su naturaleza digital, que permite a los ofensores actuar de manera remota y anónima, lo que reduce significativamente el riesgo de ser identificados. Wall (2007) sostiene que los ciberdelitos, incluido el fraude, se caracterizan por la desmaterialización del acto delictivo, pues el daño se produce mediante la manipulación de información y no a través de acciones físicas. Asimismo, estos delitos suelen tener un alcance transnacional, lo cual dificulta la competencia jurisdiccional y los procesos de investigación.

Otra característica fundamental es la automatización y velocidad con la que pueden ejecutarse estas conductas. Según Holt y Bossler (2014), los fraudes informáticos pueden perpetrarse mediante programas automatizados capaces de atacar a miles de víctimas simultáneamente, como sucede con el phishing masivo o los ataques de malware financiero. Esta capacidad de escalabilidad convierte al fraude informático en un fenómeno de alto impacto económico. De igual manera, la sofisticación técnica de los métodos usados, como el uso de botnets, troyanos bancarios o técnicas avanzadas de spoofing, evidencia una evolución constante que obliga a las instituciones a actualizar sus mecanismos de defensa.

La tipología del fraude informático ha sido desarrollada por diversos autores y organismos especializados. La European Union Agency for Cybersecurity (ENISA, 2022) clasifica estos delitos en categorías como fraude por ingeniería social (phishing, vishing, smishing), fraude financiero digital (clonación de tarjetas, manipulación de transferencias electrónicas), fraude por suplantación de identidad y fraudes asociados a criptomonedas y activos digitales. Estas tipologías permiten comprender cómo los delincuentes explotan vulnerabilidades técnicas y humanas para obtener beneficios económicos ilícitos. Cada tipo de fraude responde a un modus operandi distinto, aunque frecuentemente se combinan múltiples técnicas para incrementar la efectividad del ataque.

Finalmente, la literatura criminológica señala que las tipologías deben ser dinámicas, ya que los ciberdelincuentes innovan constantemente en sus métodos. Yar y Steinmetz (2019) afirman que la diversificación de los fraudes informáticos está influenciada por las transformaciones tecnológicas y por la expansión de nuevos entornos digitales, como las plataformas de comercio electrónico, redes sociales y sistemas de pago móvil. En consecuencia, el análisis de las características y tipologías del fraude informático debe contemplar tanto la evolución tecnológica como el comportamiento humano, lo que resulta esencial para la formulación de políticas públicas, estrategias de investigación y mecanismos de prevención efectivos.

2.2.1.3. El fraude informático en el contexto legal peruano

En el Perú, la figura del fraude informático está recogida por la Ley 30096 —conocida como Ley de Delitos Informáticos— que fue promulgada el 22 de octubre de 2013. En su artículo 8, la ley define el delito de fraude informático como aquella conducta mediante la cual una persona "deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático".

La norma no solo delimita la conducta prohibida, sino que también establece sanciones específicas para quienes la cometan. En general, el delito de fraude informático se castiga con pena privativa de libertad de entre cuatro a ocho años y con multa por sesenta a ciento veinte días-multa. Sin embargo, la pena puede aumentar —a entre cinco y diez años, y multa más elevada— cuando el delito afecta patrimonio público destinado a fines sociales o asistenciales.

El marco normativo ha experimentado actualizaciones recientes. Por ejemplo, mediante el Decreto Legislativo 1614, aprobado en diciembre de 2023, se reformaron los artículos de la Ley 30096 para fortalecer la represión de conductas asociadas a la ciberdelincuencia, incluyendo aquellas que facilitan la comisión del fraude informático. Este tipo de reformas muestran la voluntad del Estado peruano de adaptar su legislación frente a las nuevas formas de criminalidad que surgen con el avance tecnológico y la digitalización.

En cuanto al ejercicio práctico del derecho penal, la jurisprudencia nacional ya ha aplicado la Ley de Delitos Informáticos en casos reales. Por ejemplo, un fallo reciente de la Corte Suprema de Justicia de la República resolvió que, en un caso en que se atribuyeron tanto fraude informático como hurto agravado vía sistemas de transferencia electrónica, debía aplicarse exclusivamente la tipificación de fraude informático conforme al artículo 8 de la Ley 30096 —al ser considerada la norma más favorable— reduciendo así la pena. Esto evidencia que el marco legal es aplicado, y que los tribunales reconocen la especificidad del delito cuando ocurre mediante el uso de tecnologías de la información.

2.2.1.4. Impacto social y económico del fraude informático

El fraude informático genera un impacto económico significativo en sociedades modernas altamente digitalizadas. Diversos informes internacionales evidencian que el costo global de la ciberdelincuencia —del cual el fraude informático constituye una de las modalidades predominantes— ha aumentado de manera acelerada en los últimos años. De acuerdo con el Cybersecurity Ventures Report (Morgan, 2022), las pérdidas globales por ciberdelitos superaron los 6 billones de dólares en 2021 y podrían ascender a 10,5 billones para 2025. Este crecimiento exponencial demuestra que el fraude informático no solo afecta a individuos, sino también a empresas, instituciones financieras y gobiernos, generando un impacto directo sobre la estabilidad económica global.

En el ámbito social, el fraude informático deteriora la confianza de los ciudadanos en las tecnologías digitales. La International Telecommunication Union (ITU, 2021) señala que el aumento de fraudes en línea —especialmente los relacionados con suplantación de identidad y manipulación de transacciones— produce desconfianza en servicios esenciales como la banca digital, el comercio electrónico y las plataformas de servicios públicos. Esta erosión de confianza limita la adopción de herramientas tecnológicas y profundiza la brecha digital, afectando particularmente a poblaciones vulnerables, como adultos mayores, personas con bajo nivel de alfabetización digital o usuarios nuevos de servicios electrónicos.

Desde una perspectiva institucional, el fraude informático obliga a las organizaciones a incrementar sus inversiones en ciberseguridad. El World Economic Forum (2023) destaca que la mayoría de empresas destinan un porcentaje significativo de

su presupuesto anual a la protección de sistemas informáticos debido al incremento de ataques orientados al fraude. Estos gastos incluyen herramientas tecnológicas, capacitación de personal, protocolos de prevención y contratación de seguros contra ciberriesgos. Además, las empresas que sufren incidentes de fraude informático pueden experimentar interrupciones operativas, pérdida de reputación y disminución de la confianza del consumidor, lo cual afecta su competitividad en el mercado.

Finalmente, en el plano social más amplio, el fraude informático favorece la expansión de economías criminales digitalizadas. Brenner (2010) advierte que los ciberdelincuentes utilizan redes clandestinas y mercados en la "dark web" para comercializar datos robados, credenciales bancarias o herramientas diseñadas para cometer fraudes. Esta economía paralela socava los sistemas financieros formales y fomenta la aparición de estructuras criminales transnacionales difíciles de rastrear. De esta manera, el fraude informático no solo implica pérdidas económicas directas, sino también riesgos sociales, institucionales y de seguridad que afectan la gobernabilidad y la cohesión social.

2.2.2. La Evidencia Digital

2.2.2.1. Definición de evidencia digital

La evidencia digital se define como cualquier información con valor probatorio que se encuentra almacenada, transmitida o procesada mediante dispositivos o sistemas electrónicos. Según Casey (2011), la evidencia digital comprende datos creados de manera automática o intencional por dispositivos como computadoras, teléfonos móviles, servidores, cámaras digitales y redes de comunicación, y que pueden utilizarse en un proceso judicial para demostrar hechos relevantes. Esta definición destaca dos elementos esenciales: su origen tecnológico y su potencial utilidad en la administración de justicia.

La Scientific Working Group on Digital Evidence (SWGDE, 2018) amplía esta definición señalando que la evidencia digital no solo incluye archivos visibles, sino también metadatos, fragmentos de información, registros de actividad y cualquier rastro generado por la interacción humana o automatizada con un sistema digital. Esta característica distingue la evidencia digital de otras formas tradicionales, pues su recuperación exige técnicas especializadas de análisis forense. Además, la fragilidad y

volatilidad de los datos electrónicos requieren procedimientos estrictos de preservación para evitar alteraciones o pérdidas.

En el ámbito jurídico, la evidencia digital adquiere relevancia debido a la creciente dependencia de la sociedad moderna de las tecnologías de la información. Para Goodman (2015), la digitalización de actividades personales, comerciales y gubernamentales ha generado un volumen masivo de información que puede convertirse en evidencia en casos penales, civiles o administrativos. Esto incluye comunicaciones electrónicas, historiales de navegación, registros de geolocalización, transacciones digitales y datos almacenados en la nube. En consecuencia, la evidencia digital se ha convertido en un componente indispensable en la investigación contemporánea.

Finalmente, la naturaleza de la evidencia digital plantea desafíos particulares respecto a su autenticidad, integridad y admisibilidad en juicio. Kessler (2019) enfatiza que su carácter manipulable exige técnicas de verificación basadas en controles de hash, cadenas de custodia digitales y metodologías forenses estandarizadas. Además, los tribunales deben evaluar la fiabilidad de las herramientas y procedimientos utilizados para obtener y analizar estos datos. Por ello, la definición de evidencia digital no solo debe entenderse desde una perspectiva técnica, sino también jurídica y procesal, con el fin de garantizar su validez dentro del sistema de justicia.

2.2.2.2. Tipos de evidencia digital (archivos electrónicos, correos electrónicos, registros bancarios, etc.)

La evidencia digital abarca una amplia variedad de fuentes y formatos que pueden contener información relevante para una investigación. Entre los tipos más comunes se encuentran los archivos electrónicos, tales como documentos de texto, hojas de cálculo, imágenes, videos, bases de datos y archivos comprimidos. Según Casey (2011), estos archivos pueden presentar tanto información visible como metadatos que registran detalles esenciales, como la fecha de creación, modificación, autoría y ubicación del archivo en el sistema. Su análisis permite reconstruir actividades, identificar usuarios y establecer cronologías de eventos digitales.

Otro tipo fundamental de evidencia digital son los correos electrónicos, los cuales constituyen una de las formas más utilizadas de comunicación en entornos personales y corporativos. Los correos incluyen información clave como encabezados, direcciones IP,

rutas de transmisión y adjuntos, factores que permiten identificar el origen y autenticidad del mensaje. Brenner (2010) señala que los correos electrónicos suelen ser determinantes en investigaciones de fraude informático, acoso, amenazas y delitos financieros, debido a su capacidad para reflejar comunicaciones directas entre involucrados y registrar intercambios documentales relevantes.

Asimismo, los registros bancarios y transacciones electrónicas representan una categoría crucial dentro de la evidencia digital, especialmente en delitos económicos. Las instituciones financieras almacenan datos sobre transferencias, movimientos de cuentas, operaciones con tarjetas de crédito, accesos a banca en línea y patrones de comportamiento financiero. De acuerdo con Goodman (2015), estos registros permiten rastrear el flujo de dinero, identificar transacciones sospechosas y vincular a los responsables con operaciones ilícitas. En casos de fraude informático, este tipo de evidencia resulta especialmente valioso para rastrear operaciones manipuladas o realizadas mediante accesos no autorizados.

Finalmente, la evidencia digital también incluye registros de actividad del sistema, como logs de servidores, historiales de navegación, registros de geolocalización, datos de dispositivos móviles y trazas generadas en redes sociales y servicios en la nube. La Scientific Working Group on Digital Evidence (SWGDE, 2018) sostiene que estos registros permiten reconstruir el comportamiento digital de un usuario, determinar accesos, identificar dispositivos involucrados y detectar intrusiones o actividades anómalas. Debido a su diversidad y complejidad, este tipo de evidencia requiere técnicas forenses especializadas que garanticen su autenticidad e integridad.

2.2.2.3. Características y desafíos de la evidencia digital en los juicios penales

La evidencia digital posee características particulares que la distinguen de otros tipos de evidencia utilizados en el proceso penal. Una de las más relevantes es su naturaleza intangible y altamente volátil, lo que implica que puede ser alterada, destruida o sobrescrita con facilidad si no se aplican procedimientos adecuados de preservación. Casey (2011) destaca que la evidencia digital puede modificarse incluso sin intervención humana directa, por ejemplo, mediante procesos automáticos del sistema operativo, lo que exige técnicas rigurosas para asegurar su integridad. Esta volatilidad hace que la cadena de custodia sea un aspecto crítico en los juicios penales.

Otra característica importante de la evidencia digital es su dependencia de herramientas tecnológicas para su acceso e interpretación. A diferencia de la evidencia física, que puede analizarse de manera directa, la evidencia digital requiere software especializado, hardware compatible y conocimientos técnicos avanzados. Según Kessler (2019), la interpretación de datos digitales puede variar dependiendo de la herramienta forense utilizada, lo que plantea desafíos relacionados con la replicabilidad y la validación de los métodos. Esto obliga a los operadores del sistema penal a garantizar que las herramientas empleadas sean confiables, estandarizadas y verificables.

Desde la perspectiva jurídica, uno de los principales desafíos consiste en demostrar la autenticidad y fiabilidad de la evidencia digital dentro del juicio penal. Goodman (2015) señala que la manipulación potencial de los datos genera cuestionamientos respecto a su origen, integridad y exactitud, lo que requiere la presentación de peritajes técnicos detallados. Además, los tribunales deben evaluar si los procedimientos de recolección, almacenamiento y análisis cumplieron con estándares reconocidos internacionalmente, como los establecidos por organizaciones como SWGDE o ISO, para garantizar la admisibilidad probatoria.

Finalmente, el uso de evidencia digital en juicios penales también enfrenta desafíos derivados de la dimensión transnacional de los delitos informáticos. Brenner (2010) indica que los datos relevantes para una investigación pueden encontrarse almacenados en servidores ubicados en diferentes países, sujetos a legislaciones distintas en materia de privacidad, retención de datos y cooperación judicial. Esto genera dificultades en la obtención oportuna de información y puede retrasar investigaciones o limitar el acceso a evidencia crucial. Por ello, los desafíos de la evidencia digital requieren un enfoque coordinado entre aspectos técnicos, jurídicos y de cooperación internacional.

2.2.2.4. El concepto de prueba digital: ¿Qué la hace válida como prueba?

La prueba digital es toda evidencia electrónica que, tras ser obtenida y analizada correctamente, puede presentarse ante un tribunal para demostrar hechos relevantes en un proceso penal. A diferencia de la simple evidencia digital, la prueba digital implica un proceso de validación jurídica y técnica que garantiza su admisibilidad. Según Casey (2011), un dato electrónico solo se convierte en prueba cuando puede demostrarse su autenticidad, integridad y origen, elementos esenciales para que tenga valor probatorio

dentro de un juicio. Por ello, el concepto de prueba digital está estrechamente vinculado a las exigencias formales del sistema procesal.

Uno de los factores más importantes para determinar la validez de la prueba digital es la autenticidad, es decir, la capacidad de demostrar que el dato proviene de la fuente que se afirma. Kessler (2019) señala que, debido a la facilidad con la que pueden alterarse los datos electrónicos, es indispensable verificar sus características técnicas mediante hash criptográficos, análisis forenses y documentaciones claras del proceso de obtención. Estos mecanismos permiten garantizar que el contenido presentado en juicio no ha sido manipulado, reforzando así su valor como prueba confiable.

Además, la cadena de custodia digital constituye un elemento fundamental para validar la admisibilidad de la prueba. La Scientific Working Group on Digital Evidence (SWGDE, 2018) establece que toda evidencia electrónica debe ser preservada mediante procedimientos documentados que incluyan identificación, recolección, almacenamiento, transferencia y análisis. El incumplimiento de estos procedimientos puede generar dudas sobre la integridad de la evidencia y conducir a la exclusión de la prueba. La cadena de custodia garantiza que la evidencia presentada en juicio es la misma que fue recuperada durante la investigación.

Finalmente, la transformación de evidencia digital en prueba válida depende también de criterios jurídicos como la pertinencia y la licitud. Goodman (2015) destaca que la prueba digital debe haberse obtenido sin vulnerar derechos fundamentales, como la privacidad o el debido proceso. Esto implica que los investigadores deben respetar autorizaciones judiciales, límites legales y principios de proporcionalidad. Cuando estos requisitos no se cumplen, la evidencia puede ser declarada nula, aun si tiene un alto valor informativo. Por tanto, la validez de la prueba digital es el resultado de la integración de requisitos técnicos y jurídicos que garantizan su fiabilidad y legitimidad dentro del proceso penal.

2.2.2.5. El valor probatorio de la evidencia digital en el derecho penal

El valor probatorio de la evidencia digital en el derecho penal ha adquirido creciente relevancia debido al incremento de delitos cometidos mediante tecnologías de la información. La doctrina sostiene que la evidencia digital debe evaluarse bajo los mismos principios que cualquier otro medio probatorio, aunque teniendo en cuenta su

naturaleza particular. Para Casey (2011), su valor depende de la autenticidad, integridad y confiabilidad del proceso mediante el cual fue obtenida, por lo que la informática forense juega un rol indispensable en su admisión judicial. En este sentido, los tribunales exigen que toda evidencia digital preserve una cadena de custodia rigurosa que permita verificar su origen.

Un aspecto fundamental en la evaluación del valor probatorio es la integridad de los datos. La Scientific Working Group on Digital Evidence (SWGDE, 2018) establece que la preservación bit a bit, la utilización de herramientas validadas y la documentación exhaustiva del proceso fortalecen la credibilidad de la evidencia ante el juez. Esto implica que la simple obtención de información no es suficiente: el proceso técnico debe permitir demostrar que la evidencia no ha sido manipulada o alterada. De ello depende que el juzgador pueda otorgarle un valor probatorio pleno y no meramente referencial.

Asimismo, la jurisprudencia comparada reconoce la importancia de la evidencia digital como un medio idóneo para acreditar conductas delictivas que, de otro modo, serían difíciles de demostrar. En Estados Unidos, por ejemplo, los tribunales han admitido metadatos, registros de servidores y comunicaciones electrónicas como medios probatorios válidos siempre que cumplan con estándares de autenticación establecidos en reglas como la Federal Rules of Evidence (FRE 901) (Kerr, 2018). Esta tendencia se ha replicado en diversos ordenamientos, consolidando la relevancia del análisis técnico en la determinación de la fuerza probatoria del material digital.

Finalmente, en el ámbito latinoamericano, diversos sistemas judiciales han incorporado normas específicas para regular la obtención y valoración de evidencia digital, lo que ha fortalecido su uso en los procesos penales. En Perú, por ejemplo, el Código Procesal Penal admite expresamente documentos electrónicos y registros informáticos como medios probatorios válidos, siempre que se garantice su autenticidad (Ministerio de Justicia y Derechos Humanos, 2020). De esta manera, la evidencia digital se consolida como un instrumento clave en la lucha contra el delito contemporáneo, con un valor probatorio dependiente del cumplimiento de estándares técnicos y legales adecuados.

2.2.3. El Derecho al Debido Proceso en el Contexto del Fraude Informático

El derecho al debido proceso constituye un principio fundamental del Estado de derecho y garantiza que toda persona sometida a un procedimiento penal sea juzgada conforme a reglas claras, imparciales y previamente establecidas. Este principio se encuentra recogido en instrumentos como la Convención Americana sobre Derechos Humanos (Organización de Estados Americanos, 1969) y ha sido ampliamente desarrollado por la doctrina y la jurisprudencia. En los delitos de fraude informático, en los que intervienen tecnologías complejas, este derecho adquiere especial relevancia debido a la necesidad de asegurar una adecuada comprensión técnica por parte de las autoridades y de garantizar la validez de los medios probatorios digitales empleados durante el proceso.

Uno de los principales desafíos del debido proceso en casos de fraude informático radica en la obtención, preservación y análisis de evidencia digital, la cual requiere procedimientos técnicos especializados. Si se vulneran garantías como la cadena de custodia o la integridad de los datos, el imputado puede ver comprometidos sus derechos fundamentales. De acuerdo con Casey (2011), cualquier error en la recolección o tratamiento de evidencia informática afecta directamente su validez probatoria y, en consecuencia, el derecho a un juicio justo. Por ello, los operadores del sistema penal deben actuar con rigurosidad técnica y jurídica para no comprometer la equidad del procedimiento.

Asimismo, la complejidad técnica de los delitos informáticos exige que los imputados cuenten con garantías adicionales vinculadas al acceso a la información y a una defensa adecuada. La Corte Interamericana de Derechos Humanos (2013) ha subrayado que el derecho de defensa implica la posibilidad real y efectiva de contradecir la prueba presentada, lo que en el caso de evidencia digital requiere asistencia técnica especializada. Esto significa que la defensa debe tener acceso oportuno a los dispositivos, registros electrónicos y peritajes necesarios para comprender y rebatir los elementos acusatorios basados en tecnología.

Finalmente, el debido proceso también exige que los jueces cuenten con criterios claros para valorar la evidencia digital en casos de fraude informático. En varios sistemas latinoamericanos, incluidos los de Perú y Chile, se ha resaltado la importancia de la

capacitación judicial en materia tecnológica para evitar decisiones basadas en interpretaciones incorrectas o insuficientes sobre la naturaleza de la prueba digital (Badii & Castillo, 2010). De este modo, el respeto del debido proceso en delitos de fraude informático no solo depende de garantías formales, sino también de la capacidad institucional del sistema penal para comprender la tecnología involucrada y asegurar un juicio justo.

2.2.4. Normativa y Jurisprudencia en el Contexto del Fraude Informático

El marco normativo del fraude informático en el Perú se estructura a partir de tres pilares fundamentales: la Ley N° 30096 como norma interna principal, el Convenio de Budapest como estándar internacional de referencia, y la jurisprudencia desarrollada por la Corte Suprema que interpreta y aplica estos dispositivos legales. A continuación, se analiza cada uno de estos componentes.

A. La Ley N° 30096 — Ley de Delitos Informáticos

La Ley N° 30096, Ley de Delitos Informáticos, fue promulgada el 22 de octubre de 2013 con el objeto de "prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación" (artículo 1) . Esta norma constituye el instrumento normativo fundamental en la lucha contra la ciberdelincuencia en el Perú, tipificando por primera vez de manera específica las conductas relacionadas con el fraude informático y otras infracciones vinculadas a las tecnologías de la información y comunicación.

Artículo 8. Fraude informático

El delito de fraude informático se encuentra tipificado en el artículo 8 de la Ley N° 30096, cuyo texto actualizado —considerando las modificaciones introducidas por el Decreto Legislativo N° 1614, publicado el 21 de diciembre de 2023— establece:

"Artículo 8. Fraude informático

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier

interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos."

La norma no solo delimita la conducta prohibida, sino que también establece sanciones específicas, incluyendo un tipo agravado cuando el delito afecta patrimonio público destinado a fines sociales o asistenciales, así como una cláusula de participación que sanciona a quienes facilitan la transferencia de activos obtenidos ilícitamente.

2.2.4.1. Evolución normativa y modificaciones relevantes

La Ley N° 30096 ha experimentado un proceso continuo de actualización para adaptarse a las nuevas formas de ciberdelincuencia. Entre las modificaciones más relevantes se encuentran:

- **Ley N° 30171 (10 de marzo de 2014)**: Modificó diversos artículos de la Ley N° 30096, incluyendo los artículos 3, 4 y 7, y derogó el artículo 6 .

- **Decreto Legislativo N° 1614 (21 de diciembre de 2023)**: Reformó los artículos 2 y 8 de la Ley N° 30096 para fortalecer la represión de conductas asociadas a la ciberdelincuencia, incrementando las penas para el fraude informático de un mínimo de tres a cuatro años.

- **Decreto Legislativo N° 1700 (23 de enero de 2026)**: Incorporó el artículo 12-A, tipificando el delito de adquisición, posesión y tráfico ilícito de datos informáticos, sancionando a quien "posee, compra, recibe, comercialice, vende, facilite, intercambie o trafique datos informáticos, credenciales de acceso o bases de datos personales, teniendo conocimiento o debiendo presumir que se obtuvo sin consentimiento de su titular o mediante la vulneración de sistemas de

seguridad o la comisión de un delito informático" con pena privativa de libertad no menor de cinco ni mayor de ocho años .

2.2.4.2. El Convenio de Budapest sobre Ciberdelincuencia

El Convenio de Budapest es el primer tratado internacional destinado a hacer frente a los delitos informáticos mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. Fue promovido por el Consejo de Europa y firmado en Budapest el 23 de noviembre de 2001, sirviendo como ley modelo para que los países desarrollen su normativa interna sobre ciberdelincuencia.

A. Ratificación por el Perú y entrada en vigencia

El Perú se adhirió al Convenio de Budapest mediante un proceso que incluyó:

- **Resolución Legislativa N° 30913** (13 de febrero de 2019): Aprobación por el Congreso de la República.
- **Decreto Supremo N° 010-2019-RE** (10 de marzo de 2019): Ratificación por el Poder Ejecutivo.
- **Entrada en vigencia**: 1 de diciembre de 2019.

El Convenio de Budapest resulta de vital importancia porque permite que los requerimientos formulados por los operadores jurídicos a nivel nacional sean remitidos de manera célere a los Estados Parte, entre los cuales figuran Estados Unidos, España, Italia, Japón, Argentina, Chile, Colombia, entre otros.

Particularmente relevante es el artículo 35 del Convenio, que establece el funcionamiento de la **Red 24/7**, una herramienta de cooperación internacional que garantiza la asistencia inmediata en investigaciones relativas a delitos vinculados a sistemas y datos informáticos, permitiendo solicitar a los estados extranjeros la conservación de datos (artículos 29 y 30), la obtención de pruebas, el suministro de información de carácter jurídico y la localización de sospechosos.

B. Correspondencia entre el Convenio y la Ley N° 30096

El artículo 8 del Convenio de Budapest sirvió como modelo para la tipificación del fraude informático en la Ley N° 30096, estableciendo parámetros comunes para la persecución de este delito a nivel internacional. La correspondencia entre ambas normas se evidencia en la estructura de los tipos penales:

Convenio de Budapest (art. 8)	**Ley N° 30096 (art. 8)**
Manipulación deliberada e ilegítima de datos informáticos	Diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos
Interferencia en el funcionamiento de un sistema informático	Interferencia o manipulación en el funcionamiento de un sistema informático
Suplantación de interfaces o páginas web	Suplantación de interfaces o páginas web
Provecho económico ilícito para sí o para otro	Provecho ilícito en perjuicio de tercero

2.2.4.3. Jurisprudencia relevante sobre fraude informático y evidencia digital

A. Recurso de Nulidad N° 780-2022, Lima Este (Corte Suprema)

Este pronunciamiento constituye el precedente más relevante en materia de fraude informático en los últimos años. Los hechos del caso fueron los siguientes: Arturo Javier Yrigoyen Velásquez, quien laboraba como cajero terminalista en MiBanco —agencia Huachipa—, hizo uso indebido de las claves secretas personales y códigos de usuario pertenecientes a jefes de banca y supervisoras de la entidad. Mediante esta acción, logró acceder al sistema informático BANTOTAL y procedió a desbloquear su propia cuenta CTS, realizando 36 operaciones de transferencia desde el 31 de mayo de 2011 hasta el 19 de abril de 2012, generando un sobregiro total de S/ 215,208.00.

El Juzgado Especializado Penal de Lima condenó a Yrigoyen Velásquez como autor de los delitos de fraude informático (artículo 207-A del Código Penal) y hurto agravado (artículo 186 inciso 3 del Código Penal) en concurso ideal, imponiéndole 5 años de pena privativa de libertad efectiva. La Sala Penal Superior confirmó la condena.

Sin embargo, al resolver el recurso de nulidad, la **Sala Penal Transitoria de la Corte Suprema** aplicó el principio de retroactividad benigna (artículo 103 de la Constitución y artículo 6 del Código Penal), determinando que los tipos penales por los que fue condenado Yrigoyen Velásquez —previstos en el Código Penal— habían sido

derogados por la Ley N° 30096, y que la conducta debía subsumirse exclusivamente en el artículo 8 de dicha ley, por ser la norma posterior más favorable.

En consecuencia, la Corte Suprema:

- **Revocó** la condena por los delitos de fraude informático y hurto agravado.
- **Confirmó** la condena exclusivamente por el delito de fraude informático (artículo 8 de la Ley N° 30096).
- **Redujo la pena** a tres años de privación de libertad efectiva.

Este pronunciamiento es relevante por tres razones fundamentales: (i) reafirma la aplicación del principio de retroactividad benigna en materia penal; (ii) establece que la Ley N° 30096 constituye el marco normativo exclusivo para conductas de manipulación informática, desplazando a las figuras tradicionales del Código Penal; y (iii) reconoce implícitamente que la evidencia digital (registros de acceso, logs del sistema, claves de usuario) es esencial para acreditar el delito de fraude informático.

B. Recurso de Nulidad N° 206-2019, Lima

Este pronunciamiento es relevante porque reconoce el phishing bancario como una técnica delictiva para obtener de forma fraudulenta claves bancarias o información financiera. La Corte Suprema no lo señala como un delito independiente, sino que lo subsume dentro de la comisión de delitos de mayor amplitud como la estafa (artículo 196 del Código Penal) o el fraude informático (artículo 8 de la Ley N° 30096) .

C. El delito de fraude informático en cifras (contexto actual)

La magnitud del problema que enfrenta el sistema de justicia penal peruano en materia de fraude informático queda evidenciada por las siguientes cifras: según datos de la Fiscalía Especializada en Ciberdelincuencia, entre enero y septiembre de 2025, el **68.88%** de las 31,028 denuncias por delitos informáticos correspondieron a fraude informático. Esta proporción mayoritaria evidencia que el fraude informático no es un delito marginal, sino la manifestación más frecuente de la ciberdelincuencia en el Perú.

2.2.5. La Cadena de Custodia en la Evidencia Digital

La cadena de custodia constituye el conjunto de procedimientos destinados a garantizar que la evidencia digital recolectada durante una investigación penal se mantenga íntegra, auténtica y debidamente documentada desde su obtención hasta su presentación ante la autoridad judicial. Este principio es esencial en cualquier proceso penal, pues asegura la trazabilidad del indicio y evita que su valor probatorio sea cuestionado. Según ISO/IEC 27037 (2012), la cadena de custodia debe registrar detalladamente quién recolectó la evidencia, cuándo, dónde, bajo qué condiciones y qué procedimientos se emplearon para su preservación. En el ámbito digital, la dificultad radica en que los datos pueden alterarse fácilmente, incluso de manera involuntaria, lo que exige protocolos altamente estandarizados.

La evidencia digital, por su naturaleza volátil y fácilmente modificable, requiere un tratamiento especializado que permita garantizar su integridad. NIST Special Publication 800-101 (Grance et al., 2012) establece que cualquier manipulación indebida, acceso no autorizado o fallo en la copia forense puede comprometer el valor de la evidencia, ya que incluso cambios mínimos en los metadatos pueden generar dudas sobre su autenticidad. Por ello, la creación de imágenes forenses bit a bit, el uso de herramientas validadas y la aplicación de algoritmos hash (como SHA-256) son prácticas fundamentales para demostrar que la evidencia no ha sido alterada durante su transporte o análisis. De esta manera, la cadena de custodia actúa como un mecanismo de protección frente a objeciones de la defensa sobre la fiabilidad de los datos.

Asimismo, la documentación exhaustiva de cada etapa del manejo de evidencia digital constituye un elemento indispensable para su admisibilidad en juicio. La Scientific Working Group on Digital Evidence (SWGDE, 2018) señala que la evidencia debe registrarse en formularios específicos donde se consignen fechas, firmas, transferencias, análisis realizados y cualquier intervención técnica efectuada. Esta documentación permite reconstruir la “vida completa” de la evidencia, proporcionando al juez criterios claros para evaluar si se ha preservado su integridad. En ausencia de una adecuada cadena de custodia, los tribunales pueden descartar la evidencia o restarle valor probatorio, independientemente de que los datos sean técnicamente correctos.

Finalmente, en el contexto jurídico latinoamericano, incluyendo Perú, la cadena de custodia se encuentra regulada explícitamente como requisito indispensable para el uso de evidencia digital en los procesos penales. El Código Procesal Penal peruano establece que toda evidencia debe estar acompañada de un registro de custodia continuo que demuestre su autenticidad y fiabilidad antes de ser valorada por el juez (Ministerio de Justicia y Derechos Humanos, 2020). Esto refleja una tendencia global: la necesidad de estándares técnicos y jurídicos alineados para enfrentar la creciente complejidad del delito informático. En consecuencia, la cadena de custodia se convierte en una garantía esencial del debido proceso, asegurando que la evidencia digital utilizada en casos de fraude informático sea legítima, confiable y admisible ante los tribunales.

2.2.5.1. Protocolos internacionales y nacionales para la cadena de custodia

Los protocolos internacionales sobre cadena de custodia digital constituyen la base técnica para garantizar que la evidencia informática sea obtenida y preservada de forma confiable. Entre los más influyentes se encuentra la norma ISO/IEC 27037:2012, la cual establece directrices claras sobre la identificación, recolección, adquisición y preservación de evidencia digital, con especial énfasis en la trazabilidad y la protección contra alteraciones. Esta norma recomienda procedimientos uniformes para asegurar que cualquier evidencia mantenga autenticidad e integridad a lo largo de todo su ciclo de vida (ISO/IEC, 2012). Junto con otros estándares ISO, esta guía se ha convertido en un referente para múltiples países que incorporan sus lineamientos a sus normativas nacionales.

De igual manera, instituciones especializadas han desarrollado protocolos técnicos ampliamente adoptados. El National Institute of Standards and Technology (NIST) de Estados Unidos publica guías como la NIST SP 800-101 y 800-86, las cuales definen procedimientos de análisis forense, hash criptográficos, imágenes bit a bit y controles técnicos necesarios para documentar formalmente la cadena de custodia (Kent, Chevalier, Grance & Dang, 2006). Estas guías son utilizadas como referencia en investigaciones policiales, fiscales y judiciales en varios países debido a su alto nivel de estandarización. Asimismo, la Scientific Working Group on Digital Evidence (SWGDE), organismo compuesto por expertos forenses internacionales, actualiza periódicamente sus Best Practices donde define pasos rigurosos de documentación, transporte, acceso y almacenamiento seguro para preservar evidencia digital (SWGDE, 2018).

En el ámbito latinoamericano, muchos países han adoptado o adaptado estos modelos para fortalecer sus procedimientos internos. En Perú, la cadena de custodia está regulada tanto en el Código Procesal Penal como en lineamientos emitidos por la Policía Nacional y el Ministerio Público. El Protocolo Nacional de Cadena de Custodia establece que toda evidencia —incluyendo soporte digital— debe acompañarse de un "Registro de Cadena de Custodia" que documente cada transferencia, análisis o manipulación, con firmas, fechas y motivo de intervención (Ministerio Público, 2015). La normativa peruana exige que la evidencia digital sea recolectada mediante procedimientos técnicos estandarizados, restringiendo su manipulación únicamente a personal autorizado, lo cual se alinea directamente con los lineamientos de ISO y NIST.

Finalmente, organismos policiales como la INTERPOL también han publicado guías de manejo de evidencia digital que complementan los protocolos nacionales. Su Digital Forensics Handbook señala principios universales como evitar alterar datos originales, emplear duplicados forenses y registrar todas las acciones realizadas sobre los dispositivos o soportes informáticos (INTERPOL, 2019). La convergencia entre normas internacionales (ISO, NIST, INTERPOL) y las legislaciones nacionales permite establecer un marco robusto que asegura que la cadena de custodia se cumpla adecuadamente en investigaciones sobre fraude informático y otros delitos tecnológicos. La presencia de estos protocolos contribuye a que la evidencia digital sea considerada válida y confiable en procesos judiciales.

2.2.5.2. Desafíos en el manejo de la evidencia digital en el ámbito judicial

El manejo de la evidencia digital en el ámbito judicial presenta desafíos significativos derivados de su naturaleza técnica, volátil y fácilmente manipulable. A diferencia de la evidencia física, los datos digitales pueden alterarse incluso sin intervención humana directa, lo que complica su preservación y autenticación. Según Casey (2011), la volatilidad de los datos y la dependencia de sistemas tecnológicos complejos hacen que cualquier error en la recolección o almacenamiento pueda comprometer su validez probatoria. Esta vulnerabilidad exige un alto grado de especialización técnica por parte de los operadores de justicia para evitar la exclusión de evidencias cruciales en los procesos penales.

Otro desafío fundamental es la correcta preservación de la cadena de custodia, la cual debe ser estricta y documentada con precisión para asegurar la integridad y autenticidad de la evidencia. Las guías internacionales, como la ISO/IEC 27037:2012, recalcan que cada fase—identificación, adquisición y preservación—requiere herramientas forenses certificadas y metodologías reproducibles (ISO/IEC, 2012). Sin embargo, muchos sistemas judiciales, especialmente en países en desarrollo, carecen de los recursos tecnológicos necesarios o del personal capacitado para aplicar estos protocolos con rigurosidad. Esta brecha institucional puede ocasionar que evidencia digital clave sea impugnada o descartada por dudas razonables sobre su integridad.

La admisibilidad judicial también enfrenta desafíos debido a la complejidad técnica de la evidencia digital. Los jueces y abogados deben interpretar conceptos como hash criptográfico, metadatos, logs, imágenes forenses o registros de red, lo cual exige competencias tecnológicas que no siempre forman parte de la formación jurídica tradicional. Estudios de la SWGDE (2018) indican que la falta de conocimientos especializados puede generar valoraciones incorrectas, sobredependencia en peritos o incluso decisiones judiciales contradictorias respecto a la validez de la evidencia digital. Esta situación evidencia la necesidad de fortalecer la capacitación técnica del personal judicial para asegurar decisiones informadas y coherentes.

Finalmente, el manejo de evidencia digital se complica aún más por los desafíos transnacionales asociados a delitos informáticos. La obtención de datos almacenados en servicios en la nube, proveedores extranjeros o plataformas globales depende de acuerdos de cooperación internacional como el Convenio de Budapest sobre Cibercrimen (Council of Europe, 2001). La demora en obtener estas evidencias o las diferencias normativas entre países puede afectar la oportunidad y la pertinencia de su incorporación al proceso penal. En consecuencia, el sistema judicial debe adaptarse no solo técnicamente, sino también normativamente, para enfrentar un entorno digital cada vez más globalizado y dinámico.

2.2.6. Valoración Judicial de la Evidencia Digital

La valoración judicial de la evidencia digital implica un análisis riguroso que combina criterios jurídicos y conocimientos técnicos especializados. Los jueces deben verificar la autenticidad, integridad, fiabilidad y pertinencia del material digital antes de

otorgarle valor probatorio dentro del proceso penal. Para Goodman y Brenner (2002), la principal complejidad radica en que la evidencia digital no tiene una materialidad física y su interpretación depende de herramientas tecnológicas que pueden variar según el contexto. En este sentido, la valoración no puede reducirse a una simple verificación documental, sino que requiere comprender los procesos tecnológicos que sustentan su obtención y procesamiento.

Asimismo, uno de los elementos centrales en la valoración judicial es la manera en que la evidencia digital ha sido recolectada, almacenada y analizada. Según Mason (2019), la clave consiste en determinar si la evidencia ha sido gestionada conforme a estándares forenses reconocidos internacionalmente, lo que permite presumir su integridad y autenticidad. La existencia de una cadena de custodia sólida incrementa significativamente la credibilidad de los datos ante el juez. Cuando existe duda razonable sobre la integridad del soporte digital, los tribunales suelen otorgarle menor fuerza probatoria o incluso excluirla del proceso penal.

La intervención de peritos especializados constituye otro aspecto esencial en la valoración judicial. Peritos digitales no solo aportan conocimientos técnicos, sino que actúan como intermediarios entre el lenguaje tecnológico y el lenguaje jurídico. Como sostiene Kerr (2020), la interpretación de registros electrónicos, logs, metadatos e imágenes forenses exige conocimientos específicos que superan la formación jurídica tradicional. De este modo, los jueces dependen en gran medida de la calidad del peritaje y de su capacidad para explicar de manera clara y verificable el origen, tratamiento y confiabilidad de la evidencia digital presentada.

Finalmente, la valoración judicial también debe ajustarse a principios de razonabilidad y proporcionalidad. Diversos tribunales internacionales han señalado que la evidencia digital puede tener un alto grado de precisión, pero esto no implica que se deba aceptar sin un control estricto de su origen y tratamiento. Según Solove y Hartzog (2020), incluso sistemas avanzados pueden generar falsos positivos o interpretaciones erróneas si se analizan fuera de contexto. En consecuencia, la valoración judicial debe equilibrar los avances tecnológicos con garantías procesales, asegurando que la evidencia digital utilizada en los procesos penales sea realmente confiable y adecuada para fundamentar decisiones judiciales.

2.2.6.1. El proceso de valoración de pruebas en el sistema judicial peruano

En el sistema judicial peruano, la valoración de las pruebas —incluida la evidencia digital— se rige por el principio de libre valoración razonada, recogido en el artículo 158 del Código Procesal Penal (CPP). Este principio exige que los jueces fundamenten de manera lógica, coherente y motivada las razones por las cuales otorgan o niegan valor probatorio a determinado elemento. Según San Martín Castro (2017), esta valoración no es arbitraria, sino que debe sustentarse en criterios de fiabilidad, pertinencia y suficiencia probatoria, permitiendo que el juez explique cómo la prueba contribuye a la reconstrucción razonable de los hechos.

La evidencia digital, por su naturaleza intangible y fácilmente alterable, exige la aplicación de parámetros específicos dentro del marco general de valoración. Para Salinas Siccha (2019), los jueces peruanos deben examinar si la obtención, preservación y análisis de los datos digitales se realizaron conforme a los estándares establecidos en la Ley N.° 30096 y las normas del CPP sobre cadena de custodia. La integridad del soporte informático, la autenticidad del contenido y la ausencia de manipulación son elementos que el juez debe verificar antes de admitir la evidencia como válida. Cuando estos requisitos no se cumplen, la prueba puede ser descartada o recibir menor peso probatorio.

El trabajo pericial también juega un papel central en la valoración judicial. En el contexto peruano, los informes emitidos por peritos informáticos del Ministerio Público o de peritos independientes acreditados deben cumplir con parámetros técnicos establecidos por la criminalística digital. Tal como indica Reyna Alfaro (2020), el juez no solo debe considerar las conclusiones del perito, sino también evaluar la metodología empleada y la coherencia entre los resultados y los procedimientos aplicados. De esta forma, la pericia se convierte en un puente que traduce el lenguaje técnico al jurídico, permitiendo al juzgador comprender la relevancia y confiabilidad de la información digital.

Finalmente, la valoración judicial debe respetar principios constitucionales como el debido proceso, la presunción de inocencia y la prohibición de prueba ilícita. La jurisprudencia peruana ha establecido que la evidencia digital obtenida vulnerando derechos fundamentales —por ejemplo, interceptaciones sin orden judicial o registros informáticos sin autorización— carece de eficacia probatoria. Como afirma Cubas

Villanueva (2018), la exclusión de la prueba obtenida de forma ilícita no es solo un mecanismo de sanción procesal, sino una garantía para preservar la legitimidad del sistema judicial. En esa línea, la valoración de la evidencia digital en el Perú se orienta a asegurar que su fuerza probatoria sea compatible con estándares de legalidad, confiabilidad y respeto a los derechos fundamentales.

2.2.6.2. Criterios de valoración en el ámbito de los delitos informáticos

La valoración de la evidencia digital en los delitos informáticos requiere la aplicación de criterios diferenciados debido a la complejidad técnica, fragilidad e intangibilidad de este tipo de pruebas. En el contexto jurídico peruano, estos criterios se integran al marco general de la libre valoración razonada, pero incorporan estándares específicos de autenticidad, integridad, trazabilidad y fiabilidad técnica. Como señala López-López (2022), los jueces deben examinar la forma en que los datos fueron adquiridos, almacenados y analizados, garantizando que los procedimientos utilizados no hayan alterado su contenido ni su metadata. Este análisis es esencial en casos de fraude informático, donde la manipulación de archivos, registros o sistemas puede generar pruebas aparentes o distorsionadas.

Un elemento central en la valoración es la cadena de custodia digital, que asegura el recorrido ininterrumpido y documentado de la evidencia desde su obtención hasta su análisis pericial y presentación en juicio. Según Palomo Vélez (2021), en delitos informáticos se exige que cada manipulación, copia o acceso sea registrado mediante protocolos que permitan demostrar la originalidad del soporte o la fidelidad de su réplica forense. Cuando existen brechas en la cadena de custodia o falta de documentación técnica, el juez debe aplicar criterios de desconfianza reforzada, reduciendo el peso probatorio o incluso excluyendo la evidencia si compromete su autenticidad. Esta exigencia responde a la naturaleza volátil de la información digital y a su susceptibilidad a modificaciones imperceptibles sin controles adecuados.

La valoración judicial también considera la fiabilidad de las herramientas forenses empleadas para el análisis de la evidencia. En este sentido, los criterios de aceptabilidad científica basados en estándares internacionales —como las guías del NIST o los principios ACPO— adquieren relevancia para determinar si los software utilizados cumplen con parámetros de reproducibilidad y precisión. Como explica Rivas-López

(2020), los peritos deben acreditar que los programas empleados generan resultados verificables y que sus procedimientos cumplen con buenas prácticas reconocidas en la informática forense. El juez, por su parte, debe evaluar la coherencia entre el método aplicado, los resultados obtenidos y la explicación técnica brindada por el perito durante el juicio.

Finalmente, la jurisprudencia y la doctrina coinciden en que la valoración en delitos informáticos debe incorporar el análisis contextual del ecosistema tecnológico donde ocurrieron los hechos. Esto incluye la configuración de redes, sistemas de autenticación, logs, direcciones IP y patrones de comportamiento digital. Para Jiménez Rivas (2023), estos elementos permiten al juez determinar si la evidencia presentada refleja efectivamente la conducta imputada o si existen factores alternativos —como accesos remotos, errores del sistema o suplantación digital— que podrían generar dudas razonables. Este enfoque integral asegura que la valoración de la evidencia digital en casos de fraude informático se realice con criterios de rigor técnico y garantías procesales, preservando el equilibrio entre eficacia investigativa y respeto a derechos fundamentales.

2.2.6.3. El papel del juez en la valoración de la evidencia digital: Limitaciones y fortalezas

El rol del juez en la valoración de la evidencia digital se ha convertido en un elemento crucial dentro de los procesos penales, especialmente en los delitos informáticos, donde la comprensión técnica y la correcta aplicación de estándares probatorios son esenciales. El juez peruano está obligado a evaluar la evidencia conforme al principio de libre valoración razonada, lo cual implica justificar su decisión a partir de criterios de lógica, experiencia y conocimiento científico. Según San Martín Castro (2017), la labor judicial no se limita a aceptar pasivamente la prueba pericial, sino que exige un análisis activo que determine si la evidencia digital presentada cumple con requisitos de autenticidad, integridad y pertinencia. Esto revela una fortaleza sustancial del sistema, en tanto promueve decisiones fundamentadas que respetan el debido proceso.

No obstante, una de las limitaciones más relevantes radica en la brecha tecnológica existente entre la rapidez del avance digital y la formación jurídica tradicional. Como advierte López-López (2022), muchos jueces carecen de conocimientos especializados en informática forense, lo que puede dificultar la

comprensión de conceptos técnicos como replicación bit a bit, metadatos, logs o protocolos criptográficos. Esta falta de especialización puede generar dependencia excesiva del perito, reduciendo la capacidad crítica del juez al momento de evaluar la consistencia metodológica del informe técnico. Además, en casos complejos de fraude informático, en los que intervienen sistemas distribuidos o técnicas sofisticadas de ocultamiento digital, la valoración judicial puede verse seriamente limitada por la ausencia de capacitación continua y recursos tecnológicos adecuados.

A pesar de estas dificultades, el juez cuenta con herramientas institucionales que fortalecen su función. Una de ellas es la posibilidad de solicitar aclaraciones, ampliaciones o nuevas pericias, según lo establece el Código Procesal Penal. De acuerdo con Reyna Alfaro (2020), este mecanismo permite subsanar dudas técnicas o metodológicas, garantizando que la decisión judicial se sustente en información precisa y verificable. Asimismo, la existencia de protocolos nacionales e internacionales —como las guías de la Policía Nacional del Perú y los estándares del NIST— ofrece al juez parámetros objetivos para evaluar la corrección de los procedimientos de obtención, preservación y análisis de datos digitales. Ello contribuye a que la valoración no dependa únicamente de la experticia del perito, sino que se contraste con criterios reconocidos globalmente.

Finalmente, la jurisprudencia peruana ha fortalecido el papel del juez al establecer que la evidencia digital debe ser evaluada con criterios de fiabilidad reforzada cuando se trata de delitos informáticos. En pronunciamientos recientes, se ha señalado que la volatilidad de los datos digitales requiere una mayor rigurosidad en la verificación de su autenticidad y cadena de custodia. Cubas Villanueva (2018) sostiene que esta exigencia fortalece la capacidad del juez para identificar posibles vulneraciones a derechos fundamentales, especialmente en casos en los que la obtención de datos puede rozar límites constitucionales, como la intervención de comunicaciones o el acceso a dispositivos personales. Así, aunque el juez enfrenta limitaciones técnicas, su función se ve reforzada por mecanismos legales, criterios jurisprudenciales y estándares científicos que permiten una valoración adecuada y garantista de la evidencia digital.

2.2.6.4. El rol de los peritos informáticos en la valoración de la evidencia digital

El papel de los peritos informáticos es fundamental en los procesos penales relacionados con delitos informáticos, ya que son los encargados de traducir información técnica a un lenguaje comprensible para los operadores de justicia. La evidencia digital, debido a su complejidad y fragilidad, necesita ser analizada mediante procedimientos especializados que garanticen su autenticidad e integridad. Según Casey (2011), el perito informático debe aplicar metodologías científicas estandarizadas que permitan identificar, recolectar, preservar y examinar datos sin alterar su contenido. Este rol técnico se vuelve indispensable, pues los jueces y fiscales no necesariamente poseen conocimientos avanzados en informática forense.

Asimismo, los peritos informáticos cumplen una función clave en la validación del proceso de obtención de la evidencia, asegurando que se respeten los principios de cadena de custodia digital y replicación forense. De acuerdo con Carrier (2016), la utilización de herramientas como las copias bit a bit, los cálculos hash y la documentación exhaustiva de cada intervención son elementos esenciales para demostrar que los datos no han sido manipulados. Cuando estos procedimientos se ejecutan correctamente, se fortalece el valor probatorio de la evidencia digital, permitiendo que sea presentada con mayor solidez en el proceso judicial.

Un aspecto central del rol pericial es la emisión del informe técnico, el cual debe ser detallado, verificable y sustentado en pruebas científicas. En el contexto peruano, el Código Procesal Penal exige que el informe pericial incluya la metodología empleada, los instrumentos utilizados y las conclusiones basadas en el análisis objetivo de los datos. Como señala Salinas Siccha (2019), el perito no puede limitarse a describir hallazgos, sino que debe explicar de manera clara cómo la evidencia respalda o descarta hipótesis relevantes del caso. Este enfoque permite al juez valorar la coherencia interna del informe y su correspondencia con estándares reconocidos internacionalmente, como los del NIST o la ISO/IEC 27037.

Finalmente, el perito informático también desempeña un papel esencial durante el juicio oral, donde debe sustentar y defender sus conclusiones mediante interrogatorios y contrainterrogatorios. Esta etapa es crucial, pues permite evaluar la solvencia técnica del

perito y la consistencia de su trabajo bajo el escrutinio de las partes procesales. Tal como menciona Rogers (2015), la capacidad del perito para explicar conceptos técnicos en un lenguaje accesible pero riguroso contribuye decisivamente al entendimiento judicial del caso y al fortalecimiento del valor probatorio de la evidencia digital. Así, su rol no solo se limita al análisis técnico, sino que también implica una dimensión comunicativa esencial para la correcta administración de justicia.

2.2.7. Capacitación Técnica de los Jueces en Materia de Evidencia Digital

La capacitación técnica de los jueces en materia de evidencia digital se ha vuelto una necesidad impostergable en los sistemas de justicia contemporáneos, debido al incremento de delitos informáticos y al uso frecuente de datos electrónicos como medios probatorios. En el Perú, la transformación digital del proceso penal exige que los jueces cuenten con un nivel mínimo de comprensión sobre conceptos como metadatos, cadena de custodia digital, herramientas forenses, sistemas de gestión de logs y mecanismos de autenticación. Según el Banco Interamericano de Desarrollo, la brecha tecnológica en los operadores de justicia representa uno de los principales obstáculos para una adecuada persecución penal en delitos informáticos (BID, 2020). Esta brecha afecta directamente la correcta valoración de la evidencia y la garantía del debido proceso.

Las instituciones judiciales han comenzado a promover programas de especialización para enfrentar este desafío. En Perú, la Academia de la Magistratura (AMAG) ha incorporado cursos sobre informática forense, cibercriminalidad y prueba digital, con el fin de fortalecer las competencias técnicas de magistrados y fiscales. De acuerdo con Cabello (2021), estos programas resultan esenciales para proporcionar conocimientos actualizados sobre procedimientos de adquisición, preservación y análisis de evidencia digital. Sin embargo, la cobertura aún es limitada y no todos los magistrados acceden a formaciones avanzadas, lo que provoca diferencias significativas en la capacidad de resolución de casos complejos vinculados a fraudes informáticos o delitos de alta tecnología.

La capacitación también debe orientarse a desarrollar habilidades críticas que permitan a los jueces evaluar informes periciales, metodologías forenses y estándares internacionales. Como señala Casey (2011), el entendimiento judicial de la ciencia forense digital es crucial para evitar decisiones basadas exclusivamente en la autoridad

técnica del perito. Un juez técnicamente capacitado puede identificar inconsistencias metodológicas, imprecisiones en la documentación o aplicaciones incorrectas de herramientas forenses, lo que contribuye a un control judicial más riguroso y a una valoración probatoria más robusta. Esta capacidad crítica reduce la posibilidad de errores judiciales derivados de una comprensión deficiente de la evidencia digital.

Finalmente, la capacitación debe ser continua, interdisciplinaria y adaptada a los rápidos avances tecnológicos. Rogers (2015) destaca que la naturaleza volátil y cambiante de la evidencia digital obliga a que los magistrados mantengan una actualización constante en temas como criptografía, redes, sistemas operativos y nuevas modalidades de ataque digital. La formación aislada o puntual es insuficiente; se requiere un modelo sostenible que integre alianzas con universidades, organismos internacionales y laboratorios forenses. De este modo, la capacitación técnica no solo fortalece la eficiencia del sistema judicial, sino que también garantiza decisiones más informadas, respetuosas del debido proceso y acordes a las exigencias del entorno digital contemporáneo.

2.2.8. Desafíos y Obstáculos en la Valoración de la Evidencia Digita

La creciente complejidad de los delitos informáticos ha puesto en evidencia la necesidad urgente de capacitar a jueces y operadores del sistema de justicia en temas relacionados con evidencia digital. En el Perú, el avance tecnológico supera con frecuencia la formación especializada de los magistrados, lo cual genera dificultades para comprender conceptos clave como metadatos, hashing, replicación forense o trazabilidad digital. Como afirma López-López (2022), la ausencia de capacitación en informática forense limita la capacidad del juez para ejercer un control efectivo sobre la prueba digital y afecta directamente la calidad de las decisiones judiciales. Por ello, la formación en competencias tecnológicas se ha convertido en una exigencia contemporánea para garantizar la correcta administración de justicia.

La Escuela Nacional de la Magistratura y el Poder Judicial han impulsado programas de actualización en materia digital; sin embargo, su alcance aún es limitado frente a la complejidad de los delitos informáticos modernos. Según Reyna Alfaro (2020), la capacitación actual suele ser general y no profundiza en aspectos técnicos esenciales, lo cual impide que los jueces evalúen adecuadamente la metodología pericial o identifiquen posibles manipulaciones en la evidencia. Además, la dinámica evolutiva de

las tecnologías obliga a que la capacitación no sea un evento aislado, sino un proceso continuo y progresivo. La falta de actualización periódica genera rezagos que afectan la valoración probatoria y la protección de derechos fundamentales.

Otro aspecto crítico es la dependencia que generan los jueces hacia los peritos informáticos. La literatura especializada señala que, sin los conocimientos básicos adecuados, los magistrados tienden a aceptar de manera acrítica los informes periciales, sin evaluar la pertinencia de los métodos empleados o la fiabilidad de las herramientas forenses. Casey (2011) advierte que esta dependencia reduce la capacidad de control judicial y coloca el peso de la decisión en manos del especialista técnico, afectando la independencia y la solidez del razonamiento probatorio. Una adecuada formación técnica permite al juez ejercer una evaluación crítica y razonada, fortaleciendo la legitimidad del proceso penal.

Finalmente, la capacitación en evidencia digital no solo mejora la valoración de la prueba, sino que contribuye al respeto del debido proceso y a la garantía de la presunción de inocencia. Jiménez Rivas (2023) señala que la falta de comprensión técnica puede llevar a errores graves, como aceptar evidencia contaminada, no autentificada o recolectada sin garantías legales. Por ello, la profesionalización tecnológica de los magistrados es un componente clave para enfrentar los retos de la criminalidad informática y asegurar decisiones justas, coherentes y fundamentadas. En consecuencia, la capacitación especializada se convierte en una obligación institucional para fortalecer el sistema de justicia penal ante los desafíos del entorno digital.

2.2.8.1. Falta de recursos y tecnología en el sistema judicial

Uno de los principales desafíos en la valoración de la evidencia digital dentro del sistema judicial peruano es la carencia de recursos tecnológicos adecuados. Esta limitación afecta directamente la capacidad de jueces, fiscales y peritos para analizar información digital de manera eficiente y conforme a estándares internacionales. Según un informe del Banco Interamericano de Desarrollo, en América Latina persiste una brecha significativa en la modernización tecnológica de los sistemas de justicia, lo que impacta en la gestión adecuada de delitos informáticos (BID, 2020). En el caso peruano, ello se refleja en la insuficiencia de equipos informáticos especializados, laboratorios forenses digitales y plataformas integradas para el tratamiento seguro de datos.

La falta de tecnología adecuada también limita la aplicación correcta de técnicas forenses como la clonación bit a bit, el análisis de metadatos o la recuperación de información borrada. Para Flores y Medina (2021), en muchos órganos jurisdiccionales del país los peritos deben trabajar con software limitado o incluso herramientas gratuitas que no cumplen con los estándares de precisión y trazabilidad exigidos internacionalmente. Esta situación no solo dificulta la obtención y análisis de evidencia digital, sino que genera un riesgo importante de que los resultados periciales sean cuestionados durante el juicio, afectando la solidez probatoria del caso.

Otro problema derivado de la carencia tecnológica es la imposibilidad de implementar sistemas robustos de cadena de custodia digital, los cuales requieren dispositivos de almacenamiento forense, servidores seguros, sistemas de registro automatizado y herramientas de verificación hash. De acuerdo con López-López (2022), la falta de estos recursos provoca que la evidencia digital sea manipulada o trasladada utilizando procedimientos inadecuados, lo que compromete su integridad y desde luego su admisibilidad en juicio. En delitos informáticos —como el fraude electrónico, el acceso ilícito o la manipulación de datos— cualquier alteración mínima en la información puede invalidar la prueba, generando impunidad o procesos judiciales deficientes.

Finalmente, la insuficiencia de recursos tecnológicos se agrava por la falta de inversión sostenida y de políticas públicas orientadas a la transformación digital de la justicia. El Ministerio de Justicia ha reconocido en diversos informes la necesidad urgente de modernizar infraestructuras y capacitar al personal para enfrentar el aumento exponencial de delitos cometidos mediante tecnologías digitales (MINJUSDH, 2021). Sin tecnología adecuada, el sistema judicial no puede responder con eficacia a los retos probatorios que plantean estos delitos, obstaculizando la administración de justicia y disminuyendo la confianza ciudadana. En suma, la precariedad tecnológica constituye uno de los obstáculos estructurales más relevantes en la correcta valoración de la evidencia digital en el Perú.

2.2.8.2. Falta de peritos informáticos o especialistas en evidencia digital

Uno de los problemas más significativos en la valoración de la evidencia digital dentro del sistema judicial es la insuficiencia de peritos informáticos especializados. En contextos donde los delitos informáticos se han incrementado de manera exponencial,

como advierte Trend Micro (2023), la demanda de especialistas supera ampliamente la capacidad institucional para atender todos los casos. En países como el Perú, esta escasez genera retrasos en las investigaciones y limita la posibilidad de realizar pericias oportunas y exhaustivas. La falta de personal técnico especializado no solo afecta la eficiencia del sistema, sino también la calidad del análisis de datos digitales, lo que puede comprometer el derecho al debido proceso y la correcta administración de justicia.

Asimismo, la escasez de peritos genera una dependencia excesiva de informes elaborados por entidades externas o por peritos privados, cuyos criterios metodológicos pueden variar significativamente. Como señala Casey (2011), la investigación forense digital requiere procedimientos estandarizados y replicables; sin embargo, cuando los actores involucrados aplican metodologías diversas, se corre el riesgo de obtener resultados inconsistentes o poco confiables. En el ámbito peruano, esta situación se agrava debido a la limitada oferta de programas de formación especializada y la ausencia de certificaciones oficiales obligatorias para ejercer como perito digital. Esto provoca brechas de calidad entre los informes que se presentan en sede judicial, lo que dificulta la labor de valoración del juez.

Un efecto adicional de la carencia de peritos informáticos es el incremento de la carga laboral en los pocos especialistas disponibles, lo que puede repercutir en la profundidad y precisión de sus análisis. De acuerdo con la INTERPOL (2022), el aumento constante de casos de ciberdelincuencia en la región exige mayor capacidad técnica y humana para realizar investigaciones complejas que implican análisis de redes, dispositivos móviles, sistemas en la nube y criptografía. En el Perú, este déficit de profesionales limita la capacidad del Ministerio Público y de la Policía Nacional para responder adecuadamente a los delitos cibernéticos, especialmente aquellos relacionados con fraudes informáticos que requieren un análisis minucioso de logs, metadatos y patrones de comportamiento digital.

Finalmente, la falta de especialistas también afecta la defensa técnica de los imputados, pues dificulta la posibilidad de contar con peritajes independientes que permitan contrastar o refutar los informes del Ministerio Público. Rogers (2015) sostiene que la existencia de múltiples visiones periciales es fundamental para garantizar la transparencia y rigor científico en la valoración de la evidencia digital. Sin un número adecuado de peritos, se limita el principio de igualdad de armas y se corre el riesgo de

que la prueba digital adquiera un valor casi absoluto sin el debido contraste técnico. Por ello, la escasez de peritos informáticos constituye uno de los obstáculos más graves para la consolidación de un sistema judicial capaz de enfrentar adecuadamente los desafíos del entorno digital.

2.2.8.3. Problemas jurídicos y tecnológicos en la validación de la evidencia digital

La creciente digitalización de las actividades humanas ha generado nuevos retos en la administración de justicia, especialmente en los procesos penales que involucran evidencia digital. En este contexto, la capacitación técnica de los jueces se vuelve imprescindible para comprender adecuadamente la naturaleza, el origen y la fiabilidad de los elementos probatorios provenientes de dispositivos electrónicos o entornos digitales. Según López-López (2022), el desconocimiento de conceptos como metadatos, algoritmos de hashing, cadenas de bloques o copias forenses puede afectar directamente la correcta valoración judicial de la prueba. Por ello, la actualización constante resulta una exigencia que trasciende la formación jurídica tradicional.

> Diversas investigaciones han demostrado que la falta de capacitación técnica limita la capacidad de los jueces para evaluar informes periciales complejos o identificar irregularidades en el manejo de la evidencia digital. Casey (2011) sostiene que la evidencia extraída de sistemas informáticos requiere de procedimientos rigurosos cuya explicación técnica puede resultar difícil de comprender sin conocimientos especializados. La ausencia de esta formación genera una dependencia excesiva del perito, lo que puede afectar el control judicial de la prueba y comprometer el principio de libre valoración razonada.

En el Perú, el Poder Judicial y la Academia de la Magistratura han implementado programas de formación continua relacionados con delitos informáticos y prueba digital, aunque su alcance todavía es limitado. De acuerdo con Reyna Alfaro (2020), la capacitación suele centrarse en aspectos teóricos del derecho penal informático, dejando de lado competencias técnicas esenciales para la interpretación adecuada de evidencia digital compleja. Esta situación refleja la necesidad de reforzar programas interdisciplinarios que integren informática forense, ciberseguridad y análisis digital con la normativa jurídica aplicable.

2.2.9. Categorías de Análisis en la Investigación

A. **Autenticidad de la evidencia digital**

La autenticidad de la evidencia digital es uno de los pilares fundamentales para su admisibilidad y valoración en los procesos penales. Esta categoría se refiere a la capacidad de demostrar que un archivo, registro o dato informático corresponde exactamente a lo que se afirma que es, sin sufrir alteraciones durante su manipulación o preservación. Tal como afirma Casey (2011), la autenticidad implica la verificación de la fuente, el contenido y las condiciones en las que el dato fue generado, lo cual exige métodos rigurosos para asegurar la fidelidad de la información presentada al juez. Esta exigencia cobra especial relevancia en casos de fraude informático, donde los datos pueden ser fácilmente manipulados mediante técnicas de edición o falsificación digital.

Un aspecto central para garantizar la autenticidad es la verificación de la integridad del archivo mediante técnicas criptográficas, como los algoritmos hash (MD5, SHA-1, SHA-256). Estas herramientas permiten constatar que el archivo no ha sido modificado desde su obtención, lo que constituye una garantía técnica indispensable para el sistema judicial. Carrier (2016) señala que el cálculo de hashes es un estándar internacionalmente reconocido para demostrar la inalterabilidad de la evidencia digital, y su uso es obligatorio en la mayoría de procedimientos forenses. La comparación entre los valores hash generados en diferentes etapas permite identificar cualquier manipulación, accidental o intencional, del contenido digital.

La autenticidad no solo implica un análisis técnico, sino también la revisión contextual del origen de los datos. En este sentido, la procedencia del material digital debe estar claramente documentada, incluyendo información sobre el dispositivo donde fue encontrado, la fecha y hora de la extracción y las circunstancias de la intervención. Según Rogers (2015), esta perspectiva contextual es clave porque permite relacionar el dato con su entorno digital, reduciendo la posibilidad de interpretaciones erróneas o manipulaciones exógenas. De esta manera, la autenticidad se convierte en una categoría integral que combina aspectos técnicos con elementos probatorios de carácter situacional.

Finalmente, la autenticidad constituye un elemento esencial para garantizar el debido proceso y la fiabilidad de las decisiones judiciales. La jurisprudencia comparada ha resaltado que solo la evidencia auténtica puede ser considerada válida en un juicio

penal, especialmente en delitos tecnológicos donde la manipulación de datos es común. Como destaca López-López (2022), los jueces deben aplicar criterios de verificación reforzada en la evidencia digital, evaluando tanto su integridad como su origen institucional, técnico y procedimental. Por ello, la autenticidad se configura como una categoría crítica y transversal en la valoración probatoria en casos de fraude informático.

B. Cadena de custodia

La cadena de custodia constituye un conjunto de procedimientos destinados a documentar y garantizar el manejo seguro y controlado de la evidencia desde su obtención hasta su presentación en juicio. En el caso de la evidencia digital, la cadena de custodia adquiere una importancia reforzada debido a la facilidad con la que la información puede ser alterada, copiada o destruida sin dejar señales visibles. Palomo Vélez (2021) sostiene que la cadena de custodia digital debe incluir la identificación precisa del soporte, registro de accesos, preservación de la metadata y documentación exhaustiva de cada manipulación. Esto permite garantizar que la evidencia no ha sido comprometida durante las distintas fases del proceso penal.

Un componente esencial de la cadena de custodia digital es la creación de una copia forense bit a bit del dispositivo o archivo original. Este procedimiento, ampliamente validado por organizaciones como el NIST, garantiza que el análisis se realice sobre una réplica exacta, preservando el soporte original en condiciones inviolables. Carrier (2016) destaca que trabajar con copias forenses evita la alteración no intencional del contenido, al tiempo que permite repetir los análisis sin comprometer el valor probatorio de la evidencia. La cadena de custodia exige que se documenten los cálculos hash de la copia y el original, asegurando que ambos coincidan.

La cadena de custodia digital también incluye la gestión adecuada del almacenamiento y transporte de la evidencia. Esto implica el uso de contenedores seguros, acceso restringido y sistemas de registro que permitan controlar quién tuvo contacto con la evidencia y en qué circunstancias. Según Casey (2011), la transparencia y trazabilidad del manejo de los datos es fundamental para demostrar la confiabilidad de la evidencia digital ante el tribunal. Cualquier quiebre en este proceso puede comprometer la admisibilidad de la evidencia, generando dudas sobre su integridad.

Finalmente, la cadena de custodia se constituye como una garantía procesal vinculada al debido proceso y al derecho de defensa. La jurisprudencia ha establecido que las irregularidades en la cadena de custodia pueden llevar a la exclusión de la prueba, especialmente en delitos informáticos donde la autenticidad es un requisito esencial. Como menciona Reyna Alfaro (2020), la cadena de custodia no es un mero formalismo, sino un requisito indispensable para preservar la validez y confiabilidad de la evidencia digital, lo cual impacta directamente en la legitimidad del juicio.

C. **Capacitación técnica de los jueces**

La capacitación técnica de los jueces en materia de evidencia digital es una categoría crucial debido al creciente uso de tecnologías digitales en la comisión de delitos y en la producción de pruebas. Los operadores de justicia deben comprender los fundamentos de la informática forense, la naturaleza de los datos digitales y los requisitos técnicos que condicionan su validez. López-López (2022) advierte que la falta de conocimientos especializados puede dificultar la comprensión de conceptos complejos, como metadatos, logs, cifrado o copias forenses, generando riesgos en la valoración probatoria. Esta brecha tecnológica constituye uno de los mayores desafíos para la justicia contemporánea.

La formación judicial continua permite a los jueces adaptarse a los avances tecnológicos y aplicar criterios adecuados de valoración probatoria. En muchos países, incluido el Perú, el Poder Judicial ha implementado programas de capacitación en delitos informáticos, informática forense y evidencia digital. San Martín Castro (2017) señala que la capacitación técnica es una herramienta indispensable para mejorar la calidad de las resoluciones judiciales, ya que permite a los jueces identificar falencias procedimentales, cuestionar peritajes deficientes y reconocer elementos de manipulación digital. Esto garantiza decisiones más informadas y ajustadas a los estándares probatorios vigentes.

La capacitación también tiene un impacto directo en la independencia judicial durante el proceso de valoración de pruebas. Un juez con conocimientos tecnológicos es menos propenso a depender exclusivamente del perito, lo que fortalece su capacidad de control de la prueba y su función de garante del debido proceso. Como explica Reyna Alfaro (2020), el entendimiento básico de las tecnologías permite al juez realizar

preguntas pertinentes, solicitar aclaraciones técnicas y detectar inconsistencias en los informes periciales. Esto reduce la posibilidad de errores judiciales y mejora la transparencia del proceso penal.

Finalmente, la capacitación técnica fortalece la legitimidad del sistema judicial, ya que permite brindar respuestas más adecuadas a los desafíos que plantean los delitos informáticos. La evidencia digital es cada vez más frecuente no solo en casos tecnológicos, sino también en delitos comunes, lo que hace indispensable que los jueces posean competencias mínimas en materia digital. Según Rivas-López (2020), una justicia tecnológicamente preparada contribuye a decisiones más justas, eficaces y acordes al contexto digital contemporáneo, elevando la calidad institucional del sistema penal.

D. Disponibilidad de peritos informáticos

La disponibilidad de peritos informáticos constituye una categoría esencial, dado que el análisis de la evidencia digital requiere conocimientos técnicos especializados que no poseen los operadores jurídicos. Los peritos informáticos son responsables de identificar, recolectar, preservar y analizar datos digitales mediante metodologías científicas reconocidas. Tal como indica Casey (2011), la adecuada intervención pericial determina en gran medida la validez, autenticidad e integridad de la evidencia digital. Por ello, un sistema judicial sin suficientes peritos enfrentará serias dificultades para investigar y sancionar delitos informáticos.

En muchos países, incluido el Perú, existe una escasez significativa de peritos especializados en informática forense, lo que genera retrasos procesales y limitaciones en la producción de evidencia técnica. Palomo Vélez (2021) señala que la falta de peritos provoca que un solo especialista deba atender múltiples casos, afectando la profundidad de los análisis y la prontitud en la emisión de informes. Este déficit no solo afecta a delitos informáticos, sino también a delitos comunes donde la evidencia digital es clave, como homicidios, extorsiones o crimen organizado.

La disponibilidad limitada de peritos también afecta la calidad del peritaje, ya que en ocasiones se recurre a profesionales no certificados o con escasa experiencia en informática forense. Carrier (2016) advierte que el uso de herramientas inadecuadas o metodologías no estandarizadas puede comprometer la integridad de la evidencia, generando informes poco confiables que puedan ser descartados en juicio. La formación

continua y la certificación internacional (como CEH, CHFI, EnCE) resultan esenciales para garantizar la calidad de los peritajes.

Finalmente, la escasez de peritos informáticos afecta de manera directa el derecho al debido proceso, pues limita la capacidad de las partes para ofrecer prueba técnica de calidad. Como destaca Salinas Siccha (2019), tanto la defensa como la fiscalía deben tener acceso a peritos competentes para garantizar un equilibrio procesal y evitar decisiones judiciales basadas en evidencia incompleta o defectuosa. Por ello, la disponibilidad de peritos se convierte en un factor determinante para el adecuado funcionamiento del sistema penal en la era digital.

E. Factores contextuales y subjetivos

Los factores contextuales y subjetivos constituyen elementos que influyen en la valoración judicial de la evidencia digital, aunque no se desprenden directamente de la estructura técnica de la prueba. Estos factores incluyen las creencias personales del juez, su experiencia previa, el contexto social del caso, la presión mediática y las particularidades del entorno institucional. Según Kassin et al. (2013), los jueces, como cualquier ser humano, no están completamente libres de sesgos cognitivos, los cuales pueden influir en su percepción de la fiabilidad de la evidencia presentada. Esto adquiere relevancia en casos de delitos informáticos, donde la complejidad técnica puede generar incertidumbre.

El contexto institucional también influye en la valoración probatoria. La falta de recursos tecnológicos, la sobrecarga procesal o la ausencia de protocolos estandarizados pueden condicionar la capacidad del juez para evaluar la evidencia digital con precisión. López-López (2022) señala que los factores organizacionales pueden llevar a decisiones basadas en criterios pragmáticos antes que estrictamente probatorios, especialmente cuando el acceso a peritajes especializados es limitado. Ello implica que la calidad de la justicia puede variar según el contexto jurisdiccional.

Los factores subjetivos también se relacionan con el nivel de familiaridad del juez con tecnologías digitales. Como advierte Reyna Alfaro (2020), los jueces con mayor exposición a tecnologías o formación digital tienden a evaluar con mayor seguridad la evidencia digital, mientras que aquellos con menor experiencia pueden mostrar reticencia

o excesiva dependencia del perito. Esto puede generar asimetrías en la valoración probatoria entre diferentes órganos jurisdiccionales.

Finalmente, los factores sociales y culturales influyen en la percepción judicial del riesgo asociado a los delitos informáticos. Rogers (2015) menciona que el aumento de casos mediáticos de cibercrimen puede generar una percepción social de mayor peligrosidad, lo cual incide en la severidad con la que los jueces abordan la evidencia digital en sus decisiones. Comprender estos factores es esencial para analizar la dinámica real en la valoración de pruebas digitales y para identificar los puntos donde el sistema judicial puede mejorar en objetividad y rigor técnico.

2.3. Marco conceptual

a. Evidencia digital

La evidencia digital se refiere a toda información almacenada, transmitida o procesada por medios electrónicos y que puede servir como elemento probatorio en un proceso penal. Este tipo de evidencia incluye archivos, metadatos, registros de actividad, comunicaciones electrónicas, bases de datos, imágenes digitales y otros elementos presentes en dispositivos o redes tecnológicas. Su relevancia radica en que permite reconstruir hechos delictivos cometidos en entornos informáticos. Debido a su naturaleza intangible, volátil y fácilmente modificable, la evidencia digital exige procedimientos rigurosos de identificación, preservación y análisis, garantizando su autenticidad e integridad para que sea admitida y valorada correctamente en sede judicial.

b. Delitos informáticos

Los delitos informáticos comprenden aquellas conductas ilícitas que utilizan sistemas, redes o dispositivos tecnológicos como medio, objeto o finalidad del acto criminal. Entre los más frecuentes se encuentran el fraude informático, el acceso ilícito, la interceptación de datos, el sabotaje informático y la suplantación digital. La expansión del uso de tecnologías ha incrementado la incidencia de estos delitos, obligando a los sistemas jurídicos a adoptar normativas especializadas como la Ley N.º 30096 en el Perú. Estos delitos presentan desafíos particulares, ya que requieren conocimientos técnicos para su investigación y pruebas no tradicionales, cuya correcta interpretación depende de especialistas en informática forense y operadores de justicia capacitados.

c. Autenticidad de la evidencia digital

La autenticidad de la evidencia digital implica la verificación de que la información presentada en un proceso penal corresponde exactamente al estado original en que fue obtenida, sin haber sido alterada, manipulada o sustituida. Este principio es fundamental para garantizar la validez de la prueba, ya que la mínima modificación puede comprometer su credibilidad. Para demostrar autenticidad se emplean mecanismos técnicos como funciones hash, firmas digitales, registros de auditoría y documentación rigurosa de todos los procedimientos realizados sobre el soporte digital. La ausencia de autenticidad genera dudas razonables que pueden llevar a la exclusión de la evidencia o a la reducción significativa de su valor probatorio.

d. Cadena de custodia digital

La cadena de custodia digital es el procedimiento documentado que garantiza el control continuo sobre la evidencia digital desde su obtención hasta su presentación en juicio. Su propósito es asegurar que cada transferencia, análisis o almacenamiento haya sido realizado siguiendo protocolos que preserven la integridad y autenticidad del material. Este proceso debe registrar quién tuvo acceso a la evidencia, qué acciones realizó, con qué herramientas y en qué momento. Debido a la facilidad con la que la evidencia digital puede ser manipulada, la ruptura o irregularidades en la cadena de custodia pueden invalidarla como prueba. Por ello, es un elemento indispensable para su valor probatorio en investigaciones de delitos informáticos.

e. Capacitación técnica de los jueces

La capacitación técnica de los jueces en materia de evidencia digital se refiere al conjunto de conocimientos especializados que deben adquirir para comprender la naturaleza, obtención, análisis y limitaciones de las pruebas digitales. Dado que los procesos penales relacionados con delitos informáticos presentan altos niveles de complejidad tecnológica, los jueces que carecen de formación en informática forense pueden enfrentar dificultades al interpretar informes periciales o evaluar la legalidad y fiabilidad de los procedimientos realizados. Una adecuada capacitación permite fortalecer

la capacidad de valoración judicial, disminuir la dependencia absoluta del perito y garantizar decisiones motivadas que respeten estándares científicos y principios constitucionales.

f. Peritos informáticos

Los peritos informáticos son especialistas encargados del análisis técnico de evidencia digital mediante métodos científicos reconocidos internacionalmente. Su función consiste en identificar, recolectar, preservar, examinar e interpretar datos digitales relevantes para la investigación penal. Debido a que los jueces y fiscales no siempre poseen conocimientos avanzados en tecnología, los peritos actúan como mediadores entre el lenguaje técnico y el jurídico, explicando de manera comprensible los procesos utilizados y sus resultados. Su intervención es esencial en casos de delitos informáticos, ya que la fiabilidad de la prueba depende en gran medida de la pericia, metodología y herramientas empleadas durante el análisis digital.

CAPÍTULO III
SUPUESTOS Y CATEGORÍAS

3.1. Supuesto general

La valoración de la evidencia digital en las sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga durante el periodo 2022 – 2024, es predominantemente implícita, informal y asimilada a la prueba documental tradicional, sin aplicación explícita de criterios técnico-forenses (autenticidad, integridad, cadena de custodia, fiabilidad), lo que genera una deficiencia estructural en la prueba de estos delitos que no se subsana ni siquiera en los casos con debate probatorio pleno.

3.2. Supuestos específicos

- Los jueces de Huamanga **no aplican explícitamente** criterios técnicos de autenticidad, integridad, cadena de custodia o fiabilidad de la evidencia digital. En su lugar, aplican criterios jurídicos generales (pertinencia, conducencia, utilidad) y tratan la evidencia digital como prueba documental tradicional.

- Las principales limitaciones son: (a) ausencia de peritaje informático en la mayoría de casos, (b) falta de formación técnica de jueces y fiscales en evidencia digital, (c) dependencia de documentos impresos proporcionados por bancos y empresas de telecomunicaciones sin verificación de su integridad, y (d) resolución de casos por conformidad para evitar el desafío probatorio.

- Existe una **brecha significativa** entre el discurso normativo (lo que operadores declaran que debería hacerse) y la práctica documentada en sentencias (lo que realmente se hace), evidenciada en la ausencia de análisis técnico incluso cuando hay debate probatorio pleno.

3.3. Matriz de categorización

Categoría	Dimensiones	Descripción / Indicadores
1. Admisibilidad de la evidencia digital	1.1. Cadena de custodia	- Registro de incautación del dispositivo - Acta de transferencia de evidencias - Integridad del almacenamiento (hash)
	1.2. Autenticidad	- Acreditación de origen del dato (ej. logs, metadatos) - No alteración probada
	1.3. Legalidad de obtención	- Con orden judicial o excepción legal - Respeto a derechos fundamentales
2. Métodos de análisis forense empleados	2.1. Herramientas utilizadas	- Software forense reconocido (FTK, EnCase, Autopsy, etc.) - Versión y validación
	2.2. Procedimiento técnico	- Copia bit a bit (imagen forense) - Análisis de logs, correos, transacciones, malware - Preservación de metadatos
	2.3. Pericia oficial	- Designación de perito por el Ministerio Público o juzgado - Informe pericial detallado
3. Valoración probatoria según sana crítica	3.1. Motivación del juez	- Explicación razonada de por qué la evidencia digital es creíble o no - Uso de máximas de experiencia informática
	3.2. Relación con otros medios probatorios	- Corroboración con declaraciones, documentos, etc. - Coherencia interna
	3.3. Grados de convicción	- Certeza positiva / negativa - Duda razonable respecto a la evidencia digital
4. Tipicidad del fraude informático	4.1. Conducta típica (art. 207-A CP)	- Manipulación, destrucción o supresión de datos - Transferencia no consentida de activos
	4.2. Vinculación evidencia digital – sujeto activo	- Identificación del autor mediante IP, MAC, cuentas, etc. - Evidencia de engaño o abuso de confianza

	4.3. Resultado patrimonial	- Acreditación del perjuicio mediante registros digitales (bancos, wallets, etc.)
5. Limitaciones en la práctica judicial de Huamanga	5.1. Infraestructura tecnológica	- Acceso a laboratorios forenses (ej. División de Investigación Criminal de la PNP) - Disponibilidad de peritos especializados
	5.2. Argumentación judicial deficiente	- Ausencia de análisis técnico en la sentencia - Subvaloración de la evidencia digital
	5.3. Desconocimiento del juez	- Falta de capacitación en informática forense - Delegación acrítica en el peritaje

CAPÍTULO IV
METODOLOGÍA

4.1. Enfoque

La investigación adopta un **enfoque cualitativo**, el cual resulta el más adecuado para alcanzar los objetivos planteados, toda vez que se busca comprender en profundidad las prácticas, percepciones y discursos de los operadores de justicia en torno a la valoración de la evidencia digital, así como analizar detalladamente el contenido de las sentencias judiciales. Este enfoque permite, además, la triangulación de fuentes (sentencias y entrevistas) y la emergencia de categorías de análisis no previstas inicialmente, características propias del diseño flexible que orienta la presente investigación.

De acuerdo a Hernandez & Mendoza (2019) "la ruta de la investigación cualitativa se enfoca en comprender los fenómenos, explorándolos desde la perspectiva de los participantes en su ambiente natural y en relación con su contexto" (pág. 390).

4.2. Tipo de investigación

La investigación es de tipo **básica o pura**, pues tiene como propósito fundamental generar conocimiento nuevo sobre la valoración de la evidencia digital en sentencias por fraude informático, sin que exista una aplicación práctica inmediata o un desarrollo tecnológico directo derivado de los hallazgos.

Según Avendaño (2020) señala que:

> La investigación básica, fundamental o pura, también llamada teórica o dogmática, se orienta a clarificar, incrementar y profundizar la densidad conceptual de una ciencia determinada, explicando fenómenos que no han sido explicados, formulando nuevas teorías o modificando las ya existentes o encontrando nuevas relaciones entre los factores que intervienen en un fenómeno, pero sin intención de corroborar directa- mente o contrastar esos hallazgos con aspectos concretos de aplicación. (pág.94)

4.3. Nivel de investigación

En cuanto a la investigación descriptiva, Carrasco (2005) señala lo siguiente:

> Es la que no tiene propósitos aplicativos inmediatos, pues solo busca ampliar y profundizar el caudal de conocimientos científicos existentes acerca de la realidad. su objeto de estudio lo constituye las teorías científicas, las mismas que las analiza para perfeccionar sus contenidos. (Pág. 43)

El nivel de la investigación es **descriptivo-explicativo**. Es descriptivo porque se propone caracterizar detalladamente cómo los jueces de los Juzgados Penales Unipersonales de Huamanga valoran la evidencia digital en las sentencias por fraude informático, identificando los criterios técnicos que aplican —explícita o implícitamente—, las deficiencias recurrentes y las características comunes en el tratamiento de este tipo de prueba. Es explicativo porque no se limita a describir el fenómeno, sino que busca comprender las razones que subyacen a la práctica judicial observada, indagando en las limitaciones formativas, materiales y procesales que enfrentan los operadores de justicia, así como en la coherencia —o incoherencia— entre el discurso de las sentencias y las prácticas declaradas por jueces y fiscales.

4.4. Métodos

La investigación emplea, de manera articulada, el método analítico-sintético para descomponer y recomponer los elementos constitutivos de la valoración de la evidencia digital en las sentencias; el método hermenéutico o interpretativo para comprender el sentido que los operadores de justicia atribuyen a sus propias prácticas y discursos; el método comparativo para contrastar las cinco sentencias analizadas entre sí y para triangular los hallazgos documentales con las entrevistas; y los métodos fenomenológico y de análisis temático para procesar las entrevistas, accediendo a las experiencias subjetivas de jueces y fiscales e identificando categorías emergentes como confianza institucional, déficit formativo, limitaciones materiales, conclusión anticipada y brecha discurso-práctica.

4.5. Diseño de la investigación

El diseño de la investigación es no experimental, transversal. Es no experimental porque no se manipulan deliberadamente las variables ni se interviene en la realidad estudiada, limitándose el investigador a observar, analizar e interpretar los fenómenos tal como se presentan en su contexto natural, sin ejercer control ni modificar las condiciones existentes en los Juzgados Penales Unipersonales de Huamanga.

Con respecto al diseño transversal, Perez, L. Perez, R. & Seca, M. V. (2020) afirman "Tomaremos los datos una sola vez y los resultados que obtengamos serán válidos para explicar el estado de situación en ese momento específico" (Pág. 217).

4.6. Población y muestra

4.6.1. Población

Según Carrasco (2005) la población es el "Conjunto de todos los elementos que forman parte del espacio territorial al que pertenece el problema de investigación y poseen características mucho más concretas que el universo" (Pág. 236).

La población de estudio está conformada por la totalidad de sentencias por delito de fraude informático emitidas por los Juzgados Penales Unipersonales del distrito judicial de Huamanga, así como por los jueces y fiscales penales que intervienen en dichos procesos.

4.6.2. Muestra

La muestra, seleccionada mediante un muestreo intencional o por conveniencia propio de la investigación cualitativa, está compuesta por cinco sentencias representativas de los distintos tipos de resolución (absolutoria, condenatoria con juicio oral y condenatoria por conclusión anticipada), y por seis operadores de justicia (tres jueces y tres fiscales) con distintos niveles de experiencia y trayectoria, seleccionados por su disponibilidad y disposición a participar en el estudio, así como por su conocimiento directo y cotidiano de la problemática investigada.

4.6.3. Muestreo

El muestreo empleado en la presente investigación es de tipo no probabilístico e intencional o por conveniencia, el cual resulta el más adecuado en el marco de un enfoque

cualitativo donde no se busca la representatividad estadística ni la generalización de resultados a una población mayor, sino la profundidad y riqueza informativa de los casos seleccionados. Las sentencias fueron elegidas con base en los siguientes criterios de inclusión: (i) que se trate de sentencias por delito de fraude informático tipificado en el artículo 8° de la Ley N° 30096; (ii) que hayan sido emitidas por los Juzgados Penales Unipersonales de Huamanga; y (iii) que representen la diversidad de tipos de resolución existentes (absolutoria, condenatoria con juicio oral, condenatoria por conclusión anticipada).

Por su parte, los jueces y fiscales fueron seleccionados con base en los siguientes criterios: (i) que ejerzan o hayan ejercido funciones en el distrito judicial de Huamanga durante el período de estudio; (ii) que tengan experiencia en casos de fraude informático; (iii) que representen distintos niveles de antigüedad y trayectoria profesional; y (iv) que manifiesten su disposición voluntaria a participar en la entrevista. Este tipo de muestreo intencional permite asegurar que los casos seleccionados sean informativamente ricos y relevantes para los objetivos de la investigación, priorizando la calidad y pertinencia de la información sobre la cantidad de unidades analizadas.

4.7. Técnicas e instrumentos

La investigación emplea dos técnicas principales con sus respectivos instrumentos, articuladas entre sí para garantizar la triangulación de fuentes y la robustez de los hallazgos.

En primer lugar, se utiliza la técnica de análisis documental, la cual consiste en la revisión sistemática y el examen detallado de las sentencias judiciales seleccionadas. El instrumento empleado para esta técnica es la ficha de análisis documental, diseñada específicamente para los fines de la investigación, la cual contiene categorías predefinidas que orientan la extracción de información relevante: datos generales de la sentencia, identificación del caso, evidencia digital incorporada, criterios de valoración probatoria aplicados por el juez, fundamentación jurídica, decisión judicial y análisis crítico del investigador. Esta ficha permite sistematizar la información de cada sentencia de manera uniforme, facilitando el posterior análisis comparativo entre los distintos casos.

En segundo lugar, se emplea la técnica de entrevista semiestructurada, la cual consiste en un diálogo guiado por un conjunto de preguntas abiertas que permiten al

entrevistado desarrollar sus respuestas con libertad, pero dentro de los márgenes temáticos de interés para la investigación. El instrumento correspondiente es la guía de entrevista, elaborada en dos versiones diferenciadas: una para jueces y otra para fiscales, adaptando las preguntas a las funciones y perspectivas propias de cada perfil profesional. Ambas versiones abordan dimensiones comunes como criterios técnicos aplicados, autenticidad e integridad de la prueba, limitaciones de los operadores de justicia y coherencia entre discurso y práctica, pero con formulaciones específicas según el rol del entrevistado. Las entrevistas son grabadas previo consentimiento informado del participante y posteriormente transcritas textualmente para su análisis, garantizando el anonimato mediante la asignación de códigos (J01, J02, J03 para jueces; F01, F02, F03 para fiscales).

4.8. Validez y confiabilidad de instrumentos

Respecto a la validez del instrumento, Carrasco (2005) menciona: “En términos más concretos podemos decir que un instrumento es válido cuando mide lo que debe medir. es decir, cuando nos permite extraer datos que preconcebidamente necesitamos conocer” (Pág. 336).

La validez de los instrumentos de investigación ha sido garantizada mediante el procedimiento de juicio de expertos, para lo cual las fichas de análisis documental y las guías de entrevista fueron sometidas a la revisión y evaluación de tres especialistas en las áreas de derecho penal, derecho procesal penal y metodología de la investigación cualitativa, quienes emitieron sus dictámenes sobre la pertinencia, claridad y relevancia de las categorías y preguntas incluidas en cada instrumento, sugiriendo ajustes que fueron incorporados en la versión definitiva. En cuanto a la confiabilidad, tratándose de una investigación cualitativa, esta se ha asegurado mediante la triangulación de fuentes (contrastando la información obtenida de las sentencias con la de las entrevistas), la auditabilidad (dejando registro detallado de los procedimientos de recolección y análisis de datos, así como de las decisiones metodológicas adoptadas) y la consistencia interna en la aplicación de los instrumentos, verificando que las fichas de análisis documental fueran aplicadas uniformemente a las cinco sentencias y que las guías de entrevista mantuvieran la misma estructura y orientación en todos los casos, con las adaptaciones pertinentes según el perfil del entrevistado.

4.9. Técnicas de procesamiento de datos

El procesamiento de los datos recogidos se ha realizado siguiendo las fases propias del análisis cualitativo. En el caso de las sentencias, una vez completadas las fichas de análisis documental, se procedió a la sistematización de la información mediante la elaboración de tablas comparativas que organizaron los hallazgos por categorías predefinidas (tipo de sentencia, evidencia digital incorporada, criterios técnicos aplicados, fundamentación jurídica, decisión judicial), para luego identificar patrones, recurrencias y diferencias entre los cinco casos analizados. En el caso de las entrevistas, las grabaciones de audio fueron transcritas textualmente en procesadores de texto, asignando un código alfanumérico a cada entrevistado (J01, J02, J03; F01, F02, F03) para garantizar el anonimato. Posteriormente, se aplicó la técnica de análisis temático, que implicó la lectura reiterada de las transcripciones, la identificación de unidades de significado, la codificación abierta de los fragmentos relevantes, la agrupación de códigos en categorías emergentes (confianza institucional, déficit formativo, limitaciones materiales, conclusión anticipada, brecha discurso-práctica) y la síntesis final de los hallazgos en tablas y narrativas interpretativas, las cuales fueron contrastadas con los resultados del análisis documental en una fase de triangulación.

4.10. Aspectos éticos

La investigación se ha desarrollado respetando rigurosamente los principios éticos exigibles a toda investigación con seres humanos y con fuentes documentales de acceso restringido. En primer lugar, se ha garantizado el principio de confidencialidad y anonimato de los entrevistados, quienes fueron informados de que sus identidades no serían reveladas en ningún informe o publicación derivada del estudio, asignándose códigos numéricos que impiden su identificación directa o indirecta. En segundo lugar, se ha respetado el consentimiento informado de los participantes, quienes fueron invitados voluntariamente a colaborar, informados sobre los objetivos de la investigación, el uso exclusivamente académico de sus respuestas y su derecho a retirarse en cualquier momento sin consecuencia alguna. En tercer lugar, en el tratamiento de las sentencias judiciales, se ha preservado la confidencialidad de los datos personales de las partes intervinientes (imputados, agraviados, testigos), cuyos nombres han sido suprimidos o anonimizados en las citas textuales incluidas en el informe final. En cuarto lugar, la investigación se ha conducido con honestidad y transparencia académica, reportando los

hallazgos tal como fueron encontrados, sin omitir información que pudiera contradecir las expectativas iniciales del investigador. Finalmente, se ha actuado con respeto a la institución judicial, evitando juicios de valor sobre la actuación de los operadores de justicia y limitándose al análisis crítico fundado en criterios técnicos y jurídicos objetivos.

CAPÍTULO V

INTERPRETACIÓN Y DISCUSIÓN DE RESULTADOS

5.1. Interpretación de resultados

En el presente capítulo se procede a la interpretación y discusión de los resultados obtenidos a partir del análisis documental de cinco sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga entre 2022 y 2024, así como de las entrevistas realizadas a tres jueces y tres fiscales del mismo distrito judicial. El objetivo central de este capítulo es dotar de significado a los hallazgos empíricos presentados en el capítulo anterior, y los sitúa a la luz de los referentes teóricos, normativos y jurisprudenciales que sirven de marco a la investigación.

La interpretación de los resultados se organiza en función de los objetivos específicos planteados, abordando sucesivamente: (i) los criterios técnicos de valoración de evidencia digital aplicados —explícita o implícitamente— por los jueces en las sentencias analizadas; (ii) las limitaciones y dificultades que enfrentan los operadores de justicia en Huamanga para valorar técnicamente la prueba digital; y (iii) la coherencia —o incoherencia— entre la valoración documentada en las sentencias y los discursos o prácticas declaradas por jueces y fiscales en las entrevistas.

Tabla 1. Caracterización general de las sentencias analizadas

Criterio	**Sentencia 1 (Exp. 00724-2020)**	**Sentencia 2 (Exp. 00477-2023)**	**Sentencia 3 (Exp. 01263-2019)**	**Sentencia 4 (Exp. 01342-2022)**	**Sentencia 5 (Exp. 02815-2019)**
Año de emisión	2022	2024	2024	2024	2023
Tipo de resolución	Absolutoria	Condenatoria (conformada)	Condenatoria (conformada)	Condenatoria (juicio oral)	Condenatoria (conformada)
Delito	Fraude informático (art. 8° Ley 30096)	Fraude informático	Fraude informático	Fraude informático	Fraude informático
Monto involucrado	S/ 4,620	S/ 29,800	S/ 1,495	S/ 9,725	S/ 1,610
Uso de criptomonedas	No	Sí (Binance)	No	No	No

En primer lugar, la muestra abarca un periodo de tres años (2022-2024), lo que permite observar la práctica judicial reciente y homogénea respecto al marco normativo aplicable (Ley N° 30096 modificada por Ley N° 30171).

En segundo lugar, se identifica un hallazgo significativo: el 60% de las sentencias analizadas (3 de 5) corresponden a procesos resueltos mediante conclusión anticipada (conformidad). Esto implica que, en dichos casos, no existió un debate probatorio pleno ni una valoración judicial autónoma de la evidencia digital, pues el imputado renunció a al contradictorio probatorio al aceptar los cargos. Este patrón sugiere que, en el distrito judicial de Huamanga, la mayoría de los procesos por fraude informático no alcanzan un juicio oral contradictorio, lo que limita la posibilidad de que los órganos jurisdiccionales desarrollen estándares técnicos de valoración de evidencia digital.

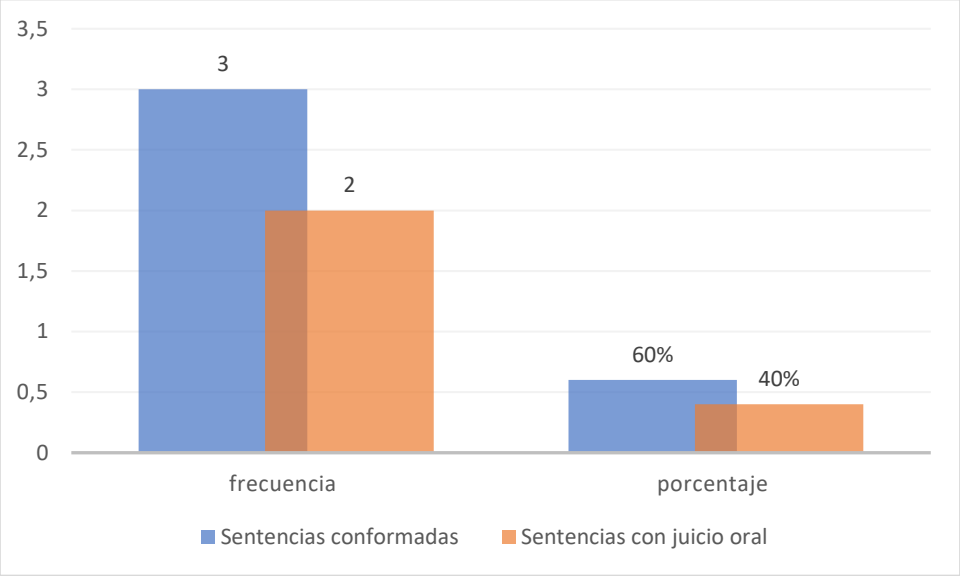
En tercer lugar, se observa que los montos involucrados no determinan el tipo de resolución. El caso de mayor cuantía (S/ 29,800, Sentencia 2) se resolvió por conformidad, mientras que el único caso con juicio oral contradictorio (Sentencia 4) corresponde a un monto intermedio (S/ 9,725). Por su parte, la sentencia absolutoria (Sentencia 1) involucra un monto de S/ 4,620, lo que evidencia que la absolución no está asociada a montos menores.

Finalmente, un dato relevante es que solo una sentencia (20%) incorpora el uso de criptomonedas como parte del modus operandi (Sentencia 2, Exp. 00477-2023). Sin embargo, como se analizará en apartados posteriores, dicho elemento no fue sometido a un análisis técnico-forense, sino que fue aceptado fácticamente por la conformidad del acusado. Esto evidencia una oportunidad perdida para establecer criterios de valoración de evidencia digital basada en tecnología blockchain.

Cuadro 1 Frecuencia de tipos de resolución y características relevantes en la muestra analizada

Criterio	**Frecuencia**	**Porcentaje**
Sentencias conformadas	3/5	60%
Sentencias con juicio oral	2/5	40%

Figura 1 Frecuencia de tipos de resolución y características relevantes en la muestra analizada



Fuente: Elaboración propia

Tabla 2 Tratamiento de la evidencia digital por tipo de sentencia

Tipo de sentencia	Expediente	¿Se aplicaron criterios técnicos? (Autenticidad/Integridad/Cadena de custodia)	¿Se realizó peritaje informático?	Forma de valoración predominante	Nivel de incidencia de la evidencia digital
Absolutoria	00724-2020	No (0/3)	Testimonio pericial genérico (no forense)	Implícita (como documental)	Complementaria
Condenatoria (conformada)	00477-2023	No (0/3)	No	Basada en aceptación de cargos	Determinante (no valorada)
Condenatoria (conformada)	01263-2019	No (0/3)	No	Basada en aceptación de cargos	Determinante (no valorada)
Condenatoria (conformada)	02815-2019	No (0/3)	No	Basada en aceptación de cargos	Determinante (no valorada)

Condenatoria (juicio oral)	01342-2022	No (0/3)	No	Implícita (como documental)	Determinante

La tabla revela un hallazgo transversal a toda la muestra: en ninguno de los cinco casos analizados se aplicaron criterios técnicos de valoración de evidencia digital (autenticidad, integridad, cadena de custodia). Esta ausencia es independiente del sentido del fallo (absolución o condena) y de la etapa procesal (juicio oral con debate o conclusión anticipada). Sin embargo, se identifican diferencias significativas en la forma de valoración y en el rol de la evidencia digital, según el tipo de sentencia:

a) En la sentencia absolutoria (Exp. 00724-2020)

La evidencia digital (registros bancarios) fue tratada implícitamente como prueba documental tradicional, sin cuestionar su autenticidad ni origen técnico. Se incorporó un testimonio pericial, pero este fue genérico (explicación del spoofing como modus operandi) y no implicó un análisis forense del caso concreto. La evidencia digital tuvo un rol complementario: acreditó la materialidad del delito (la transferencia existió), pero no la responsabilidad penal de la acusada, lo que condujo a la absolución por duda razonable.

b) En las sentencias condenatorias por conformidad (Exps. 00477-2023, 01263-2019 y 02815-2019):

La evidencia digital tuvo un rol determinante en la acusación, pero no fue valorada técnicamente por el juez. La condena se basó exclusivamente en la aceptación de cargos del imputado (conclusión anticipada), lo que, conforme al Acuerdo Plenario N° 05-2008/CJ-116, sustituye la actividad probatoria. En estos casos, la evidencia digital sirvió como base fáctica de la acusación fiscal, pero el órgano jurisdiccional no realizó un análisis de autenticidad, integridad o cadena de custodia.

c) En la sentencia condenatoria con juicio oral (Exp. 01342-2022):

Este caso es particularmente relevante porque, a pesar de haberse desarrollado un debate probatorio pleno (sin conformidad), el tratamiento de la evidencia digital fue idéntico al de la sentencia absolutoria: valoración implícita como prueba documental tradicional, ausencia de peritaje informático y nula aplicación de criterios técnicos. La

condena se sustentó en prueba indiciaria (retiros realizados con tarjeta y clave personalísima, falta de denuncia de robo por parte de la imputada) y no en un análisis técnico de la manipulación del sistema informático del BBVA.

Hallazgo central:

La Tabla 2 evidencia una paradoja estructural: cuando hay conformidad, no se valora técnicamente la evidencia digital porque la aceptación de cargos la vuelve innecesaria; cuando hay juicio oral contradictorio, tampoco se valora técnicamente, porque los jueces la tratan como documental tradicional. En ambos escenarios, el resultado es el mismo: ausencia de aplicación de estándares técnico-forenses (autenticidad, integridad, cadena de custodia, peritaje informático).

Este hallazgo sugiere que el problema no es coyuntural ni atribuible a un juez o caso específico, sino estructural en la práctica judicial del distrito de Huamanga para el delito de fraude informático.

Tabla 3 Criterios técnicos evaluados

Criterio técnico	**Sentencia 1 (Absolutoria)**	**Sentencia 2 (Conformada)**	**Sentencia 3 (Conformada)**	**Sentencia 4 (Juicio oral)**	**Sentencia 5 (Conformada)**	**Total aplicado**
Autenticidad	No menciona	No menciona	No menciona	No menciona	No menciona	0/5
Integridad	No menciona	No menciona	No menciona	No menciona	No menciona	0/5
Cadena de custodia	No menciona	No menciona	No menciona	No menciona	No menciona	0/5
Licitud	Sobreentendido	No menciona	No menciona	No menciona	No menciona	0/5
Fiabilidad técnica	No menciona	No menciona	No menciona	No menciona	No menciona	0/5
Peritaje informático forense	Testimonio genérico	No	No	No	No	0/5

La Tabla 3 muestra un resultado contundente y uniforme en toda la muestra: ninguno de los cinco criterios técnicos evaluados fue aplicado de manera efectiva en ninguna de las sentencias.

a) Ausencia absoluta de criterios básicos:

Los criterios de autenticidad, integridad, cadena de custodia y fiabilidad técnica no fueron mencionados ni una sola vez en el total de las cinco sentencias. Esto implica que los jueces no verificaron: (i) si los registros bancarios incorporados eran auténticos y no habían sido alterados (autenticidad e integridad); (ii) cómo se aseguró la evidencia desde su obtención hasta su incorporación al juicio (cadena de custodia); ni (iii) si los sistemas informáticos del banco emisor eran fiables o presentaban vulnerabilidades (fiabilidad técnica).

b) El caso de la licitud:

Solo en la sentencia absolutoria (Exp. 00724-2020) se sobreentendió la licitud de la evidencia por su origen bancario, pero no hubo un análisis explícito. En las cuatro sentencias restantes, el criterio de licitud ni siquiera fue mencionado. Ninguna sentencia cuestionó o verificó activamente que la obtención de la evidencia digital se hubiera realizado conforme a la ley.

c) El peritaje informático forense: la deficiencia más grave:

Cinco de cinco sentencias carecieron de un peritaje informático forense propiamente dicho. La sentencia absolutoria (Exp. 00724-2020) incorporó un testimonio pericial, pero este fue genérico: el perito explicó la modalidad delictiva del spoofing en abstracto, sin realizar un análisis forense del equipo del agraviado, de los logs del banco o de la página web clonada. En las cuatro sentencias restantes, directamente no se solicitó ni actuó peritaje informático alguno.

d) Un hallazgo revelador: la uniformidad de la deficiencia

Más allá del sentido del fallo (absolución o condena) o de la etapa procesal (juicio oral o conclusión anticipada), el resultado es idéntico en todos los casos: 0/5 criterios técnicos aplicados. Esto descarta que la deficiencia sea atribuible a un juez específico o a las particularidades de un caso concreto.

Interpretación sistémica:

La Tabla 3 evidencia lo que puede calificarse como una carencia estructural en la cultura judicial del distrito de Huamanga respecto a la prueba digital. Los jueces no están aplicando, ni siquiera mencionando, los estándares mínimos que la comunidad técnico-forense internacional considera indispensables para validar evidencia digital (autenticidad, integridad, cadena de custodia, peritaje).

Esta ausencia tiene dos consecuencias igualmente problemáticas:

En sentencias absolutorias (como la Exp. 00724-2020): se absuelve por duda razonable, pero no porque se haya aplicado un análisis técnico riguroso que revele la insuficiencia probatoria, sino porque directamente no se solicitó la prueba técnica necesaria (cámaras de seguridad, peritaje informático).

En sentencias condenatorias (como la Exp. 01342-2022): se condena sin verificar técnicamente que la evidencia digital sea auténtica, íntegra y fiable, lo que genera un riesgo de condenas basadas en prueba no validada técnicamente.

Conexión con la literatura:

Este hallazgo contrasta frontalmente con los estándares propuestos por la doctrina especializada. Autores como Mason (2016) señalan que la evidencia digital no puede ser tratada como prueba documental tradicional, pues su carácter maleable y su facilidad de alteración exigen controles específicos (hash, cadena de custodia, peritaje independiente). Asimismo, la Convención de Budapest (artículo 14) y la Ley N° 30096 exigen, implícitamente, la incorporación de prueba pericial especializada para acreditar la manipulación del sistema informático, extremo que no se cumple en ninguno de los casos analizados.

Tabla 4 Comparación de decisiones penal y civil

Expediente	Decisión penal	Pena	Decisión civil	Monto reparación civil	Observación clave
00724-2020	Absolución	No aplica	Condena	S/ 4,820	Paradoja: absuelve penal, condena civil

00477-2023	Condena (conformada)	2a 6m 27d (suspendida)	Condena	S/ 30,600 (incluye restitución)	Pago condicionado a suspensión
01263-2019	Condena (conformada)	2a 7m (suspendida)	Condena	S/ 1,895	Pago en cuotas
01342-2022	Condena (juicio oral)	4 años (suspendida)	Condena	S/ 3,000 + restitución S/ 9,017	Ordena transferencia bancaria directa
02815-2019	Condena (conformada)	3 años (suspendida)	Condena	S/ 1,810 (incluye restitución)	8 cuotas

La Tabla 4 revela una tendencia uniforme en la dimensión civil: todas las sentencias, independientemente del sentido del fallo penal, imponen una condena civil. Esto confirma que, en la práctica judicial de Huamanga, la acción civil es sistemáticamente estimada cuando se acredita la transferencia patrimonial, con independencia de que se haya logrado probar la responsabilidad penal del acusado más allá de toda duda razonable.

El caso más relevante es el Expediente 00724-2020, que constituye una paradoja jurídica: la jueza absuelve penalmente por duda razonable (no se acreditó la participación de la acusada en la manipulación informática), pero condena civilmente a pagar S/ 4,820.00. Esta decisión se sustenta en la teoría de la responsabilidad civil extracontractual autónoma (artículos 1969 y 1970 del Código Civil), según la cual el hecho dañoso acreditado —la recepción del dinero en la cuenta de la acusada y su no devolución— genera obligación de reparar, incluso si no se configura el tipo penal. Este criterio, si bien jurídicamente sólido, plantea una tensión con el principio de presunción de inocencia.

En las sentencias condenatorias, se observa un patrón recurrente: todas imponen penas privativas de libertad suspendidas, condicionadas al pago de la reparación civil en cuotas. La Sentencia 4 (Exp. 01342-2022) destaca por incorporar una medida innovadora: ordena al BBVA transferir directamente los S/ 9,017.35 retenidos en la cuenta de la condenada a la agraviada, lo que evidencia un intento de hacer efectiva la restitución sin depender de la voluntad de pago del sentenciado. Este mecanismo podría constituir una buena práctica replicable, aunque no suple la ausencia de valoración técnica de la evidencia digital.

Tabla 5 Deficiencias técnicas identificadas

N°	Deficiencia técnica	Sentencia 1	Sentencia 2	Sentencia 3	Sentencia 4	Sentencia 5	Frecuencia
1	No se solicitaron cámaras de seguridad de cajeros	Deficiencia presente	No aplica al caso concreto	No aplica al caso concreto	No aplica al caso concreto	No aplica al caso concreto	1/5
2	No se realizó peritaje informático forense	(testimonio genérico)	Deficiencia presente	Deficiencia presente	Deficiencia presente	Deficiencia presente	4/5 + 1 parcial
3	No se aplicaron criterios de autenticidad/integridad	Deficiencia presente	Deficiencia presente	Deficiencia presente	Deficiencia presente	Deficiencia presente	**5/5**
4	No se menciona cadena de custodia	Deficiencia presente	Deficiencia presente	Deficiencia presente	Deficiencia presente	Deficiencia presente	**5/5**
5	No se determinó ubicación geográfica de retiros	Deficiencia presente	No aplica al caso concreto	No aplica al caso concreto	No aplica al caso concreto	No aplica al caso concreto	1/5
6	Evidencia digital tratada como documental tradicional	Deficiencia presente	Deficiencia presente	Deficiencia presente	Deficiencia presente	Deficiencia presente	**5/5**

La Tabla 5 sistematiza las deficiencias técnicas recurrentes en la valoración de evidencia digital. Se identifican tres deficiencias con una frecuencia del 100% (5/5): la no aplicación de criterios de autenticidad e integridad, la ausencia total de mención a la cadena de custodia, y el tratamiento de la evidencia digital como si fuera prueba documental tradicional. Estas tres deficiencias constituyen el núcleo duro del problema estructural detectado en la práctica judicial de Huamanga, pues están presentes en absolutamente todos los casos analizados, sin excepción.

Una segunda deficiencia igualmente grave es la ausencia de peritaje informático forense, que alcanza una frecuencia de 4/5 (más un caso con testimonio genérico que no constituye peritaje forense propiamente dicho). En cuatro sentencias directamente no se realizó ningún peritaje; en la sentencia absolutoria (Exp. 00724-2020) se incorporó un testimonio pericial, pero este se limitó a explicar en abstracto la modalidad del spoofing, sin realizar un análisis forense concreto del caso. Esta carencia es particularmente

relevante porque el delito de fraude informático exige probar la "manipulación del sistema informático", extremo que difícilmente puede acreditarse sin prueba pericial especializada.

Las deficiencias restantes (no solicitar cámaras de seguridad y no determinar ubicación geográfica de retiros) solo fueron relevantes en la sentencia absolutoria, donde la jueza criticó expresamente a la Fiscalía por no haber recabado dichas pruebas. Sin embargo, incluso en los casos donde estas deficiencias no aplicaban, las tres deficiencias estructurales (autenticidad, cadena de custodia, tratamiento documental) se mantuvieron invariables. Esto confirma que el problema no es de estrategia fiscal en un caso concreto, sino de ausencia de cultura forense digital en todo el distrito judicial

Cuadro 2 Deficiencias técnicas identificadas

Deficiencia técnica	**Frecuencia (n)**	**Porcentaje (%)**
No se aplicaron criterios de autenticidad/integridad	5	100%
No se menciona cadena de custodia	5	100%
Evidencia digital tratada como documental tradicional	5	100%
No se realizó peritaje informático forense	4	80%
No se solicitaron cámaras de seguridad de cajeros	1	20%
No se determinó ubicación geográfica de retiros	1	20%

Figura 2 Deficiencias técnicas identificadas

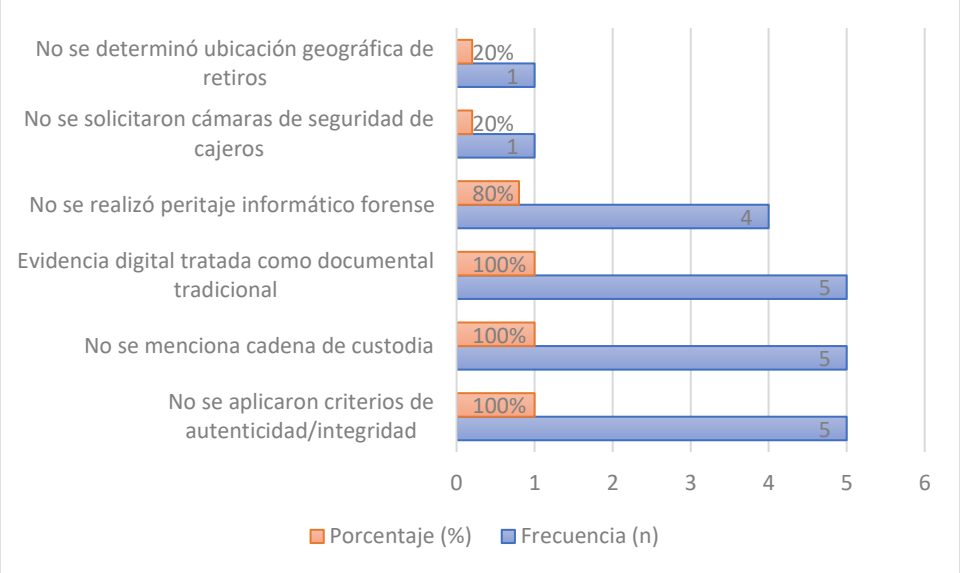


Tabla 6 Hallazgos agregados

Hallazgo	**Evidencia en las sentencias**	**Frecuencia**
No existe valoración técnico-forense de evidencia digital en fraude informático en los juzgados de Huamanga	Todas las sentencias (0/5 aplican criterios técnicos)	**5/5 (100%)**
La evidencia digital se trata como prueba documental tradicional	Sentencias 1, 2, 3, 4, 5	**5/5 (100%)**
En sentencias conformadas (conclusión anticipada), no hay valoración probatoria de evidencia digital	Sentencias 2, 3, 5 (3 casos)	**3/5 (60% de la muestra)**
No se realiza peritaje informático forense (solo testimonio genérico en un caso)	Sentencias 1 (parcial), 2, 3, 4, 5	**4/5 sin peritaje + 1 con testimonio genérico**
La cadena de custodia nunca se menciona	Sentencias 1, 2, 3, 4, 5	**5/5 (100%)**
Es posible condenar civilmente a pesar de absolución penal (responsabilidad civil extracontractual autónoma)	Sentencia 1	**1 caso paradigmático**

La Tabla 6 sintetiza los hallazgos transversales que emergen del análisis de las cinco sentencias, permitiendo identificar patrones estructurales más allá de los casos particulares. El hallazgo más contundente es que, en el 100% de la muestra (5/5), no existe valoración técnico-forense de la evidencia digital y la cadena de custodia nunca es mencionada. Esto revela que la deficiencia no es excepcional ni atribuible a la actuación de un juez específico, sino que constituye una práctica judicial arraigada en el distrito de Huamanga para el delito de fraude informático.

Un segundo hallazgo relevante es que el 60% de los casos (3/5) se resolvieron mediante conclusión anticipada (conformidad). En estos supuestos, el Acuerdo Plenario

N° 05-2008/CJ-116 permite sustituir la actividad probatoria por la aceptación de cargos del imputado, lo que implica que el juez no realiza —y no está obligado a realizar— valoración técnica alguna de la evidencia digital. Este dato es significativo porque sugiere que la mayoría de los procesos por fraude informático no llegan a un juicio oral contradictorio, perdiéndose así la oportunidad de que los órganos jurisdiccionales desarrollen estándares probatorios especializados.

El tercer hallazgo, de naturaleza cualitativamente distinta, es la posibilidad de condenar civilmente a pesar de la absolución penal, evidenciada en el Expediente 00724-2020. Este caso constituye un precedente relevante porque demuestra la autonomía de la responsabilidad civil extracontractual (artículos 1969 y 1970 del Código Civil) frente a la responsabilidad penal. La jueza absolvió por duda razonable respecto a la participación de la acusada en la manipulación informática, pero la condenó civilmente por haberse beneficiado patrimonialmente de la transferencia no consentida. Esta decisión, aunque jurídicamente sólida, plantea una tensión con el principio de presunción de inocencia y merece un análisis más detallado en la discusión de la tesis.

Tabla 7 Clasificación final de las sentencias según calidad de valoración

Categoría	**Expediente**	**Tipo de valoración probatoria**	**Nivel de desarrollo de criterios técnicos**	**Tratamiento de la evidencia digital**
Deficiente (con debate)	00724-2020	Parcial	Bajo	Como prueba documental tradicional
Deficiente (con debate)	01342-2022	Parcial	Bajo	Como prueba documental tradicional
No aplica (conformidad)	00477-2023	Deficiente (no hay valoración)	Bajo (nulo)	Como prueba documental tradicional
No aplica (conformidad)	01263-2019	Deficiente (no hay valoración)	Bajo (nulo)	Como prueba documental tradicional
No aplica (conformidad)	02815-2019	Deficiente (no hay valoración)	Bajo (nulo)	Como prueba documental tradicional

La Tabla 7 presenta la clasificación final de las cinco sentencias a partir de los criterios analizados en las tablas precedentes. Se distinguen dos categorías claramente

diferenciadas: (i) sentencias deficientes con debate probatorio (2 casos) y (ii) sentencias donde la valoración no aplica por conformidad (3 casos). Esta distinción es fundamental porque, aunque el resultado práctico sea el mismo —ausencia de valoración técnico-forense—, las razones jurídicas son radicalmente distintas.

En la primera categoría (Expedientes 00724-2020 y 01342-2022), nos encontramos ante juicios orales contradictorios donde existió debate probatorio, la imputada no aceptó los cargos y, sin embargo, la valoración de la evidencia digital fue solo parcial y deficiente. En ambos casos, el nivel de desarrollo de criterios técnicos fue calificado como "bajo" y la evidencia digital fue tratada como prueba documental tradicional. Lo preocupante de esta categoría es que, a pesar de tener la oportunidad procesal para aplicar estándares técnicos (autenticidad, integridad, cadena de custodia, peritaje), los jueces no lo hicieron. La sentencia absolutoria (00724-2020) refleja una valoración que, aunque jurídicamente motivada, adolece de sustento técnico; la sentencia condenatoria (01342-2022) refleja una condena basada en prueba indiciaria e inferencias lógicas, no en análisis forense digital.

En la segunda categoría (Expedientes 00477-2023, 01263-2019 y 02815-2019), nos encontramos ante sentencias conformadas por conclusión anticipada. Aquí, la ausencia de valoración técnica no es propiamente una "deficiencia" en el sentido de mala práctica judicial, sino una consecuencia directa del mecanismo procesal elegido: la imputada renuncia a su derecho a la prueba y al juicio público, y el juez dicta sentencia condenatoria con base en la aceptación de cargos, sin necesidad de valorar prueba alguna. Sin embargo, desde la perspectiva de la presente investigación, esta categoría revela un dato igualmente relevante: el 60% de los casos de fraude informático se resuelven por conformidad, lo que implica que no se genera jurisprudencia ni estándares técnicos sobre cómo debe valorarse la evidencia digital en esta materia.

Finalmente, la Tabla 7 confirma un hallazgo uniforme en toda la muestra: independientemente de la categoría, el tratamiento de la evidencia digital es siempre "como prueba documental tradicional". Ni siquiera en los dos casos con debate probatorio los jueces concibieron la evidencia digital como una categoría probatoria autónoma que exige criterios técnicos específicos. Este es, probablemente, el hallazgo más relevante de la investigación y aquel que mayores implicancias tiene para la propuesta de mejora que se desarrollará en el capítulo de discusión.

5.2. Resultados de las entrevistas

Se realizaron seis entrevistas semiestructuradas a operadores de justicia del distrito judicial de Huamanga: tres jueces penales unipersonales y tres fiscales penales. Las entrevistas fueron transcritas y analizadas mediante la técnica de análisis temático de contenido, identificándose categorías recurrentes en el discurso de los entrevistados.

Para garantizar el anonimato, se asignaron códigos a cada entrevistado: J01, J02 y J03 para los jueces; F01, F02 y F03 para los fiscales.

Tabla 8 Perfil de los entrevistados

Código	Cargo	Años de experiencia	Especialidad
J01	Juez Penal Unipersonal	10 años	Derecho Penal
J02	Juez Penal Unipersonal	6 años	Derecho Penal
J03	Juez Penal Unipersonal	14 años	Derecho Penal
F01	Fiscal	9 años	Derecho Penal
F02	Fiscal	4 años	Derecho Penal
F03	Fiscal	15 años	Derecho Penal

Fuente: Elaboración propia a partir de entrevistas realizadas.

Tabla 9 Posturas de los jueces entrevistados

Criterio	Postura de los jueces
Aplicación de cadena de custodia	Ninguno de los jueces aplica cadena de custodia a los reportes bancarios. J01 señala: *"La cadena de custodia la asumimos como válida si viene del banco"*. J02 indica: *"Reviso los elementos formales: sello, firma, membrete"*. J03 reconoce: *"Es una debilidad estructural"*.
Verificación de autenticidad e integridad	Los jueces no realizan verificación técnica mediante hash ni solicitan archivos digitales originales. J01 manifiesta: *"Nunca he pedido un hash ni algo similar"*. J02 añade: *"Si el documento tiene membrete del banco, lo tomo como auténtico"*. J03 admite: *"No puedo estar seguro de que no haya sido manipulado"*.

Formación en evidencia digital	Los tres jueces coinciden en que su formación es insuficiente. J01 manifiesta: *"En la academia llevamos un curso básico, pero nada sobre evidencia digital forense"*. J02 señala: *"La formación fue teórica, no práctica"*. J03 afirma: *"Cuando estudié Derecho, los delitos informáticos no existían"*.
Dificultades para valorar prueba digital	Los jueces enfrentan dificultades con informes periciales complejos y ausencia de peritos en audiencia. J01 señala: *"Los peritos explican en audiencia como a un niño"*. J02 indica: *"Sin un perito que me explique, es muy complicado"*. J03 añade: *"Revisar un peritaje de 50 páginas lleva horas o días"*.
Rechazo de evidencia digital	Solo J01 y J03 han restado valor probatorio a evidencia digital. J01 rechazó capturas de WhatsApp sin certificación. J03 restó valor a capturas de pantalla de una página web falsa sin cadena de custodia. J02 señala no haber rechazado evidencia digital en casos de fraude informático.
Hallazgo general	Existe consenso entre los jueces en cuanto a la **ausencia de verificación técnica** y el **déficit formativo** en materia de evidencia digital. Sin embargo, se identifican matices: J01 y J02 adoptan una postura pragmática (conformidad con los requisitos formales), mientras que J03 muestra una posición más crítica, calificando la situación como una *"debilidad estructural"*.

Fuente: Elaboración propia a partir de entrevistas realizadas.

La Tabla 9 sintetiza las posturas de los tres jueces entrevistados en torno a cinco criterios fundamentales para la valoración de la evidencia digital en casos de fraude informático. Del análisis de sus respuestas emergen dos grandes hallazgos: la ausencia generalizada de verificación técnica y el déficit formativo común, aunque con matices diferenciados entre los entrevistados.

a) La ausencia de verificación técnica como práctica generalizada

En cuanto a la aplicación de cadena de custodia, los tres jueces coinciden en que no aplican este criterio a los reportes bancarios. Sin embargo, sus justificaciones revelan distintos niveles de conciencia sobre el problema. J01 y J02 adoptan una postura pragmática: el primero confía ciegamente en el origen bancario ("la asumimos como válida si viene del banco"), mientras que el segundo se limita a verificar requisitos

formales como sello, firma y membrete. J03, en cambio, muestra una mayor reflexividad crítica al calificar esta práctica como una "debilidad estructural", reconociendo implícitamente que la mera confianza institucional no sustituye la cadena de custodia técnicamente exigible.

En materia de verificación de autenticidad e integridad, el patrón se repite. Ninguno de los jueces realiza verificación técnica mediante hash ni solicita los archivos digitales originales. J01 es explícito: "Nunca he pedido un hash ni algo similar". J02 basa su decisión en la apariencia formal del documento ("lo tomo como auténtico"). J03, nuevamente el más crítico, admite su limitación: "No puedo estar seguro de que no haya sido manipulado". Esta última declaración es particularmente relevante porque evidencia que, incluso el juez con mayor conciencia del problema, carece de las herramientas o los conocimientos para resolverlo.

b) El déficit formativo como denominador común

Los tres jueces coinciden en que su formación en evidencia digital es insuficiente, aunque sus testimonios reflejan distintas generaciones y trayectorias formativas. J01, con diez años de experiencia, señala que la Academia de la Magistratura ofrece solo un "curso básico" sin contenido forense. J02, con seis años de experiencia, distingue entre la formación teórica recibida (sobre el tipo penal) y la formación práctica que le falta (cómo leer un peritaje, qué preguntar a un perito). J03, el de mayor experiencia (catorce años), contextualiza el problema generacionalmente: "Cuando estudié Derecho, los delitos informáticos no existían".

Este hallazgo es consistente con lo manifestado por los fiscales en la Tabla 10, quienes perciben que los jueces no cuestionan técnicamente los peritajes porque carecen de la formación para hacerlo.

c) Las dificultades prácticas en la valoración probatoria

En cuanto a las dificultades para valorar la prueba digital, los jueces coinciden en señalar dos problemas principales: la complejidad de los informes periciales y la ausencia de peritos en audiencia. J01 revela que los peritos deben explicar "como a un niño", lo que sugiere que el nivel técnico de los informes supera la capacidad de comprensión del juzgador. J02 confiesa que sin un perito que explique, el análisis se vuelve "muy

complicado". J03 añade una dimensión procesal: el tiempo. Revisar un peritaje extenso es incompatible con la carga laboral que enfrentan los jueces de Huamanga.

Estas dificultades prácticas explican, al menos parcialmente, por qué los jueces optan por vías más simples: confiar en el reporte bancario sin verificación técnica adicional.

d) El rechazo de evidencia digital: la excepción que confirma la regla

Solo dos jueces (J01 y J03) reportan haber rechazado o restado valor probatorio a evidencia digital, y en ambos casos se trató de capturas de pantalla (de WhatsApp o de una página web falsa), no de reportes bancarios. J02, en cambio, señala no haber rechazado nunca evidencia digital en casos de fraude informático.

Este hallazgo es revelador porque demuestra que los jueces sí son capaces de aplicar criterios de autenticidad y cadena de custodia cuando la evidencia proviene de fuentes no institucionales (como un particular que presenta capturas de pantalla). Sin embargo, no aplican esos mismos criterios cuando la evidencia proviene de una entidad bancaria. Existe, por tanto, una confianza institucional diferenciada: el banco merefe confianza automática; el ciudadano particular, no.

J03, en particular, muestra coherencia en su postura crítica: así como calificó la falta de cadena de custodia como una "debilidad estructural", también restó valor probatorio a capturas de pantalla que carecían de dicha cadena.

Tabla 10 Percepción de los fiscales entrevistados

Criterio	Postura de los fiscales
Aplicación de cadena de custodia	Los fiscales no aplican cadena de custodia a los reportes bancarios. F01 señala: *"No aplicamos una cadena de custodia formal a la evidencia digital en la mayoría de casos"*. F02 indica: *"La verdad es que no soy tan estricto con la cadena de custodia"*. F03 reconoce: *"La cadena de custodia es prácticamente inexistente"*. Solo en casos con dispositivos incautados (celulares, laptops) los fiscales levantan acta de incautación y cadena de custodia.

Limitaciones materiales en Huamanga	Los tres fiscales coinciden en la falta de laboratorio forense informático en Huamanga. F01 señala: *"No tenemos laboratorio forense informático en Huamanga. Para un peritaje serio, tenemos que derivar a Lima"*. F02 indica: *"Falta personal especializado"*. F03 afirma: *"Un peritaje puede tardar seis meses o más. Eso es inaceptable"*.
Relación con los jueces	Los fiscales perciben que los jueces no cuestionan técnicamente los peritajes. F01 manifiesta: *"Nunca he visto que un juez pida el hash de un archivo"*. F02 indica: *"Nunca me han cuestionado la cadena de custodia ni la metodología usada"*. F03 señala: *"Los aceptan sin reparos, no entran en detalles técnicos"*.
Brecha discurso-práctica	Los tres fiscales coinciden en que existe diferencia entre el discurso y la práctica judicial. F01 afirma: *"En las sentencias escriben páginas sobre sana crítica, pero en la práctica miran si el nombre del acusado aparece en el reporte bancario"*. F02 indica: *"Escriben bonito para protegerse"*. F03 concluye: *"Discurso vacío, hacen lo mínimo indispensable"*.
Conclusión anticipada	Los fiscales prefieren la conformidad para evitar el debate probatorio técnico. F02 señala: *"Prefiero la conclusión anticipada, evita todo el problema del peritaje"*. F01 reconoce: *"La mayoría de casos los resolvemos por conclusión anticipada"*. F03, aunque más crítico, entiende la práctica: *"No es porque no queramos investigar bien. Es porque no podemos"*.
Hallazgo general	Los fiscales coinciden en que las **limitaciones materiales** (falta de laboratorio forense, demoras en peritajes) y la **falta de cuestionamiento técnico por parte de los jueces** incentivan la conclusión anticipada como vía de escape. Adicionalmente, todos perciben una **brecha significativa** entre el discurso sofisticado de las sentencias y la práctica judicial real.

Fuente: Elaboración propia a partir de entrevistas.

La Tabla 10 sintetiza las percepciones de los tres fiscales entrevistados en torno a cinco criterios fundamentales: aplicación de cadena de custodia, limitaciones materiales en Huamanga, relación con los jueces, brecha discurso-práctica y conclusión anticipada. Del análisis de sus respuestas emergen dos grandes hallazgos: las limitaciones estructurales del sistema y la percepción crítica sobre la actuación judicial.

a) La cadena de custodia: inexistente para reportes bancarios, presente para dispositivos

Al igual que los jueces, los fiscales coinciden en que no aplican cadena de custodia a los reportes bancarios. F01 es explícito: "No aplicamos una cadena de custodia formal a la evidencia digital en la mayoría de casos". F02 admite una postura laxa: "La verdad es que no soy tan estricto con la cadena de custodia". F03, con mayor experiencia, califica la situación como "prácticamente inexistente".

Sin embargo, se identifica una diferencia relevante respecto de los jueces: los fiscales sí aplican cadena de custodia cuando se trata de dispositivos incautados (celulares, laptops). Esta distinción revela que los fiscales conocen el procedimiento y lo aplican cuando la evidencia lo requiere, pero no lo extienden a los reportes bancarios por considerar que no es necesario o por falta de protocolos específicos. Esta diferenciación, aunque comprensible desde una perspectiva práctica, es jurídicamente problemática, pues la evidencia digital bancaria es tan susceptible de alteración como cualquier otro archivo digital.

b) Las limitaciones materiales: un problema estructural no resuelto

Los tres fiscales coinciden en señalar la falta de laboratorio forense informático en Huamanga como la principal limitación material. F01 describe el procedimiento: "Para un peritaje serio, tenemos que derivar a Lima". F02 añade la dimensión de personal: "Falta personal especializado". F03 cuantifica el impacto temporal: "Un peritaje puede tardar seis meses o más. Eso es inaceptable".

Este hallazgo es particularmente relevante porque evidencia que el problema no es solo formativo (como en el caso de los jueces), sino también infraestructural. La ausencia de un laboratorio forense en Huamanga no es una deficiencia menor; es una carencia estructural que afecta la calidad de la investigación fiscal y que, como se verá más adelante, incentiva la conclusión anticipada.

La declaración de F03 es especialmente elocuente: "El proceso se enquista, el agraviado se cansa, el imputado a veces fuga". Esta descripción del impacto procesal de las demoras revela cómo una limitación material termina afectando derechos fundamentales (plazo razonable, tutela judicial efectiva).

c) La relación con los jueces: aceptación acrítica de los peritajes

Los tres fiscales coinciden en que los jueces no cuestionan técnicamente los peritajes que ellos presentan. F01 señala: "Nunca he visto que un juez pida el hash de un

archivo". F02 añade: "Nunca me han cuestionado la cadena de custodia ni la metodología usada". F03 resume: "Los aceptan sin reparos, no entran en detalles técnicos".

Este hallazgo es consistente con lo manifestado por los propios jueces en la Tabla 9, donde reconocieron no tener la formación necesaria para realizar dichos cuestionamientos. Se configura así un círculo virtuoso a la inversa: los fiscales no aplican criterios técnicos rigurosos porque saben que los jueces no los exigirán; los jueces no los exigen porque no tienen la formación para hacerlo. Esta mutua complacencia, funcional desde una perspectiva de celeridad procesal, es profundamente problemática desde una perspectiva de garantías y rigor probatorio.

d) La brecha discurso-práctica: el "discurso vacío" de las sentencias

Los tres fiscales coinciden en señalar la existencia de una brecha significativa entre lo que los jueces declaran en sus sentencias (sana crítica, valoración conjunta, estándares probatorios) y lo que realmente hacen en la práctica.

F01 describe esta brecha con precisión: "En las sentencias escriben páginas sobre sana crítica, pero en la práctica miran si el nombre del acusado aparece en el reporte bancario". Esta afirmación sugiere que la valoración judicial, en los hechos, se reduce a una operación binaria: ¿el nombre está? → condena; ¿el nombre no está o hay duda? → absolución. No hay, según los fiscales, un análisis técnico intermedio.

F02 introduce un matiz relevante al señalar que los jueces "escriben bonito para protegerse". Esta expresión sugiere que el discurso sofisticado de las sentencias no es tanto una expresión de la práctica real del juzgador, sino una estrategia de blindaje para evitar que la sentencia sea anulada en apelación. La cita a autores extranjeros (Taruffo, Ferrer Beltrán) y la invocación de estándares probatorios funcionarían, desde esta perspectiva, como un revestimiento retórico que no se corresponde con el razonamiento probatorio real.

F03 es el más crítico: "Discurso vacío, hacen lo mínimo indispensable". Esta declaración, proveniente del fiscal con mayor experiencia (15 años), sugiere que la brecha no es un fenómeno aislado ni atribuible a jueces inexpertos, sino una práctica institucional arraigada en el distrito judicial de Huamanga.

e) La conclusión anticipada: la vía de escape estructural

Los fiscales reconocen que, ante las limitaciones materiales y la falta de cuestionamiento técnico por parte de los jueces, la conclusión anticipada (conformidad) se ha convertido en la vía preferida para resolver casos de fraude informático.

F02 es el más explícito: "Prefiero la conclusión anticipada, evita todo el problema del peritaje". Esta declaración revela que la conformidad no es solo una opción procesal entre otras, sino una estrategia deliberada para evitar los costos (en tiempo, recursos y complejidad) de un juicio oral con debate probatorio pleno.

F01 confirma que esta práctica es mayoritaria: "La mayoría de casos los resolvemos por conclusión anticipada". Este dato, que en una investigación cuantitativa se expresaría como un porcentaje, adquiere aquí un significado cualitativo: la conformidad no es la excepción, sino la regla en la persecución penal del fraude informático en Huamanga.

F03, aunque más crítico y con mayor experiencia, comprende la práctica: "No es porque no queramos investigar bien. Es porque no podemos". Esta declaración es clave porque exculpa a los fiscales individuales y señala al sistema como responsable. La conclusión anticipada no sería, desde esta perspectiva, una manifestación de mala praxis, sino una respuesta racional a un contexto de limitaciones estructurales.

Tabla 11 Categorías de análisis identificadas

Categoría	**Descripción**	**Entrevistados que la mencionan**
Confianza institucional	La confianza en el banco como entidad emisora reemplaza la verificación técnica de autenticidad e integridad. Los operadores asumen que los reportes bancarios son auténticos por su origen, sin aplicar controles como hash o cadena de custodia.	J01, J02, J03, F01, F02, F03
Déficit formativo	Los jueces reconocen que su formación en evidencia digital forense es insuficiente. La Academia de la Magistratura ofrece cursos básicos de informática, pero no capacitación específica sobre valoración técnica de prueba digital.	J01, J02, J03
Limitaciones materiales	Ausencia de laboratorio forense informático en Huamanga, falta de peritos especializados, demoras de meses en peritajes derivados a Lima, y carencia	F01, F02, F03

	de equipos forenses (write blockers, software especializado).	
Conclusión anticipada	La conformidad se ha convertido en la vía preferida para resolver casos de fraude informático, permitiendo evitar el debate probatorio técnico, las demoras de los peritajes y el riesgo de absolución.	F01, F02, J02
Brecha discurso-práctica	Existe una diferencia significativa entre el discurso sofisticado de las sentencias (que citan estándares probatorios y autores especializados) y la práctica judicial real (que se limita a verificar la presencia del nombre del acusado en el reporte bancario).	F01, F02, F03

Fuente: Elaboración propia a partir de entrevistas.

La Tabla 11 sistematiza las cinco categorías emergentes del análisis de las seis entrevistas realizadas a jueces y fiscales del distrito judicial de Huamanga. Estas categorías no son mutuamente excluyentes, sino que se articulan entre sí configurando un sistema de prácticas y creencias que explica por qué la evidencia digital en casos de fraude informático no recibe un tratamiento técnicamente adecuado. A continuación, se analiza críticamente cada categoría, sus interrelaciones y sus implicancias para la administración de justicia.

Primera categoría: confianza institucional.

Los seis entrevistados coinciden en que la confianza en el banco como entidad emisora reemplaza cualquier verificación técnica de autenticidad o integridad. Los reportes bancarios se aceptan como válidos por su origen, sin aplicar controles como hash, cadena de custodia o verificación del archivo digital original. Esta categoría revela una presunción de veracidad de la prueba bancaria que no tiene correlato en la regulación de la prueba digital. Desde una perspectiva técnico-forense, un reporte bancario impreso es tan susceptible de alteración como una captura de pantalla de WhatsApp. Sin embargo, los operadores de justicia tratan a ambos de manera diametralmente opuesta: la captura de WhatsApp es recibida con escepticismo y frecuentemente rechazada si no cumple estándares formales, mientras que el reporte bancario es aceptado sin cuestionamiento. Esta diferencia de trato revela un sesgo institucional que no se justifica en la naturaleza de la prueba digital, sino en la confianza socialmente construida en las entidades

bancarias. El banco es percibido como una institución confiable, mientras que el ciudadano particular es percibido como potencialmente manipulador. Este sesgo, aunque comprensible sociológicamente, es problemático desde una perspectiva epistemológica porque la confianza no sustituye la verificación. Las consecuencias prácticas de esta categoría son múltiples: se elude la aplicación de criterios técnicos mínimos, se genera un trato desigual entre tipos de evidencia digital y se vulnera el principio de igualdad de armas procesales.

Segunda categoría: déficit formativo.

Los tres jueces entrevistados reconocen que su formación en evidencia digital forense es insuficiente. La Academia de la Magistratura ofrece cursos básicos de informática, pero no capacitación específica sobre valoración técnica de prueba digital. Esta categoría revela una brecha generacional y curricular en la formación de los jueces peruanos. El juez de mayor experiencia, con catorce años en el cargo, señala que cuando estudió Derecho los delitos informáticos no existían en el Código Penal. El juez con diez años de experiencia señala que la formación recibida fue un curso básico sin contenido forense. Incluso el juez de menor experiencia, con seis años y quien ha llevado un diplomado en delitos informáticos, califica su formación como teórica, no práctica. El problema no es solo que los jueces no sepan aplicar criterios técnicos; es que saben que no saben, pero no tienen incentivos suficientes para aprender. La carga procesal, la ausencia de capacitación obligatoria y la falta de consecuencias por una valoración probatoria deficiente perpetúan este déficit. Como resultado, los jueces dependen excesivamente de lo que digan los peritos en audiencia, no pueden cuestionar técnicamente los informes periciales y se genera una delegación acrítica de la función valoradora en los peritos.

Tercera categoría: limitaciones materiales.

Los tres fiscales entrevistados coinciden en señalar la ausencia de laboratorio forense informático en Huamanga como la principal limitación material. A ello se suman la falta de peritos especializados, las demoras de meses en los peritajes derivados a Lima y la carencia de equipos forenses básicos como write blockers o software especializado. Esta categoría revela que el problema no es solo formativo, como en el caso de los jueces, sino también infraestructural. La ausencia de un laboratorio forense en Huamanga no es

una deficiencia menor; es una carencia estructural que hace técnicamente inviable una investigación forense rigurosa en el distrito. La derivación de pericias a Lima genera demoras de seis meses o más, tiempo durante el cual el proceso se paraliza, el agraviado se desgasta y el imputado, si está en libertad, puede eludir la acción de la justicia. En este contexto, la conclusión anticipada aparece no como una opción entre otras, sino como la única opción racional para quienes buscan una condena en un plazo razonable. Las consecuencias prácticas son evidentes: se incentiva la conclusión anticipada como vía de escape, se desalienta la investigación técnicamente rigurosa y se vulnera el derecho del imputado a un juicio justo con prueba válida.

Cuarta categoría: conclusión anticipada.

La conformidad se ha convertido en la vía preferida para resolver casos de fraude informático, permitiendo evitar el debate probatorio técnico, las demoras de los peritajes y el riesgo de absolución. Esta categoría es particularmente relevante porque revela cómo una estrategia procesal legítima, diseñada como un mecanismo excepcional para casos de evidente responsabilidad, se ha transformado en la regla general en la persecución penal del fraude informático en Huamanga. Es significativo que sea un juez quien también menciona esta categoría, al señalar que si hay conformidad no necesita analizar la prueba técnica. Esta declaración revela que la conformidad no solo es preferida por los fiscales, sino también aceptada y validada por los jueces como un mecanismo que les permite evitar el trabajo de valorar técnicamente la evidencia digital. El problema no es la conformidad en sí misma, sino que su uso generalizado impide el desarrollo de jurisprudencia técnica sobre valoración de evidencia digital. Si la mayoría de los casos se resuelven por conformidad, los jueces nunca tienen la oportunidad de enfrentarse al desafío de valorar técnicamente un peritaje informático, de aplicar criterios de cadena de custodia o de verificar un hash. La falta de práctica perpetúa la falta de competencia, generando un círculo vicioso del que es difícil salir.

Quinta categoría: brecha discurso-práctica.

Los tres fiscales coinciden en señalar la existencia de una diferencia significativa entre el discurso sofisticado de las sentencias, que citan estándares probatorios y autores especializados como Taruffo o Ferrer Beltrán, y la práctica judicial real, que se limita a verificar la presencia del nombre del acusado en el reporte bancario. Esta categoría es

quizás la más reveladora desde una perspectiva crítica porque evidencia una incoherencia institucional: los jueces saben qué deberían hacer, lo escriben en sus sentencias, pero no lo hacen en la práctica. Un fiscal señala que los jueces escriben bonito para protegerse, lo que sugiere que el discurso sofisticado de las sentencias no es tanto una expresión de la práctica real del juzgador, sino una estrategia de blindaje para evitar que la sentencia sea anulada en apelación. La cita a autores extranjeros y la invocación de estándares probatorios funcionarían, desde esta perspectiva, como un revestimiento retórico que no se corresponde con el razonamiento probatorio real. El fiscal de mayor experiencia califica este fenómeno como discurso vacío, señalando que los jueces hacen lo mínimo indispensable. Esta declaración, proveniente de un fiscal con quince años de experiencia, sugiere que la brecha no es un fenómeno aislado ni atribuible a jueces inexpertos, sino una práctica institucional arraigada en el distrito judicial de Huamanga.

5.3. Discusión de resultados

La discusión de resultados constituye el eje vertebrador de la presente investigación, pues en este apartado se contrastan los hallazgos empíricos obtenidos del análisis documental de cinco sentencias y de las entrevistas a seis operadores de justicia con los referentes teóricos, normativos y jurisprudenciales desarrollados en el marco teórico. El objetivo central es determinar en qué medida la práctica judicial observada en los Juzgados Penales Unipersonales de Huamanga se ajusta —o se distancia— de los estándares técnicos, legales y doctrinales que rigen la valoración de la evidencia digital en casos de fraude informático.

La discusión se organiza en torno a seis ejes temáticos que emergen de los hallazgos: (i) la ausencia de valoración técnico-forense como problema estructural; (ii) la confianza institucional como sucedáneo de la verificación técnica; (iii) el déficit formativo de los operadores de justicia; (iv) las limitaciones materiales del distrito judicial de Huamanga; (v) la conclusión anticipada como vía de escape al debate probatorio; y (vi) la brecha entre discurso y práctica judicial. Finalmente, se presentan las implicancias de los hallazgos para la teoría, la práctica judicial y las políticas públicas.

A. La ausencia de valoración técnico-forense como problema estructural

El hallazgo más contundente de la investigación es que, en el 100% de las sentencias analizadas (5/5), los jueces no aplicaron criterios técnicos de valoración de

evidencia digital (autenticidad, integridad, cadena de custodia, fiabilidad). Esta ausencia se mantuvo invariable independientemente del sentido del fallo (absolución o condena) y de la etapa procesal (juicio oral con debate o conclusión anticipada). En las dos sentencias con debate probatorio contradictorio (Expedientes 00724-2020 y 01342-2022), la evidencia digital fue tratada implícitamente como prueba documental tradicional; en las tres sentencias conformadas (Expedientes 00477-2023, 01263-2019 y 02815-2019), directamente no existió valoración alguna, pues la aceptación de cargos sustituyó la actividad probatoria.

Este hallazgo confirma el supuesto general de la investigación: la valoración de la evidencia digital en las sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga es predominantemente implícita, informal y asimilada a la prueba documental tradicional, sin aplicación explícita de criterios técnico-forenses, lo que genera una deficiencia estructural en la prueba de estos delitos que no se subsana ni siquiera en los casos con debate probatorio pleno.

Este hallazgo contrasta frontalmente con los estándares propuestos por la doctrina internacional más calificada. Casey (2011) sostiene que la evidencia digital, por su naturaleza maleable y fácilmente alterable, exige procedimientos rigurosos de autenticación que incluyen la verificación mediante funciones hash, la preservación de metadatos y la documentación exhaustiva de la cadena de custodia. La práctica judicial de Huamanga, sin embargo, prescinde por completo de estos procedimientos, tratando los reportes bancarios impresos como si fueran documentos en papel con valor probatorio intrínseco.

Mason (2016) señala que la evidencia digital no puede ser tratada como prueba documental tradicional, pues su carácter intangible y su dependencia de herramientas tecnológicas para su interpretación exigen un tratamiento probatorio diferenciado. La asimilación acrítica de la evidencia digital a la prueba documental —observada en todas las sentencias analizadas— constituye, desde esta perspectiva, un error epistemológico y metodológico de primera magnitud, pues desconoce las particularidades que distinguen a los datos digitales de los documentos físicos.

La deficiencia identificada también contradice los estándares normativos aplicables. El artículo 158 del Código Procesal Penal peruano establece el principio de

libre valoración razonada, exigiendo a los jueces fundamentar de manera lógica, coherente y motivada las razones por las cuales otorgan o niegan valor probatorio a determinado elemento. San Martín Castro (2017) interpreta que esta valoración no es arbitraria, sino que debe sustentarse en criterios de fiabilidad, pertinencia y suficiencia probatoria. Sin embargo, en las sentencias analizadas, la "valoración" de la evidencia digital se reduce a una constatación formal de su existencia (el reporte bancario existe, menciona el nombre del acusado, hay una transferencia), sin ningún análisis de su fiabilidad técnica.

La Ley N° 30096, por su parte, exige probar la "manipulación en el funcionamiento de un sistema informático", extremo que —como señala Salinas Siccha (2019) — requiere prueba pericial especializada. En cuatro de las cinco sentencias analizadas no se realizó ningún peritaje informático; en la quinta (Expediente 00724-2020), el testimonio pericial fue genérico (explicación del spoofing en abstracto) y no implicó un análisis forense concreto del caso. Esta ausencia de peritaje implica que el elemento central del tipo penal —la manipulación informática— quedó sin acreditar técnicamente, vulnerando el principio de tipicidad y el estándar de prueba más allá de toda duda razonable.

El Convenio de Budapest (artículo 14) establece que los Estados Parte deben adoptar las medidas necesarias para asegurar la obtención y presentación de evidencia digital en forma expedita. La práctica judicial de Huamanga, al no exigir ni valorar técnicamente dicha evidencia, incumple este mandato internacional.

La Casación N° 1445-2017-Lima estableció que la evidencia digital debe ser sometida a un control riguroso de autenticidad y cadena de custodia, siendo insuficiente la mera presentación de documentos impresos sin verificación técnica. La sentencia absolutoria del Expediente 00724-2020 aplica implícitamente este criterio al señalar que la Fiscalía no cumplió con recabar las cámaras de seguridad ni determinar la ubicación geográfica de los retiros, pero no exige el mismo estándar para la evidencia digital bancaria. Esta asimetría revela una concepción distorsionada de lo que constituye "prueba técnica" en el ámbito digital.

El Acuerdo Plenario N° 04-2015/CIJ-116, que incorpora los criterios Daubert para la valoración de la prueba pericial, exige evaluar la fiabilidad de la metodología

empleada, la tasa de error conocida o potencial, la existencia de estándares que controlen su funcionamiento y la aceptación general en la comunidad científica. En ninguna de las sentencias analizadas se aplicaron estos criterios, ni siquiera en el Expediente 01342-2022, donde hubo debate probatorio pleno y se citó extensamente doctrina sobre valoración probatoria.

B. La confianza institucional como sucedáneo de la verificación técnica

Los seis entrevistados (tres jueces y tres fiscales) coincidieron en que la confianza en el banco como entidad emisora reemplaza cualquier verificación técnica de autenticidad o integridad. Los reportes bancarios se aceptan como válidos por su origen, sin aplicar controles como hash, cadena de custodia o verificación del archivo digital original. Esta categoría, denominada "confianza institucional" en el análisis temático, revela una presunción de veracidad de la prueba bancaria que no tiene correlato en la regulación de la prueba digital.

Desde una perspectiva técnico-forense, un reporte bancario impreso es tan susceptible de alteración como una captura de pantalla de WhatsApp. Sin embargo, los operadores de justicia tratan a ambos de manera diametralmente opuesta: la captura de WhatsApp es recibida con escepticismo y frecuentemente rechazada si no cumple estándares formales, mientras que el reporte bancario es aceptado sin cuestionamiento.

López-López (2022) advierte que esta confianza institucional diferenciada constituye un sesgo cognitivo que distorsiona la valoración probatoria. El banco es percibido como una institución confiable, mientras que el ciudadano particular es percibido como potencialmente manipulador. Este sesgo, aunque comprensible sociológicamente, es problemático desde una perspectiva epistemológica porque la confianza no sustituye la verificación. La evidencia digital debe ser evaluada por sus características intrínsecas (autenticidad, integridad, fiabilidad), no por la reputación de la entidad que la emite.

C. El déficit formativo de los operadores de justicia

Los tres jueces entrevistados reconocieron que su formación en evidencia digital forense es insuficiente. El juez de mayor experiencia (14 años) señaló que cuando estudió Derecho los delitos informáticos no existían en el Código Penal. El juez con diez años de

experiencia indicó que la formación recibida en la Academia de la Magistratura fue un curso básico sin contenido forense. Incluso el juez de menor experiencia (6 años), que ha llevado un diplomado en delitos informáticos, calificó su formación como teórica, no práctica.

Rogers (2015) sostiene que la naturaleza volátil y cambiante de la evidencia digital obliga a que los magistrados mantengan una actualización constante en temas como criptografía, redes, sistemas operativos y nuevas modalidades de ataque digital. La formación aislada o puntual es insuficiente; se requiere un modelo sostenible que integre alianzas con universidades, organismos internacionales y laboratorios forenses.

Rivas-López (2020) añade que la capacitación no debe limitarse a aspectos teóricos del derecho penal informático, sino que debe incluir competencias técnicas esenciales para la interpretación adecuada de evidencia digital compleja: cómo leer un informe pericial, qué preguntas hacer a un perito en audiencia, cómo identificar inconsistencias metodológicas, cómo evaluar la fiabilidad de las herramientas forenses utilizadas.

El déficit formativo tiene consecuencias directas en la calidad de las decisiones judiciales. En primer lugar, genera una dependencia excesiva del perito, pues el juez carece de los conocimientos básicos para cuestionar técnicamente el informe pericial. En segundo lugar, impide que el juez ejerza un control efectivo sobre la cadena de custodia digital. En tercer lugar, favorece la aceptación acrítica de la evidencia proveniente de fuentes institucionales (bancos) y el rechazo automático de la evidencia proveniente de fuentes no institucionales (particulares). En cuarto lugar, desincentiva la realización de juicios orales con debate probatorio pleno, pues los jueces prefieren la conclusión anticipada para evitar enfrentarse a una prueba que no están capacitados para valorar.

D. Las limitaciones materiales del distrito judicial de Huamanga

Los tres fiscales entrevistados coincidieron en señalar la ausencia de laboratorio forense informático en Huamanga como la principal limitación material. A ello se suman la falta de peritos especializados, las demoras de meses en los peritajes derivados a Lima, y la carencia de equipos forenses básicos como write blockers o software especializado.

Esta situación no es exclusiva de Huamanga, sino que refleja una problemática estructural en el sistema de justicia penal peruano. Reyna Alfaro (2020) señala que la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional y la Fiscalía Especializada en Ciberdelincuencia tienen su sede principal en Lima, con limitada presencia en el interior del país. La derivación de pericias a la capital genera demoras que pueden extenderse por seis meses o más, tiempo durante el cual el proceso se paraliza, el agraviado se desgasta y el imputado, si está en libertad, puede eludir la acción de la justicia.

El Banco Interamericano de Desarrollo (BID, 2020) ha documentado que en América Latina persiste una brecha significativa en la modernización tecnológica de los sistemas de justicia, lo que impacta en la gestión adecuada de delitos informáticos. El caso peruano es paradigmático: mientras Lima cuenta con laboratorios forenses informáticos y personal especializado, los distritos judiciales del interior carecen de infraestructura básica para la investigación y juzgamiento de estos delitos.

Las limitaciones materiales no solo afectan la calidad de las investigaciones, sino que incentivan perversamente la conclusión anticipada como vía de escape. Como señaló el Fiscal F02: "Prefiero la conclusión anticipada, evita todo el problema del peritaje". Esta declaración revela que la conformidad no es solo una opción procesal entre otras, sino una estrategia deliberada para evitar los costos (en tiempo, recursos y complejidad) de un juicio oral con debate probatorio pleno.

El Fiscal F03, con 15 años de experiencia, fue el más crítico: "No es porque no queramos investigar bien. Es porque no podemos". Esta declaración exculpa a los fiscales individuales y señala al sistema como responsable. La conclusión anticipada no sería, desde esta perspectiva, una manifestación de mala praxis, sino una respuesta racional a un contexto de limitaciones estructurales.

E. La conclusión anticipada como vía de escape al debate probatorio

El 60% de las sentencias analizadas (3/5) corresponden a procesos resueltos mediante conclusión anticipada (conformidad). Los fiscales reconocieron que esta figura se ha convertido en la vía preferida para resolver casos de fraude informático, permitiendo evitar el debate probatorio técnico, las demoras de los peritajes y el riesgo de absolución.

El Acuerdo Plenario N° 05-2008/CJ-116 establece que la conclusión anticipada es un mecanismo legítimo de simplificación procesal que permite al imputado renunciar al juicio público y a la actividad probatoria a cambio de una reducción de la pena. Sin embargo, su uso generalizado en materia de fraude informático tiene un efecto colateral preocupante: impide que los jueces se enfrenten al desafío de valorar técnicamente la evidencia digital.

San Martín Castro (2017) advierte que la conclusión anticipada no debe convertirse en la regla general en ningún tipo penal, pues ello vacía de contenido el principio de inmediación y contradicción que rige el juicio oral. En el caso específico del fraude informático, el uso masivo de la conformidad tiene una consecuencia adicional: al no haber debate probatorio, no se genera jurisprudencia ni estándares técnicos sobre cómo debe valorarse la evidencia digital en esta materia. La falta de práctica perpetúa la falta de competencia, generando un círculo vicioso del que es difícil salir.

Se configura así una paradoja preocupante: cuanto más se tecnifica el delito, menos técnica es la prueba que se presenta y valora en el proceso penal. El fraude informático, que por definición implica la manipulación de sistemas informáticos, se prueba casi exclusivamente con reportes bancarios impresos, sin peritajes forenses, sin cadena de custodia, sin verificación de integridad. Y los jueces, carentes de formación especializada y enfrentados a limitaciones materiales y procesales, convalidan esta práctica, ya sea absolviendo por falta de prueba o condenando en virtud de conformidades que eluden cualquier análisis técnico.

F. La brecha entre discurso y práctica judicial

Los tres fiscales entrevistados coincidieron en señalar la existencia de una diferencia significativa entre el discurso sofisticado de las sentencias (que citan estándares probatorios y autores especializados como Taruffo, Ferrer Beltrán o Laudan) y la práctica judicial real (que se limita a verificar la presencia del nombre del acusado en el reporte bancario). Un fiscal señaló que los jueces "escriben bonito para protegerse", lo que sugiere que el discurso sofisticado de las sentencias no es tanto una expresión de la práctica real del juzgador, sino una estrategia de blindaje para evitar que la sentencia sea anulada en apelación.

Este hallazgo evidencia una incoherencia institucional que Cubas Villanueva (2018) ha calificado como "discurso vacío": los jueces saben qué deberían hacer, lo escriben en sus sentencias, pero no lo hacen en la práctica. La cita a autores extranjeros y la invocación de estándares probatorios funcionan, desde esta perspectiva, como un revestimiento retórico que no se corresponde con el razonamiento probatorio real.

La Sentencia Plenaria Casatoria N° 1-2017/CIJ-433 estableció que el estándar de prueba en el proceso penal peruano es "más allá de toda duda razonable", no la mera convicción del juez. Sin embargo, en la práctica judicial de Huamanga, la "duda razonable" se satisface con prueba indiciaria e inferencias lógicas (como en el Expediente 01342-2022), no con prueba técnica digital. Y cuando hay conformidad, directamente no se aplica estándar probatorio alguno.

Ferrer Beltrán (2021) —uno de los autores citados en las sentencias— sostiene que la motivación de la sentencia debe dar cuenta del razonamiento probatorio que lleva al juez a considerar probado o no un hecho. En las sentencias analizadas, la motivación sobre la evidencia digital es inexistente o meramente formal. No se explica por qué se considera auténtico un reporte bancario impreso, ni cómo se garantiza su integridad, ni qué cadena de custodia se siguió. La "valoración" se reduce a una constatación: el documento existe, tiene membrete del banco, menciona el nombre del acusado. Eso es todo.

G. Implicancias de los hallazgos

La investigación confirma la necesidad de una teoría de la prueba digital que no se limite a trasladar acríticamente los conceptos de la prueba documental tradicional. Casey (2011) y Mason (2016) han propuesto modelos de valoración específicos para la evidencia digital, pero estos modelos requieren no solo su adopción formal, sino también su internalización por parte de los operadores de justicia a través de procesos de capacitación y actualización continua.

El hallazgo de la "confianza institucional" como sucedáneo de la verificación técnica sugiere la necesidad de revisar críticamente las presunciones implícitas que guían la valoración probatoria en el sistema penal peruano. La confianza en el banco no puede reemplazar la verificación de la autenticidad y la integridad de la evidencia digital.

Las implicancias prácticas son múltiples. En primer lugar, la investigación proporciona un diagnóstico detallado de las deficiencias en la valoración de la evidencia digital en el distrito judicial de Huamanga, que puede servir como base para el diseño de programas de capacitación específicos para jueces y fiscales.

En segundo lugar, los hallazgos evidencian la necesidad de asignar recursos para la creación de un laboratorio forense informático en Huamanga o, como medida transitoria, para establecer protocolos de cadena de custodia estandarizados para la evidencia digital bancaria.

En tercer lugar, la investigación sugiere la necesidad de reducir el uso de la conclusión anticipada como regla general en casos de fraude informático, promoviendo el debate probatorio pleno para que los jueces desarrollen competencias en la valoración técnica de la evidencia digital.

Desde una perspectiva normativa, la investigación sugiere la conveniencia de incorporar en el Código Procesal Penal peruano criterios explícitos para la valoración de la evidencia digital, tal como proponen Flores Sánchez y Guevara Castillo (2021) en su tesis sobre la incorporación de un artículo 185-A en el Código Procesal Penal. Estos criterios deberían incluir, al menos: (i) la obligación de verificar la autenticidad mediante hash u otros mecanismos técnicos; (ii) la obligación de documentar la cadena de custodia digital; (iii) la obligación de realizar peritaje informático forense en todos los casos de fraude informático; y (iv) la obligación de motivar expresamente la valoración de la evidencia digital en la sentencia.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- En el distrito judicial de Huamanga, la valoración de la evidencia digital en sentencias por fraude informático es predominantemente implícita, informal y asimilada a la prueba documental tradicional. No existe aplicación explícita de criterios técnico-forenses como autenticidad, integridad, cadena de custodia o fiabilidad en ninguno de los casos analizados (0/5), independientemente del sentido del fallo (absolución o condena) o de la etapa procesal (juicio oral o conclusión anticipada). Esta deficiencia es estructural y no coyuntural.

- Los criterios técnicos de valoración de evidencia digital —autenticidad, integridad, cadena de custodia, fiabilidad— no son aplicados explícita ni implícitamente por los jueces de Huamanga. En las sentencias con debate probatorio, la evidencia digital se trata como prueba documental tradicional; en las sentencias conformadas, la aceptación de cargos sustituye cualquier valoración técnica. Ninguna sentencia menciona la cadena de custodia, verificación mediante hash o peritaje informático forense.

- Las principales limitaciones que enfrentan los operadores de justicia en Huamanga son: (a) ausencia de laboratorio forense informático y falta de peritos especializados en el distrito; (b) demoras de meses en peritajes derivados a Lima; (c) déficit formativo de jueces y fiscales en materia de evidencia digital forense; (d) carencia de equipos forenses básicos; y (e) uso generalizado de la conclusión anticipada como vía de escape al debate probatorio técnico.

- Existe una brecha significativa entre el discurso normativo y la práctica judicial documentada. Los fiscales entrevistados coinciden en que las sentencias citan estándares probatorios y autores especializados (Taruffo, Ferrer Beltrán) como "discurso vacío" o "estrategia de blindaje", mientras que la valoración real se limita a verificar la presencia del nombre del acusado en el reporte bancario impreso, sin análisis técnico alguno.

- La ausencia de peritaje informático forense en cuatro de cinco sentencias (y testimonio genérico en la quinta) implica que el elemento central del tipo penal de fraude informático —la "manipulación en el funcionamiento de un sistema informático"— queda sin acreditar técnicamente, vulnerando el principio de tipicidad y el estándar de prueba más allá de toda duda razonable.

6.2. RECOMENDACIONES

- Se recomienda al Poder Judicial implementar un programa de capacitación obligatoria y continua para jueces de Huamanga en informática forense y valoración técnica de evidencia digital, con énfasis en aspectos prácticos como lectura de peritajes y cadena de custodia.

- Se recomienda al Ministerio Público implementar un protocolo estandarizado de cadena de custodia para evidencia digital bancaria, que incluya la obtención del archivo digital original, la generación de hash y la documentación de la trazabilidad.

- Se recomienda a la Academia de la Magistratura incorporar en los programas de formación inicial y continua cursos obligatorios sobre informática forense y evidencia digital, con metodología práctica basada en estudio de casos reales.

- Se recomienda al Congreso de la República incorporar en el Código Procesal Penal un artículo específico sobre valoración de evidencia digital, que establezca criterios mínimos de autenticidad, integridad y cadena de custodia.

- Se recomienda a los operadores de justicia de Huamanga reducir progresivamente el uso de la conclusión anticipada como regla general en casos de fraude informático, promoviendo el debate probatorio pleno para fortalecer la cultura de valoración técnica de la prueba digital.

BIBLIOGRAFÍA

Abel, S. (2020). Digital evidence challenges and admissibility standards. Journal of Digital Forensics, Security and Law, 15(2), 45–60.

Alva Arévalo, S. D. (2025). Valor probatorio de la prueba digital en el proceso penal y su relación con el debido proceso [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional UCV. https://hdl.handle.net/20.500.12692/180127

Asociación Internacional de Policía (ACPO). (2011). Good Practice Guide for Digital Evidence.

Avendaño, F. (2020). Animarse a la tesis. Homo Sapiens Ediciones. https://elibro.net/es/lc/unsch/titulos/177169

Avila Contreras, L., & Serrano Campoverde, J. (s.f.). Eficacia de las pruebas electrónicas en el sistema judicial mediante criterios específicos de peritaje. http://scielo.sld.cu/pdf/sc/v17n11/2306-2495-sc-17-11-132.pdf

Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

Britz, M. T. (2013). Computer forensics and cyber crime: An introduction (3rd ed.). Pearson.

Cadillo Quispe, B. A. (2022). Evidencia digital y su valoración en los delitos informáticos en el proceso penal peruano [Tesis de grado, Universidad Privada del Norte]. Repositorio Institucional UPN. https://hdl.handle.net/11537/32802

Cadillo, J. (2022). La evidencia digital en el cibercrimen – Perú 2022 (Tesis de licenciatura). [Universidad correspondiente].

Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.

Carrasco Díaz, S. (2005). Metodología de la investigación científica. Editorial San Marcos.

Casey, E. (2019). Handbook of digital forensics and investigation. Academic Press.

Congreso de la República del Perú. (2004). Código Procesal Penal. Diario Oficial El Peruano.

Congreso de la República del Perú. (2013). Ley N.° 30096 – Ley de Delitos Informáticos. Diario Oficial El Peruano.

Corte Suprema de Justicia de la República. (2018). Casación N.° 1445-2017-Lima.

Corte Suprema de Justicia de la República. (2020). Casación N.° 173-2019-Arequipa.

Espinoza, R. (2021). Análisis de los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021 (Tesis de licenciatura). [Universidad correspondiente].

Europol. (2021). Internet Organized Crime Threat Assessment (IOCTA). Europol Publications.

Flores Sánchez, M. L., & Guevara Castillo, J. E. (2021). Evidencia digital en el proceso penal peruano [Tesis de grado, Universidad César Vallejo]. Repositorio Institucional UCV. https://hdl.handle.net/20.500.12692/70226

García, M., & López, A. (2021). Ciberdelitos y prueba digital. Tirant lo Blanch.

Gercke, M. (2012). Comprensión del ciberdelito: Guía para los países en desarrollo. Unión Internacional de Telecomunicaciones.

González, M. (2019). El valor de la prueba digital en el sistema acusatorio penal mexicano (Tesis de licenciatura). Universidad Nacional Autónoma de México.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system. RAND Corporation.

Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. Doubleday.

Hernández Sampieri, R., & Mendoza Torres, C. (2019). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill Interamericana Editores.

Holt, T. J., & Bossler, A. M. (2014). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

International Organization for Standardization. (2012). ISO/IEC 27037: Guidelines for identification, collection and preservation of digital evidence.

Interpol. (2022). Global Cybercrime Trends and Responses. Interpol Cybercrime Directorate.

Jiménez Rivas, A. (2023). Delitos informáticos y valoración probatoria en sistemas digitales. Editorial Jurídica Continental.

Kessler, G. C. (2019). Guide to computer forensics and investigations (6th ed.). Cengage Learning.

López, D. (2020). La evidencia digital y su eficacia probatoria en los procesos penales en Colombia (Tesis de licenciatura). Universidad Libre de Colombia.

López-López, M. (2022). La valoración judicial de la prueba digital en procesos penales. Revista Iberoamericana de Derecho Procesal, 12(2), 45–67.

Mason, S. (2019). Electronic evidence and electronic signatures (6th ed.). Institute of Advanced Legal Studies.

Ministerio Público del Perú. (2020). Manual de criminalística digital. Instituto de Medicina Legal y Ciencias Forenses.

Morgan, S. (2022). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybersecurity Ventures.

National Institute of Standards and Technology. (2020). Guide to integrating forensic techniques into incident response (SP 800-86). NIST.

National Institute of Standards and Technology. (2022). Digital forensics framework. NIST.

Palomo Vélez, C. (2021). Cadena de custodia digital: estándares y buenas prácticas. Revista de Criminalística y Ciencias Forenses, 9(1), 78–95.

Pecchioni, M. (s.f.). Estafa informática: El caso de la incorporación de la prueba digital en el proceso penal de Córdoba. https://repositorio.21.edu.ar/bitstreams/a51073b4-2630-4c8e-960c-1445e74d3920/download

Pérez, L., Pérez, R., & Seca, M. V. (2020). Metodología de la investigación científica. Editorial Maipue. https://elibro.net/es/lc/unsch/titulos/138497

Poder Judicial del Perú. (2018). Guía para el manejo de evidencia digital y cadena de custodia. Fondo Editorial del Poder Judicial.

Ramírez, A. (2022). Importancia de la evidencia digital en la resolución de casos de la Ley de Delitos Informáticos – Ley N.° 30096 y modificatorias con la Ley N.° 30171 en la División de Alta Tecnología PNP, Lima, 2022 (Tesis de licenciatura). [Universidad correspondiente].

Ramírez, J. (2021). La prueba electrónica y su valoración judicial en el proceso penal español (Tesis de maestría). Universidad Complutense de Madrid.

Reyna Alfaro, L. (2020). Prueba digital y pericia informática en el proceso penal peruano. Instituto Pacífico.

Rogers, M. (2015). Computer forensics: Hard disk and operating systems. EC-Council Press.

Rogers, M. K. (2015). Cyber forensics. En G. Brown (Ed.), The essentials of cyber security (pp. 233–255). Syngress.

Salinas Siccha, R. (2019). Código Procesal Penal comentado. Instituto Pacífico.

San Martín Castro, C. (2017). La prueba en el proceso penal. Fondo Editorial del Poder Judicial del Perú.

Schjølberg, S., & Ghernaouti-Hélie, S. (2011). A global treaty on cybersecurity and cybercrime. Cybercrimelaw.net.

Sotomayor, A. (2021). Cibercrimen y evidencia digital en América Latina. Universidad Externado de Colombia.

Tribunal Constitucional del Perú. (2016). Expediente N.° 00165-2016-PHC/TC.

Vadell, L., & Rúa, M. (s.f.). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. https://dialnet.unirioja.es/descarga/articulo/8084167.pdf

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (3rd ed.). Sage Publications.

ANEXOS

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA PROFESIONAL DE DERECHO

Valoración de la evidencia digital en sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga.			
PROBLEMAS	**OBJETIVOS**	**SUPUESTOS**	**METODOLOGÍA**
Problema general: ¿Cómo se valora la evidencia digital en las sentencias por delito de fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga durante el período 2022-2024, y en qué medida dicha valoración se ajusta a los estándares técnicos y legales vigentes?	**Objetivo general:** Analizar la valoración de la evidencia digital en las sentencias por delito de fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga, determinando el grado de ajuste de dicha valoración a los estándares técnicos y legales vigentes.	**Supuesto general:** La valoración de la evidencia digital en las sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga es predominantemente implícita, informal y asimilada a la prueba documental tradicional, sin aplicación explícita de criterios técnico-forenses (autenticidad, integridad, cadena de custodia, fiabilidad), lo que genera una deficiencia estructural en la prueba de estos delitos.	**Enfoque:** Cualitativo **Tipo:** Básica o pura **Nivel:** Descriptivo-explicativo **Diseño:** No experimental, transversal, cualitativo **Muestra:** 5 sentencias + 6 operadores de justicia (3 jueces, 3 fiscales) **Técnicas:** Análisis documental y entrevista semiestructurada **Instrumentos:** Ficha de análisis documental y guía de entrevista
Problemas específicos: 1. ¿Qué criterios técnicos de valoración de evidencia digital (autenticidad, integridad, cadena de custodia, fiabilidad) son explícita o implícitamente aplicados por los	**Objetivos específicos:** 1. Identificar los criterios técnicos de valoración de evidencia digital (autenticidad, integridad, cadena de custodia, fiabilidad) que son explícita o implícitamente	**Supuestos específicos:** 1. Los jueces de Huamanga no aplican explícitamente criterios técnicos de autenticidad, integridad, cadena de custodia o fiabilidad de la evidencia digital. En su lugar, aplican criterios	

jueces en las sentencias por fraude informático emitidas en Huamanga entre 2022 y 2024? 2. ¿Cuáles son las principales limitaciones o dificultades que enfrentan los operadores de justicia (jueces, fiscales, peritos) en Huamanga para valorar técnicamente la evidencia digital en casos de fraude informático? 3. ¿Existe coherencia entre la valoración de la evidencia digital documentada en las sentencias y los discursos o prácticas declaradas por los operadores de justicia sobre cómo debería valorarse dicha evidencia?	aplicados por los jueces en las sentencias por fraude informático emitidas en Huamanga entre 2022 y 2024. 2. Describir las principales limitaciones o dificultades que enfrentan los operadores de justicia en Huamanga para valorar técnicamente la evidencia digital en casos de fraude informático. 3. Contrastar la valoración de la evidencia digital documentada en las sentencias con los discursos y prácticas declaradas por los operadores de justicia, a fin de determinar el nivel de coherencia entre ambos planos.	jurídicos generales y tratan la evidencia digital como prueba documental tradicional. 2. Las principales limitaciones son: (a) ausencia de peritaje informático en la mayoría de casos, (b) falta de formación técnica de jueces y fiscales, (c) dependencia de documentos impresos de bancos sin verificación de integridad, y (d) resolución de casos por conformidad para evitar el desafío probatorio. 3. Existe una brecha significativa entre el discurso normativo (lo que operadores declaran que debería hacerse) y la práctica documentada en sentencias (lo que realmente se hace).	

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA PROFESIONAL DE DERECHO

FICHA DE ANÁLISIS DOCUMENTAL DE SENTENCIAS

I. DATOS GENERALES DE LA SENTENCIA

Campo	Registro
Número de Expediente	
Órgano jurisdiccional	
Juzgado	
Distrito judicial	
Tipo de resolución	☐ Sentencia condenatoria ☐ Sentencia absolutoria ☐ Sentencia conformada
Fecha de emisión	
Juez/Ponente	
Ministerio Público (Fiscal)	
Delito imputado	
Etapa procesal	

II. IDENTIFICACIÓN DEL CASO

Campo	Registro
Imputado(s)	
Agraviado(s)	
Descripción de los hechos relevantes (sintética, máximo 150 palabras)	

III. EVIDENCIA DIGITAL INCORPORADA AL PROCESO

3.1. Tipo de evidencia digital identificada (marque todas las que correspondan)

Tipo de evidencia	Presente	Observaciones
☐ Correos electrónicos	☐ Sí ☐ No	
☐ Mensajes de texto (WhatsApp, SMS, etc.)	☐ Sí ☐ No	
☐ Registros bancarios (estados de cuenta, transferencias)	☐ Sí ☐ No	

☐ Plataforma web / phishing / sitio clonado	☐ Sí ☐ No	
☐ Registros informáticos (logs, metadatos)	☐ Sí ☐ No	
☐ Capturas de pantalla	☐ Sí ☐ No	
☐ Videos de cámaras de seguridad	☐ Sí ☐ No	
☐ Dispositivos móviles o computadoras incautadas	☐ Sí ☐ No	
☐ Otro (especificar):	☐ Sí ☐ No	

3.2. Fuente de obtención de la evidencia digital

Fuente	Mencionada
Banco de la Nación / entidad financiera	☐ Sí ☐ No
Proveedor de servicios de internet	☐ Sí ☐ No
Empresa de telecomunicaciones	☐ Sí ☐ No
Incautación directa (policial)	☐ Sí ☐ No
Entrega voluntaria por parte del imputado	☐ Sí ☐ No
Otro (especificar):	

3.3. Forma de incorporación al proceso

Medio de incorporación	Utilizado
☐ Prueba documental (impresa)	☐ Sí ☐ No
☐ Prueba pericial (informe técnico)	☐ Sí ☐ No
☐ Prueba testimonial (declaración sobre lo digital)	☐ Sí ☐ No
☐ Inspección judicial (visualización directa)	☐ Sí ☐ No

3.4. Cadena de custodia

Aspecto	Registro
¿Se menciona la cadena de custodia en la sentencia?	☐ Sí ☐ No
¿Se describe el procedimiento de aseguramiento?	☐ Sí ☐ No ☐ No aplica
¿Se identifica al responsable de la custodia?	☐ Sí ☐ No ☐ No aplica
¿Se detectan rupturas o deficiencias en la cadena?	☐ Sí ☐ No ☐ No se precisa

3.5. Descripción detallada de la evidencia digital (citar textualmente lo que dice la sentencia)

IV. CRITERIOS DE VALORACIÓN PROBATORIA APLICADOS POR EL JUEZ

4.1. Criterios jurídicos mencionados (marque todos los que identifique)

Criterio	Mencionado	¿Cómo lo aplica? (textual o resumen)
Pertinencia	☐ Sí ☐ No	
Conducencia	☐ Sí ☐ No	
Utilidad	☐ Sí ☐ No	
Legalidad	☐ Sí ☐ No	
Otro (especificar):	☐ Sí ☐ No	

4.2. Criterios técnicos de valoración de evidencia digital

Criterio técnico	¿Se aplica?	¿Cómo se desarrolla? (textual)
Autenticidad (¿la evidencia es lo que dice ser?)	☐ Sí ☐ No ☐ No menciona	
Integridad (¿no ha sido modificada?)	☐ Sí ☐ No ☐ No menciona	
Licitud (¿obtenida conforme a ley?)	☐ Sí ☐ No ☐ No menciona	
Fiabilidad técnica (¿el sistema es confiable?)	☐ Sí ☐ No ☐ No menciona	
Cadena de custodia (trayectoria controlada)	☐ Sí ☐ No ☐ No menciona	

4.3. Forma de valoración de la evidencia digital

Modalidad	Aplica	Descripción
☐ Explícita (el juez desarrolla análisis técnico detallado)	☐ Sí ☐ No	
☐ Implícita (se presume su validez sin desarrollo)	☐ Sí ☐ No	
☐ Basada en aceptación del imputado	☐ Sí ☐ No	
☐ Basada en otros medios probatorios (testigos, peritos)	☐ Sí ☐ No	

4.4. Nivel de incidencia de la evidencia digital en la decisión final

Nivel	Marque	Justificación (según la sentencia)

☐ Determinante (sin ella no se habría decidido igual)	☐	
☐ Complementaria (apoya otras pruebas)	☐	
☐ Secundaria (meramente ilustrativa)	☐	
☐ Ninguna (no se tomó en cuenta)	☐	

V. FUNDAMENTACIÓN JURÍDICA RELEVANTE

5.1. Normas aplicadas

Norma	Contenido relevante

5.2. Jurisprudencia citada

Tribunal / N° de expediente	Año	Extracto relevante

5.3. Doctrina mencionada

Autor	Obra	Año	Cita relevante

5.4. Argumentos específicos del juez sobre la evidencia digital (transcribir textualmente lo más relevante)

VI. DECISIÓN JUDICIAL

6.1. Decisión penal

Aspecto	Resolución
Tipo de decisión	☐ Condena ☐ Absolución ☐ Otro
Pena privativa de libertad impuesta (si aplica)	
Pena suspendida	☐ Sí ☐ No ☐ No aplica
Fundamentos principales para la decisión penal	

6.2. Decisión civil

Aspecto	Resolución
Reparación civil fijada	S/
¿Se concede a pesar de absolución penal?	☐ Sí ☐ No ☐ No aplica
Fundamentos para la reparación civil	

6.3. Sentencia completa

Fecha de la resolución	
¿Es firme / consentida?	☐ Sí ☐ No ☐ No se precisa

VII. ANÁLISIS CRÍTICO DEL INVESTIGADOR (llenar después del análisis)

7.1. Evaluación de la valoración probatoria

Aspecto	Valoración (Adecuado / Parcial / Deficiente)	Observación
Identificación de la evidencia digital	☐ Adecuado ☐ Parcial ☐ Deficiente	
Aplicación de criterios técnicos	☐ Adecuado ☐ Parcial ☐ Deficiente	
Respeto a la cadena de custodia	☐ Adecuado ☐ Parcial ☐ Deficiente	
Fundamentación de la decisión	☐ Adecuado ☐ Parcial ☐ Deficiente	

7.2. Deficiencias técnicas identificadas

N°	Deficiencia	Impacto en la decisión
1		
2		
3		

7.3. Observaciones generales

VIII. CATEGORIZACIÓN FINAL PARA RESULTADOS DE INVESTIGACIÓN

Categoría	Nivel	Marque
Tipo de valoración probatoria	☐ Adecuada ☐ Parcial ☐ Deficiente	☐
Nivel de desarrollo de criterios técnicos	☐ Alto ☐ Medio ☐ Bajo	☐
Tratamiento de la evidencia digital	☐ Como prueba digital autónoma ☐ Como prueba documental tradicional ☐ Mixto	☐

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA PROFESIONAL DE DERECHO

GUÍA DE ENTREVISTA PARA JUECES

Tesis: Valoración de la evidencia digital en sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga.

Instrucción inicial

La presente entrevista es anónima y confidencial, y tiene fines estrictamente académicos. Agradecemos su participación y honestidad. Las preguntas se orientan a conocer su experiencia práctica en la valoración de evidencia digital en casos de fraude informático.

I. DATOS GENERALES DEL ENTREVISTADO (Opcional)

- Cargo: _____
- Institución: _____
- Años de experiencia: _____
- Especialidad: _____

II. PREGUNTAS

Dimensión: Criterios técnicos aplicados

1. En las sentencias que ha emitido por fraude informático, ¿qué elementos de la evidencia digital considera indispensables para declarar la culpabilidad?
   (Ejemplo: cadena de custodia, hash, informe pericial, etc.)

   _____
   _____

Dimensión: Autenticidad e integridad de la prueba

2. ¿Cómo verifica usted que la evidencia digital presentada no ha sido alterada desde su incautación hasta el juicio?
   ¿Qué documentos o procedimientos revisa en el expediente?

   _____
   _____

Dimensión: Limitaciones de los operadores de justicia

3. ¿Qué dificultades concretas ha enfrentado para entender o valorar técnicamente la prueba digital?
   (Ejemplo: informes periciales complejos, falta de estandarización, ausencia de peritos en audiencia)

4. ¿Considera que la formación que recibió en derecho penal o en capacitaciones judiciales es suficiente para valorar adecuadamente evidencia digital?
   ¿Por qué?

Dimensión: Coherencia entre discurso y práctica

5. ¿Recuerda algún caso en el que haya rechazado evidencia digital por no cumplir estándares técnicos?
   ¿Cuál fue el motivo principal?

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
ESCUELA PROFESIONAL DE DERECHO

GUÍA DE ENTREVISTA PARA FISCALES

Tesis: Valoración de la evidencia digital en sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga.

Instrucción inicial

La presente entrevista es anónima y confidencial, y tiene fines estrictamente académicos. Agradecemos su participación y honestidad. Las preguntas se orientan a conocer su experiencia práctica en la valoración de evidencia digital en casos de fraude informático.

I. DATOS GENERALES DEL ENTREVISTADO (Opcional)

- Cargo: _____
- Institución: _____
- Años de experiencia: _____
- Especialidad: _____

II. PREGUNTAS

Dimensión: Criterios técnicos aplicados

1. Durante la etapa de investigación, ¿cómo asegura que la evidencia digital (capturas, logs, dispositivos) cumpla con la cadena de custodia y autenticidad antes de presentarla al juzgado?

   _____
   _____

Dimensión: Limitaciones de los operadores de justicia

2. ¿Qué limitaciones materiales o técnicas ha encontrado en Huamanga para obtener y preservar evidencia digital válida?
   (Ejemplo: falta de equipos forenses, demoras en peritajes, personal no especializado)

   _____
   _____

Dimensión: Coherencia entre discurso y práctica

3. En su experiencia, ¿los jueces suelen cuestionar o aceptar sin reparos los informes periciales digitales que usted presenta?

¿Ha observado casos donde se desestime la prueba por mala práctica?

_____

_____

Dimensión: Criterios técnicos y coherencia

4. Cuando ha impugnado una sentencia por fraude informático, ¿qué argumentos técnicos sobre la evidencia digital ha utilizado?
   (Ejemplo: falta de cadena de custodia, alteración, ausencia de hash, pericia parcializada)
   ¿El juez los ha acogido?

   _____

   _____

Dimensión: Coherencia entre discurso y práctica

5. Desde su experiencia, ¿existe diferencia entre lo que los jueces declaran en sus sentencias sobre la valoración de la prueba digital (sana crítica) y lo que realmente hacen?
   Mencione un ejemplo sin identificar el caso.

   _____

   _____

UNIVERSIDAD NACIONAL DE SAN CRITÓBAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Creado el 14 de junio de 1979

ACTA DE SUSTENTACIÓN DE TESIS DEL ASPIRANTE JHONATAN CISNEROS OLANO

En la ciudad de Ayacucho, siendo las 10:00 a.m., del día lunes 18 de mayo del 2026. Reunidos, en la Facultad de Derecho de la Universidad Nacional San Cristóbal de Huamanga. Richard Almonacid Zamudio (Presidente), Iván Chumbe Carrera, Marlene León Palacios, Jenny Juana Barraza Torres y Khaterine Irma Quispe Vargas (Miembros), reunidos para evaluar la tesis: Valoración de la evidencia digital en sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga, Acto seguido se da lectura a la Resolución Decanal N° 113-2026-UNSCH-FDCP-D del 05 de mayo de 2026 y el artículo 25 del Reglamento de Grados y Títulos de la Facultad de Derecho y Ciencias Políticas.

El presidente del Jurado otorga el uso de la palabra al aspirante, luego de la sustentación, el jurado realiza al aspirante las preguntas y objeciones correspondientes. Una vez concluido, el Presidente del jurado indica salir del auditorio al aspirante y los miembros del jurado proceden a deliberar.

El jurado luego de la deliberación decidió: **APROBAR** por mayoría con la nota de quince (15). Concluye el acto académico con la firma del acta.

Richard Almonacid Zamudio

Iván Chumbe Carrera

Marlene León Palacios

Katherine Irma Quise Vargas

Jenny Juana Barraza Torres

CONSTANCIA DE ORIGINALIDAD N° 07-2026-UNSCH-FDCP

El que suscribe responsable verificador de originalidad de trabajo de tesis de la Facultad de Derecho y Ciencias Políticas de la UNSCH, en cumplimiento a la Resolución de Consejo Universitario N.º 039-2021-UNSCH-CU (16-03-2021) Reglamento de Originalidad de Trabajos de Investigación de la UNSCH, otorga lo siguiente:

CONSTANCIA DE ORIGINALIDAD

Autor	**Bach. JHONATAN CISNEROS OLANO**
Para	**Título profesional**
Denominación de la tesis	**Valoración de la evidencia digital en sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga.**
Evaluación de Originalidad	**8%**
Numero de trabajo	**2969514691**
Fecha	**25 de mayo 2026**

Amparo la presente en los artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación de la UNSCH, es procedente otorgar la constancia de originalidad con deposito.

Se expide la presente constancia a solicitud de la parte interesada para los fines que crea por conveniente.

Ayacucho, 25 de mayo de 2026

Iván Chumbe Carrera

Valoración de la evidencia digital en sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga.

por Jhonatan CISNEROS OLANO

Fecha de entrega: 25-may-2026 08:57p. m. (UTC-0500)
Identificador de la entrega: 2969514691
Nombre del archivo: BORRADOR_de_tesis_Jhonatan_corregido.docx (292.5K)
Total de palabras: 34802
Total de caracteres: 207825

Valoración de la evidencia digital en sentencias por fraude informático emitidas por los Juzgados Penales Unipersonales de Huamanga.

INFORME DE ORIGINALIDAD

8%	9%	3%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.21.edu.ar Fuente de Internet	1%
2	repositorio.upn.edu.pe Fuente de Internet	1%
3	scielo.sld.cu Fuente de Internet	1%
4	alicia.concytec.gob.pe Fuente de Internet	1%
5	repositorio.ucv.edu.pe Fuente de Internet	1%
6	hdl.handle.net Fuente de Internet	<1%
7	lpderecho.pe Fuente de Internet	<1%
8	Submitted to Universidad Autonoma de Chile Trabajo del estudiante	<1%

9	img.lpderecho.pe Fuente de Internet	<1 %
10	Submitted to Universidad Tecnologica del Peru Trabajo del estudiante	<1 %
11	dspace.unach.edu.ec Fuente de Internet	<1 %
12	repositorio.ujcm.edu.pe Fuente de Internet	<1 %
13	sebastianrocano1.blogspot.com Fuente de Internet	<1 %
14	repositorio.uap.edu.pe Fuente de Internet	<1 %
15	Flores Ostos, Saul Edgard. "La aplicación del control de convencionalidad difuso en la función fiscal y su repercusión en la administración de justicia en el Distrito Fiscal de Puno, 2024", Universidad Nacional del Altiplano de Puno (Peru), 2025 Publicación	<1 %
16	Luis Eduardo Morante Mendoza, Jorge Andrés Safadi Mendoza, Gonzalo Patricio Gómez Rivera. "Delitos Informáticos y prueba digital en el COIP: validez, cadena de custodia y pericia forense en el Ecuador", Tesla Revista Científica, 2025	<1 %

	Publicación	
17	repositorio.unjfsc.edu.pe Fuente de Internet	<1 %
18	www.eje.pe Fuente de Internet	<1 %
19	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
20	lisseinquilla.blogspot.com Fuente de Internet	<1 %
21	Submitted to Integración Blackboard Trabajo del estudiante	<1 %
22	repositorio.uandina.edu.pe Fuente de Internet	<1 %
23	esdeglibros.edu.co Fuente de Internet	<1 %
24	repositorio.une.edu.pe Fuente de Internet	<1 %
25	Lopez Lopez, Renzo Saul. "Los límites de la conclusión anticipada en los procesos con pluralidad de imputados en el ordenamiento jurídico procesal peruano.", Pontificia Universidad Catolica del Peru (Peru) Publicación	<1 %
26	repositorio.continental.edu.pe Fuente de Internet	<1 %

27	Balseca Ruiz, María José. "Documentos que regulan el manejo de animales con fines investigativos en Colombia : Una revisión crítica desde la mirada bioética.", Universidad de La Sabana (Colombia) Publicación	<1 %
28	Submitted to Universidad Mariano Gálvez de Guatemala Trabajo del estudiante	<1 %
29	www.researchgate.net Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		