

**UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL
DE HUAMANGA**

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO



TESIS:

La atribución de responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados en el delito de fraude informático en el distrito judicial de Ayacucho, 2022-2024.

Para optar el título profesional de:

ABOGADA

PRESENTADO POR:

Bach. Luz Esperanza LIZANA TINCO

ASESOR:

Mtro. Iván CHUMBE CARRERA

AYACUCHO - PERÚ

2026

AGRADECIMIENTO

A mis docentes de la Escuela Profesional de Derecho, por compartir sus conocimientos con pasión y compromiso, en especial a mi asesor y aquellos quienes me guiaron en el desarrollo de esta investigación, brindándome orientación académica y crítica constructiva.

DEDICATORIA

Dedico este trabajo a mis padres, Gerbet y María Elena, y a mi hermano Cluber, quienes fueron mi guía y soporte en el desarrollo de mi vida personal y académica, por su apoyo, paciencia y comprensión; asimismo, se lo dedico a mi tío Ebert, quien me demostró a base de ejemplos y luchas, que, pese a las circunstancias y adversidades de la vida, uno debe de persistir hasta el momento que el corazón deje de latir.

Tabla de contenido

RESUMEN	11
ABSTRACT.....	13
INTRODUCCIÓN	15
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA	20
1.1. Descripción de la realidad problemática	20
1.2. Formulación del problema	22
1.2.1. Problema general	22
1.2.2. Problemas específicos	22
1.3. Objetivos de la investigación	22
1.3.1. Objetivo general.....	22
1.3.2. Objetivos específicos	22
1.4. Justificación de la investigación	23
1.4.1. Justificación teórica	23
1.4.2. Justificación práctica.....	24
1.4.3. Justificación jurídica	25
1.4.4. Justificación metodológica.....	26
1.4.5. Justificación social	26
1.5. Delimitación de la investigación.....	27
1.5.1. Delimitación temática	27
1.5.4. Delimitación poblacional	28

CAPÍTULO II: MARCO TEORICO	30
2.1. Antecedentes de la investigación	30
2.2.1. Antecedentes internacionales	30
2.2.2. Antecedentes Nacionales	32
2.2. Bases teóricas	36
2.2.1. El delito informático: concepto, naturaleza y características.....	36
2.2.2. El delito de fraude informático en la legislación penal peruana	38
2.2.3. El Convenio de Budapest sobre la Ciberdelincuencia y su recepción en el ordenamiento peruano.....	41
2.2.4. La autoría, la participación y la atribución de responsabilidad penal en el fraude informático.....	42
2.2.5. La cuenta bancaria receptora como elemento de conexión entre el hecho y su titular	45
2.2.6. La prueba indiciaria y su aplicación a la criminalidad informática	47
2.2.7. La evidencia digital y las herramientas forenses informáticas	49
2.2.8. Impunidad y desafíos institucionales frente a los delitos informáticos	51
2.2.9. Ciberseguridad y protección de datos personales	51
2.3. Marco normativo.....	52
2.3.1. Constitución Política del Perú.....	52
2.3.2. Código Penal peruano	53
2.3.3. Código Procesal Penal (artículo 158.3)	54

2.3.4. Ley N.º 30096, Ley de Delitos Informáticos, y su modificatoria Ley N.º 30171.....	55
2.3.5. Convenio de Budapest sobre la Ciberdelincuencia.....	56
2.3. Marco conceptual.....	57
CAPÍTULO III: CATEGORÍAS DE LA INVESTIGACIÓN.....	61
3.1. Matriz de categorización apriorística y emergente	61
3.2. Desarrollo de las categorías y subcategorías	66
3.2.2. Categoría 2: Valoración de la intervención de sujetos no identificados y de las hipótesis alternativas	67
3.2.3 Categoría 3: Construcción y motivación de la inferencia probatoria entre el titular registral y el titular con conocimiento y voluntad	69
CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN	71
4.1. Enfoque de investigación.....	71
4.2. Tipo de investigación.....	71
4.3. Diseño de investigación	72
3.4. Escenario de estudio	72
4.5. Sujetos de estudio	73
4.5.1. Unidades de análisis documental	73
3.5.2. Participantes de la entrevista.....	73
4.7. Técnicas e instrumentos de recolección de datos	74
4.8. Procedimiento de recolección de datos.....	75
4.9. Método de análisis de la información	75

4.10. Rigor científico	76
4.11. Aspectos éticos.....	76
CAPÍTULO V: PRESENTACIÓN DE RESULTADOS	78
5.2. Caracterización de las unidades de análisis	78
5.2.1. Muestra documental.....	78
5.2.2. Muestra de entrevistados.....	80
5.2.3. Organización y tratamiento de la información.....	80
5.3. Resultados de la categoría 1: VALOR JURÍDICO-PROBATORIO DE LA TITULARIDAD, RECEPCIÓN Y DISPOSICIÓN	81
5.3.1. Titularidad formal de la cuenta receptora	81
5.3.2. Recepción efectiva de los fondos.....	82
5.3.3. Actos posteriores de disposición.....	83
5.3.4. Síntesis de la primera categoría	84
5.4. Resultados de la categoría 2: sujetos no identificados e hipótesis alternativas	85
5.4.1. Intervención de sujetos no identificados.....	85
5.4.2. Pérdida de tarjeta o documentos y falta de bloqueo	86
5.4.3. Préstamo, suplantación y utilización no autorizada	86
5.4.4. Síntesis de la segunda categoría.....	87
5.5. Resultados de la categoría 3: construcción y motivación de la inferencia	88
5.5.1. Hechos indicadores del conocimiento y la voluntad.....	88
5.5.2. Regla inferencial y valoración conjunta	89
5.5.3. Diferenciación entre titular registral y responsable penal.....	89

5.5.4. Suficiencia de la motivación	90
5.5.5. Síntesis de la tercera categoría	90
5.6. Triangulación de los resultados	91
5.7. Hallazgos emergentes	92
5.7.1. Asimetría entre trazabilidad financiera y atribución digital	92
5.7.2. Diferencia entre egreso bancario y disposición personalmente atribuida..	92
5.7.3. Efecto metodológico de la conclusión anticipada.....	92
5.7.4. Riesgo de inversión de la carga probatoria	93
5.8. Resultado integrado respecto del objetivo general	93
CAPÍTULO VI: DISCUSIÓN DE RESULTADOS.....	95
6.1. Discusión del resultado general	95
6.2. Discusión respecto del primer objetivo específico: criterios jurídicos para calificar la intervención del titular	96
6.3. Discusión respecto del segundo objetivo específico: elementos probatorios del conocimiento y la voluntad.....	98
6.4. Discusión respecto del tercer objetivo específico: incidencia de los sujetos no identificados en la motivación	99
6.5. Discusión de los hallazgos emergentes.....	101
6.6. Implicancias teóricas y prácticas de los resultados.....	102
6.7. Limitaciones y alcance interpretativo	103
6.8. Síntesis de la discusión	103
CONCLUSIONES	105

RECOMENDACIONES	108
BIBLIOGRAFÍA	111
ANEXOS	114
ANEXO 1. MATRIZ DE CONSISTENCIA	115
ANEXO 2. MATRIZ DE CATEGORIZACIÓN.....	116
ANEXO 3. FICHA DE ANÁLISIS DOCUMENTAL	117
ANEXO 4. GUÍA DE ENTREVISTA SEMIESTRUCTURADA	118
ANEXO 5. CONSENTIMIENTO INFORMADO	120
ANEXO 6. FICHA DE VALIDACIÓN POR JUICIO DE EXPERTO	¡Error!

Marcador no definido.

ANEXO 7. RELACIÓN CODIFICADA DE SENTENCIAS¡Error! **Marcador no definido.**

ANEXO 8. MATRIZ CONSOLIDADA DE ANÁLISIS DOCUMENTAL	121
ANEXO 9. RELACIÓN CODIFICADA DE PARTICIPANTES.....	122
ANEXO 10. MATRIZ DE TRIANGULACIÓN.....	123

ÍNDICE DE TABLAS

Tabla 1	79
Tabla 2	80
Tabla 3	84
Tabla 4	87
Tabla 5	90
Tabla 6	91

RESUMEN

La investigación tuvo como objetivo analizar la forma en que los órganos jurisdiccionales penales del distrito judicial de Ayacucho atribuyeron responsabilidad penal al titular de la cuenta receptora del dinero fraudulentamente transferido, frente a la intervención de sujetos no identificados en la manipulación del sistema informático, durante el periodo 2022-2024. El estudio se desarrolló desde un enfoque cualitativo, de tipo básico, nivel descriptivo-interpretativo y diseño de estudio de casos múltiples. La muestra fue seleccionada intencionalmente y estuvo conformada por cinco sentencias emitidas por juzgados penales unipersonales de Ayacucho y nueve participantes: tres jueces penales, tres fiscales penales, dos abogados penalistas y un perito informático forense. Se emplearon el análisis documental y la entrevista semiestructurada como técnicas de recolección de información, mediante una ficha de análisis documental y una guía de entrevista. La información fue organizada mediante tres categorías apriorísticas y una subcategoría emergente, y se aplicó la triangulación de fuentes, técnicas y perfiles profesionales.

Los resultados evidenciaron que la titularidad formal de la cuenta y la recepción del dinero constituyeron únicamente elementos de vinculación inicial, pero no demostraron por sí solas el conocimiento ni la voluntad del titular de participar en el fraude informático. El elemento probatorio de mayor fuerza fue el acto de disposición personalmente atribuible, valorado conjuntamente con el control efectivo de la cuenta, la proximidad temporal, el aprovechamiento de los fondos y el contraste de las hipótesis alternativas. En los procesos contradictorios, la falta de individualización de la persona que efectuó el retiro y la ausencia de evidencia técnica mantuvieron la duda razonable y determinaron la absolución. En cambio,

la acreditación de retiros presenciales mediante tarjeta y clave, junto con el descarte razonado de la pérdida alegada, sustentó la condena.

Se concluyó que la intervención de sujetos no identificados no excluye la responsabilidad penal del titular de la cuenta receptora, pero incrementa la exigencia de individualización, corroboración y motivación. En consecuencia, la responsabilidad penal no puede presumirse a partir de la sola trazabilidad financiera, sino que requiere la acreditación de hechos adicionales que demuestren el aporte consciente del titular y una motivación que explique por qué dichos hechos resultan más compatibles con la participación dolosa que con la utilización no autorizada de la cuenta.

Palabras clave: fraude informático, responsabilidad penal, cuenta receptora, prueba indiciaria, sujetos no identificados, motivación judicial.

ABSTRACT

The study aimed to analyze how criminal courts in the Judicial District of Ayacucho attributed criminal liability to the holder of an account receiving fraudulently transferred funds when unidentified persons were involved in the manipulation of the computer system during the 2022-2024 period. The research followed a qualitative approach, was basic in nature, had a descriptive-interpretive scope, and used a multiple-case study design. The purposive sample comprised five judgments issued by single-judge criminal courts in Ayacucho and nine participants: three criminal judges, three criminal prosecutors, two criminal defense attorneys, and one digital forensics expert. Documentary analysis and semi-structured interviews were used as data collection techniques through a documentary analysis form and an interview guide. The information was organized according to three a priori categories and one emergent subcategory, and triangulation of sources, techniques, and professional profiles was applied.

The findings showed that formal account ownership and receipt of the money constituted only initial linkage elements and did not, by themselves, establish the account holder's knowledge or intent to participate in computer fraud. The strongest evidentiary element was an act of disposal personally attributable to the account holder, assessed together with effective control of the account, temporal proximity, benefit from the funds, and examination of alternative hypotheses. In adversarial proceedings, the failure to identify the person who withdrew the money and the absence of technical evidence preserved reasonable doubt and led to an acquittal. Conversely, proof of in-person withdrawals using the account holder's card and password, together with a reasoned rejection of the alleged loss of the card, supported a conviction.

It was concluded that the involvement of unidentified persons does not rule out the criminal liability of the recipient account holder, but it heightens the requirements of

individualization, corroboration, and judicial reasoning. Therefore, criminal liability cannot be presumed solely from financial traceability. It requires proof of additional facts demonstrating the account holder's conscious contribution and reasoning explaining why those facts are more consistent with intentional participation than with unauthorized use of the account.

Keywords: computer fraud, criminal liability, recipient account, circumstantial evidence, unidentified persons, judicial reasoning.

INTRODUCCIÓN

El avance de las tecnologías de la información y la consolidación de la banca digital han transformado la forma en que las personas realizan operaciones financieras. Las transferencias electrónicas, aplicaciones bancarias y sistemas de pago digital permiten ejecutar transacciones de manera inmediata y desde diferentes lugares. Sin embargo, estas ventajas también han generado nuevas formas de criminalidad patrimonial, caracterizadas por la utilización de medios tecnológicos, la actuación a distancia, la fragmentación de funciones y la dificultad para identificar a todos los participantes.

Entre estas conductas se encuentra el fraude informático, previsto en el artículo 8 de la Ley N.º 30096, Ley de Delitos Informáticos. Este delito sanciona a quien, deliberada e ilegítimamente, procura para sí o para otro un beneficio ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático. A diferencia de otros delitos patrimoniales, su ejecución suele requerir conocimientos tecnológicos específicos y puede realizarse sin contacto directo entre el autor y la víctima.

En la práctica, el fraude informático presenta frecuentemente una estructura de ejecución colectiva. Una persona puede encargarse de captar las credenciales bancarias de la víctima mediante modalidades como el *phishing*, *smishing* o *spoofing*; otra puede efectuar la manipulación del sistema o realizar la transferencia; y una tercera puede proporcionar la cuenta bancaria receptora o retirar el dinero. Esta división de funciones dificulta la reconstrucción del hecho y la determinación de la responsabilidad individual de cada participante.

En el distrito judicial de Ayacucho se advirtió que la persecución penal suele concentrarse en el titular de la cuenta receptora, debido a que su identidad puede ser obtenida con relativa facilidad mediante la información proporcionada por la entidad financiera. En contraste, los sujetos que enviaron los enlaces fraudulentos, captaron las credenciales o

manipularon el sistema informático frecuentemente permanecen sin identificar. Esta situación produce una asimetría entre la trazabilidad financiera y la atribución digital: se conoce la cuenta a la que llegó el dinero, pero no siempre se determina quién controló el dispositivo, ejecutó la transferencia o realizó el retiro.

La identificación del titular de la cuenta receptora no significa necesariamente que este haya intervenido con conocimiento y voluntad en el fraude. Su cuenta pudo haber sido utilizada sin autorización, sus datos pudieron ser obtenidos mediante suplantación de identidad o pudo haber cedido el acceso sin conocer el origen ilícito específico de los fondos. Por ello, la sola titularidad registral y la recepción del dinero no deben convertirse en una presunción automática de responsabilidad penal.

Esta problemática adquirió especial relevancia al verificarse que las sentencias examinadas presentaron resultados diferentes ante estructuras fácticas semejantes. En algunos casos, los titulares fueron condenados debido a que la recepción del dinero estuvo acompañada de retiros inmediatos, uso de tarjeta y clave, conversión de fondos en criptomonedas o aceptación de los cargos. En otro caso, pese a encontrarse acreditado que el dinero ingresó a la cuenta de la procesada, no se individualizó a la persona que realizó el retiro ni se incorporaron imágenes, ubicación o registros técnicos suficientes, lo que determinó la permanencia de duda razonable y la emisión de una sentencia absolutoria.

En ese contexto, la investigación formuló como problema general la siguiente interrogante: ¿cómo atribuyen los órganos jurisdiccionales penales del distrito judicial de Ayacucho responsabilidad penal al titular de la cuenta receptora del dinero fraudulentamente transferido, frente a la intervención de sujetos no identificados en la manipulación del sistema informático, en el delito de fraude informático, durante el periodo 2022-2024?

A partir del problema general se formularon tres problemas específicos. El primero estuvo referido a los criterios jurídicos empleados para calificar al titular como autor o coautor

cuando se alegó la intervención de sujetos no identificados. El segundo examinó los elementos probatorios utilizados para acreditar el conocimiento y la voluntad del titular. El tercero analizó la incidencia de la falta de individualización de los ejecutores técnicos en la motivación de la responsabilidad penal.

El objetivo general consistió en analizar la forma en que los órganos jurisdiccionales penales del distrito judicial de Ayacucho atribuyeron responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados, durante el periodo 2022-2024. Los objetivos específicos estuvieron orientados a identificar los criterios jurídicos utilizados para calificar la intervención del titular, examinar los elementos probatorios empleados para acreditar el conocimiento y la voluntad, y analizar la incidencia de la falta de individualización de los demás participantes en la motivación judicial.

La investigación se justificó teóricamente porque permitió aplicar las categorías de autoría, coautoría, complicidad, dominio funcional del hecho y prueba indiciaria a una modalidad delictiva caracterizada por la distribución de funciones. Asimismo, permitió diferenciar la conexión objetiva producida por la titularidad de la cuenta de la atribución subjetiva que exige conocimiento y voluntad de participar en el fraude.

Desde el punto de vista jurídico, el estudio fue relevante porque la persecución eficaz del fraude informático debe ser compatible con la presunción de inocencia, el principio de responsabilidad por el hecho propio y el deber constitucional de motivación. La necesidad de enfrentar la ciberdelincuencia no justifica que la responsabilidad penal se determine únicamente porque el dinero ingresó a una cuenta registrada a nombre del procesado. Toda condena requiere prueba de cargo suficiente y una explicación clara del razonamiento que vincula los hechos acreditados con la conclusión sobre la participación dolosa.

La justificación práctica radicó en la posibilidad de sistematizar criterios útiles para jueces, fiscales, abogados y peritos. La identificación de los elementos de mayor valor

probatorio puede orientar la obtención temprana de imágenes de cajeros, registros de acceso, direcciones IP, dispositivos, ubicación, comunicaciones y metadatos. También puede contribuir a que las sentencias diferencien expresamente la trazabilidad bancaria de la atribución penal.

Metodológicamente, el estudio adoptó un enfoque cualitativo, de tipo básico, nivel descriptivo-interpretativo y diseño de estudio de casos múltiples. La muestra documental estuvo conformada por cinco sentencias emitidas por juzgados penales unipersonales del distrito judicial de Ayacucho entre 2022 y 2024. Cuatro decisiones fueron condenatorias y una absolutoria; tres condenas se emitieron mediante conclusión anticipada y dos decisiones fueron dictadas después de un juicio contradictorio.

La muestra personal estuvo integrada por nueve participantes seleccionados intencionalmente por su experiencia en casos de fraude informático: tres jueces penales unipersonales, tres fiscales penales, dos abogados penalistas y un perito informático forense. Se emplearon el análisis documental y la entrevista semiestructurada como técnicas de recolección de información. Los instrumentos fueron una ficha de análisis documental y una guía de entrevista compuesta por nueve preguntas abiertas.

La información fue organizada mediante tres categorías apriorísticas. La primera estuvo referida al valor jurídico-probatorio de la titularidad, la recepción de los fondos y los actos posteriores de disposición. La segunda comprendió la valoración de la intervención de sujetos no identificados y de las hipótesis alternativas de pérdida, préstamo, suplantación o utilización no autorizada. La tercera se vinculó con la construcción y motivación de la inferencia probatoria entre el titular registral y el titular que actuó con conocimiento y voluntad. Durante el análisis emergió la subcategoría del préstamo remunerado o “alquiler” de cuentas.

Los resultados mostraron que la titularidad y la recepción del dinero constituyeron elementos de vinculación inicial, pero no resultaron suficientes para acreditar responsabilidad

penal. La disposición personalmente atribuible presentó mayor fuerza probatoria, especialmente cuando estuvo acompañada de control de la tarjeta y clave, proximidad temporal, aprovechamiento económico y evidencia técnica. También se determinó que la mención genérica de una actuación coordinada con sujetos no identificados no sustituye la prueba del acuerdo ni del aporte consciente.

La comparación entre las sentencias contradictorias evidenció que la diferencia decisiva estuvo en la individualización del acto de disposición. Cuando no se acreditó quién retiró el dinero ni se incorporaron elementos técnicos suficientes, subsistió la duda razonable. Cuando se demostraron retiros presenciales con tarjeta y clave y se descartó razonadamente la hipótesis de pérdida, la cadena indiciaria sustentó la condena.

La investigación se estructuró en seis capítulos. El capítulo I desarrolló la realidad problemática, la formulación de los problemas, los objetivos, la justificación y las delimitaciones. El capítulo II presentó los antecedentes, las bases teóricas, el marco normativo y las definiciones conceptuales. El capítulo III expuso las categorías, subcategorías e indicadores. El capítulo IV describió el enfoque, diseño, muestra, técnicas, instrumentos, procedimiento, rigor científico y consideraciones éticas. El capítulo V presentó y trianguló los resultados documentales y testimoniales. Finalmente, el capítulo VI discutió los hallazgos frente a los antecedentes, las bases teóricas y el marco jurídico, seguido de las conclusiones, recomendaciones, bibliografía y anexos.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

El delito de fraude informático, previsto en el artículo 8 de la Ley N.º 30096, presenta en su ejecución una estructura criminal frecuentemente colectiva, en la que intervienen, por un lado, sujetos con conocimientos técnicos suficientes para manipular el sistema informático de la entidad financiera o diseñar la página web fraudulenta empleada para captar los datos de la víctima, y, por otro lado, el titular de la cuenta bancaria hacia la cual se dirige finalmente el dinero sustraído. En la práctica judicial del distrito judicial de Ayacucho, resulta recurrente que el primer grupo de sujetos —a quienes se atribuye la manipulación técnica propiamente dicha— nunca llegue a ser identificado ni sometido a proceso, mientras que la persecución penal se concentra exclusivamente en el titular de la cuenta receptora, quien sí resulta plenamente identificable a través de la información bancaria.

Esta circunstancia se advierte de manera expresa en el propio relato fáctico de tres de las cinco sentencias que integran la muestra documental de la presente línea de investigación. En el expediente N.º 02815-2019-9-0501-JR-PE-06, se imputó al acusado Tello Vela haber actuado "en coordinación con otros sujetos no identificados" para manipular el sistema informático del Banco de la Nación. En el expediente N.º 01342-2022-33-0501-JR-PE-04, se atribuyó a la acusada Aspajo Laulate su intervención en calidad de coautora, precisándose expresamente que fueron "personas no identificadas" quienes realizaron la manipulación técnica del sistema del Banco BBVA, mientras que a la acusada se le imputó haber facilitado su cuenta para beneficiarse del fraude. De manera similar, en el expediente N.º 00724-2020-83-0501-JR-PE-06, se imputó a la acusada Guerra Manihuari haberse "puesto de acuerdo con tercero no identificado" para la manipulación del sistema informático del Banco de la Nación.

Resulta especialmente relevante para el planteamiento del problema que estos dos últimos expedientes, pese a compartir una estructura fáctica sustancialmente similar —la imputación de una coordinación con un tercero no identificado que ejecutó materialmente la manipulación informática—, hayan culminado en resultados diametralmente opuestos: mientras que en el expediente N.º 01342-2022-33 el órgano jurisdiccional condenó a la acusada como coautora, sustentando dicha calificación en un conjunto de indicios que, en su conjunto, permitían inferir razonablemente su conocimiento y participación voluntaria en el fraude, en el expediente N.º 00724-2020-83 el mismo tipo de imputación culminó en absolución, al considerar el juzgador que las pruebas actuadas no permitían establecer con la certeza exigida

que la acusada hubiera tenido participación o conocimiento efectivo de la operación, ni que hubiera sido ella quien materialmente dispuso del dinero transferido a su cuenta.

Esta disparidad de resultados ante una estructura de imputación fácticamente análoga —la alegación de un tercero no identificado como ejecutor material de la manipulación informática— evidencia la existencia de un problema jurídico de primer orden: la necesidad de determinar con claridad cuáles son los criterios, jurídicos y probatorios, que permiten atribuir válidamente responsabilidad penal al titular de una cuenta receptora cuando la persona que ejecutó materialmente el acceso o la manipulación del sistema informático no ha sido identificada ni sometida a proceso, sin que ello vulnere el derecho a la presunción de inocencia del titular de la cuenta, quien podría, en determinados casos, ser también víctima de la utilización no consentida de sus propios datos o cuentas bancarias por parte de terceros.

A ello se suma que, en los expedientes en los que no se invoca la intervención de terceros no identificados —como el expediente N.º 00477-2023-59-0501-JR-PE-04, en el que el propio acusado Cuadra Pinedo diseñó personalmente la página web fraudulenta empleada para captar los datos de la víctima, o el expediente N.º 01263-2019-33-0501-JR-PE-05, en el que se identificó y procesó a dos coimputados plenamente individualizados—, la estructura de la imputación y su motivación resultan considerablemente menos complejas, lo que sugiere que la presencia de un tercero no identificado constituye, en sí misma, un factor que incrementa significativamente la exigencia argumentativa que recae sobre el juzgador al momento de motivar la atribución de responsabilidad penal al titular de la cuenta.

En este contexto, la presente investigación se propone analizar, a partir del estudio de las sentencias emitidas por los órganos jurisdiccionales penales de Ayacucho durante el periodo 2022-2024, los criterios jurídicos y probatorios empleados para atribuir responsabilidad penal al titular de la cuenta receptora del dinero fraudulentamente transferido, en aquellos supuestos en los que se alega la intervención de sujetos no identificados en la manipulación del sistema informático, con la finalidad de sistematizar dichos criterios y contribuir a una motivación judicial más rigurosa, predecible y respetuosa de las garantías del debido proceso en esta modalidad delictiva.

1.2. Formulación del problema

1.2.1. Problema general

¿Cómo atribuyen los órganos jurisdiccionales penales del distrito judicial de Ayacucho responsabilidad penal al titular de la cuenta receptora del dinero fraudulentamente transferido, frente a la intervención de sujetos no identificados en la manipulación del sistema informático, en el delito de fraude informático, durante el periodo 2022-2024?

1.2.2. Problemas específicos

1. ¿Qué criterios jurídicos emplean los órganos jurisdiccionales penales de Ayacucho para calificar el grado de intervención delictiva —autoría o coautoría— del titular de la cuenta receptora en el delito de fraude informático, cuando se alega la intervención de sujetos no identificados en la manipulación del sistema informático?

2. ¿Qué elementos probatorios permiten a los órganos jurisdiccionales penales de Ayacucho acreditar el conocimiento y la voluntad del titular de la cuenta receptora de participar en el fraude informático, ante la falta de individualización de los sujetos que ejecutaron materialmente la manipulación del sistema informático?

3. ¿Cómo incide la falta de individualización de los sujetos que intervinieron en la manipulación del sistema informático en la motivación de la responsabilidad penal atribuida al titular de la cuenta receptora en las sentencias por el delito de fraude informático emitidas en el distrito judicial de Ayacucho?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Analizar la forma en que los órganos jurisdiccionales penales del distrito judicial de Ayacucho atribuyen responsabilidad penal al titular de la cuenta receptora del dinero fraudulentamente transferido, frente a la intervención de sujetos no identificados en la manipulación del sistema informático, en el delito de fraude informático, durante el periodo 2022-2024.

1.3.2. Objetivos específicos

1. Identificar los criterios jurídicos que emplean los órganos jurisdiccionales penales de Ayacucho para calificar el grado de intervención delictiva —autoría o

coautoría— del titular de la cuenta receptora en el delito de fraude informático, cuando se alega la intervención de sujetos no identificados en la manipulación del sistema informático.

2. Examinar los elementos probatorios que permiten a los órganos jurisdiccionales penales de Ayacucho acreditar el conocimiento y la voluntad del titular de la cuenta receptora de participar en el fraude informático, ante la falta de individualización de los sujetos que ejecutaron materialmente la manipulación del sistema informático.

3. Analizar la incidencia de la falta de individualización de los sujetos que intervinieron en la manipulación del sistema informático en la motivación de la responsabilidad penal atribuida al titular de la cuenta receptora en las sentencias por el delito de fraude informático emitidas en el distrito judicial de Ayacucho.

1.4. Justificación de la investigación

1.4.1. Justificación teórica

La investigación se justificó teóricamente porque permitió profundizar en la aplicación de las categorías dogmáticas de autoría, coautoría y participación en el ámbito del fraude informático. Esta modalidad delictiva presenta una estructura frecuentemente fragmentada, en la que el sujeto que realiza la manipulación técnica del sistema informático puede ser distinto de la persona que proporciona la cuenta receptora, controla los medios de acceso o dispone posteriormente del dinero transferido.

En ese contexto, el estudio examinó los presupuestos que permitieron atribuir responsabilidad penal al titular de la cuenta receptora cuando los ejecutores materiales de la manipulación informática no fueron identificados. La investigación permitió establecer que la titularidad registral y la recepción del dinero constituyeron hechos objetivos de vinculación, pero no demostraron por sí mismos la existencia de un acuerdo común, un aporte esencial ni el conocimiento del origen ilícito de los fondos.

Asimismo, el estudio contribuyó al desarrollo de la teoría de la prueba indiciaria aplicada a la criminalidad informática. Se examinó la secuencia argumentativa que permitió

pasar de hechos indicadores —como la titularidad, la recepción, el control de la tarjeta y clave, la proximidad temporal y los actos posteriores de disposición— a la conclusión sobre el conocimiento y la voluntad del titular. Con ello, se precisó la diferencia entre la trazabilidad financiera del dinero y la atribución penal individual.

La investigación también aportó una sistematización de los criterios utilizados para distinguir entre el titular meramente registral, el titular cuya cuenta fue utilizada sin autorización y el titular que intervino conscientemente en el circuito fraudulento. Esta distinción resultó necesaria para evitar formas de responsabilidad objetiva incompatibles con la presunción de inocencia y el principio de responsabilidad penal por el hecho propio.

1.4.2. Justificación práctica

La investigación se justificó desde el punto de vista práctico porque abordó una dificultad recurrente en la investigación y el juzgamiento del fraude informático en el distrito judicial de Ayacucho. En estos casos, las entidades financieras permiten identificar con relativa facilidad al titular de la cuenta receptora, mientras que las personas que captaron las credenciales, manipularon el sistema o ejecutaron las transferencias frecuentemente permanecen sin identificar.

Los resultados proporcionaron criterios útiles para la actuación de fiscales, jueces, abogados defensores y peritos informáticos. Para el Ministerio Público, el estudio permitió identificar las diligencias necesarias para diferenciar la titularidad registral del control efectivo de la cuenta, como la obtención de imágenes de cajeros, ubicación de operaciones, registros de acceso, direcciones IP, dispositivos vinculados, comunicaciones, mecanismos de autenticación y destino posterior del dinero.

Para los órganos jurisdiccionales, la investigación ofreció una estructura destinada a mejorar la motivación de las sentencias. Esta estructura comprende la identificación del hecho registral, los hechos indicadores, la regla inferencial aplicada, el contraste de las hipótesis

alternativas y la conclusión sobre el conocimiento y la voluntad. Su aplicación puede contribuir a reducir los saltos inferenciales y las decisiones sustentadas únicamente en la titularidad bancaria.

Para la defensa técnica, el estudio permitió reconocer la importancia de plantear y corroborar oportunamente las hipótesis de pérdida, préstamo, suplantación de identidad o utilización no autorizada de la cuenta. También evidenció la necesidad de solicitar diligencias técnicas desde las primeras etapas del proceso, evitando que la estrategia defensiva se limite a la sola negación de los hechos.

1.4.3. Justificación jurídica

La investigación se justificó jurídicamente porque la persecución penal del fraude informático debe realizarse respetando la presunción de inocencia, el derecho de defensa y el deber constitucional de motivación de las resoluciones judiciales. La necesidad de enfrentar eficazmente la ciberdelincuencia no permite atribuir responsabilidad a una persona por la sola circunstancia de que el dinero fraudulentamente transferido haya ingresado a una cuenta registrada a su nombre.

El artículo 2, inciso 24, literal e, de la Constitución Política reconoce la presunción de inocencia, mientras que el artículo 139, inciso 5, establece el deber de motivación de las resoluciones judiciales. En concordancia con estas disposiciones, el artículo 394, numeral 3, del Código Procesal Penal exige una motivación clara, lógica y completa de los hechos considerados probados o improbadados y del razonamiento que sustenta la decisión.

Por ello, resultó necesario examinar si las sentencias individualizaron el aporte del titular, acreditaron los elementos objetivos y subjetivos de su intervención y explicaron la regla inferencial utilizada. La investigación permitió determinar que la intervención de sujetos no identificados no impide necesariamente la condena del titular, pero incrementa la exigencia de corroboración y motivación.

Asimismo, el estudio fue relevante para la aplicación de los artículos 23 a 25 del Código Penal, referidos a la autoría, coautoría y complicidad. Los resultados permitieron advertir que la calificación del titular como coautor exige acreditar un aporte funcional consciente y no únicamente su vinculación bancaria con el dinero transferido.

1.4.4. Justificación metodológica

La investigación se justificó metodológicamente porque desarrolló un procedimiento cualitativo que integró el análisis documental de sentencias y las entrevistas semiestructuradas a operadores jurídicos y a un especialista técnico. Esta combinación permitió contrastar el razonamiento exteriorizado en las resoluciones judiciales con la experiencia de quienes intervienen en la investigación, juzgamiento, defensa y análisis pericial del fraude informático.

La categorización apriorística permitió organizar la información en tres ejes: el valor probatorio de la titularidad, recepción y disposición; la intervención de sujetos no identificados y las hipótesis alternativas; y la construcción de la inferencia entre titularidad registral y responsabilidad penal. Durante el análisis también se incorporó la subcategoría emergente relativa al préstamo remunerado o alquiler de cuentas.

La triangulación de cinco sentencias y nueve entrevistas fortaleció la credibilidad de los hallazgos. Además, la ficha de análisis documental y la guía de entrevista pueden ser adaptadas y utilizadas en futuras investigaciones sobre cuentas receptoras, fraude informático, suplantación de identidad u otras modalidades de criminalidad digital con pluralidad de intervinientes.

1.4.5. Justificación social

La investigación se justificó socialmente porque el fraude informático afecta el patrimonio, la confianza en los sistemas financieros y la seguridad de las operaciones digitales. Su incremento perjudica especialmente a personas que no cuentan con conocimientos técnicos

suficientes para identificar enlaces falsos, suplantaciones de identidad o mecanismos fraudulentos de obtención de credenciales.

Al mismo tiempo, la investigación consideró que el titular de una cuenta receptora también puede ser víctima de la utilización no autorizada de sus datos o instrumentos bancarios. Por tanto, una respuesta penal adecuada debe proteger a las víctimas de las transferencias fraudulentas sin generar condenas basadas en presunciones automáticas contra quienes aparecen formalmente como titulares de las cuentas receptoras.

Los resultados contribuyeron a promover decisiones más rigurosas, predecibles y respetuosas de los derechos fundamentales. De esta manera, el estudio buscó fortalecer tanto la eficacia de la persecución penal como la legitimidad del sistema de justicia frente a la criminalidad informática.

1.5. Delimitación de la investigación

1.5.1. Delimitación temática

La investigación se delimitó al análisis de la atribución de responsabilidad penal al titular de la cuenta bancaria receptora del dinero obtenido mediante fraude informático. El estudio examinó los supuestos en los que se alegó la intervención de sujetos no identificados en la captación de datos, manipulación del sistema o ejecución de la transferencia.

El análisis se concentró en los criterios jurídicos aplicados para calificar la autoría o coautoría, los elementos probatorios utilizados para acreditar conocimiento y voluntad, y la motivación judicial que permitió distinguir al titular meramente registral del titular que intervino conscientemente en el hecho.

No se estudiaron de manera autónoma otras modalidades de ciberdelincuencia, como el acceso ilícito, atentado contra la integridad de sistemas informáticos, interceptación de datos, proposiciones sexuales a menores o suplantación de identidad, salvo cuando resultaron necesarias para comprender el mecanismo de ejecución del fraude informático.

1.5.2. Delimitación espacial

La investigación se desarrolló en el distrito judicial de Ayacucho. La muestra documental estuvo constituida por sentencias emitidas por los juzgados penales unipersonales de la Corte Superior de Justicia de Ayacucho, con sede en la provincia de Huamanga.

Las entrevistas fueron aplicadas a jueces penales, fiscales penales, abogados penalistas y un perito informático forense con ejercicio profesional o experiencia relevante en el ámbito del distrito judicial de Ayacucho.

1.5.3. Delimitación temporal

La investigación comprendió las sentencias emitidas durante el periodo 2022-2024. Este intervalo permitió examinar decisiones recientes relacionadas con la aplicación del artículo 8 de la Ley N.º 30096 y comparar sentencias condenatorias y absolutorias.

Aunque algunos hechos delictivos analizados ocurrieron antes del periodo señalado, el criterio de delimitación temporal estuvo determinado por el año de emisión de la sentencia y no por la fecha de comisión del hecho investigado.

Las entrevistas fueron realizadas durante el periodo de ejecución de la investigación, con la finalidad de recoger criterios profesionales vinculados con la experiencia acumulada en casos de fraude informático.

1.5.4. Delimitación poblacional

La población documental estuvo integrada por las sentencias emitidas por el delito de fraude informático en el distrito judicial de Ayacucho durante el periodo 2022-2024, en las que una persona fue procesada por su condición de titular de una cuenta receptora.

La muestra documental estuvo conformada intencionalmente por cinco sentencias. Cuatro fueron condenatorias y una absolutoria; tres condenas se dictaron mediante conclusión anticipada y dos decisiones fueron emitidas después de juicio contradictorio.

La población personal comprendió a operadores jurídicos y especialistas con experiencia en casos de fraude informático. La muestra estuvo integrada por nueve participantes: tres jueces penales unipersonales, tres fiscales penales, dos abogados penalistas y un perito informático forense.

1.5.5. Delimitación documental

El análisis se circunscribió al contenido escrito de las cinco sentencias seleccionadas y a las respuestas obtenidas mediante las entrevistas semiestructuradas. Las sentencias fueron examinadas en relación con la imputación, los hechos acreditados, los medios probatorios valorados, las hipótesis alternativas, la calificación jurídica y la motivación de la decisión.

No se analizaron íntegramente las carpetas fiscales, los expedientes judiciales, las grabaciones de audiencias ni los archivos técnicos que no fueron incorporados o descritos en las sentencias. En consecuencia, el estudio evaluó principalmente la prueba y el razonamiento exteriorizados en las resoluciones judiciales.

CAPÍTULO II: MARCO TEORICO

2.1. Antecedentes de la investigación

2.2.1. Antecedentes internacionales

Rodríguez Pilco, K. K., & Chimborazo Castillo, L. A. (2026). Responsabilidad penal por criminalidad organizada en entornos digitales. Los autores desarrollaron un estudio de enfoque cualitativo y documental orientado a analizar críticamente el marco normativo ecuatoriano frente a la criminalidad organizada que opera en entornos digitales, examinando las capacidades institucionales del sistema penal y los desafíos que plantea la tecnología en la persecución del delito organizado digital. Concluyeron que persisten limitaciones normativas, técnicas y operativas relevantes en el ordenamiento ecuatoriano, entre ellas la insuficiente regulación de conductas digitales complejas, las dificultades en el manejo y valoración de la evidencia digital, y la escasez de operadores de justicia especializados, factores que en conjunto obstaculizan la atribución efectiva de responsabilidad penal y favorecen escenarios de impunidad.

Este antecedente resulta pertinente porque confirma, desde la realidad ecuatoriana, que la dificultad para atribuir responsabilidad penal en la criminalidad digital no es un problema exclusivo del distrito judicial de Ayacucho, sino un fenómeno regional vinculado estructuralmente a la naturaleza técnica de este tipo de delitos. El énfasis de los autores en las dificultades de valoración de la evidencia digital dialoga directamente con la categoría de elementos de convicción de la presente investigación.

Manobanda Guangasi, N. A., & Chiriboga Sabando, D. V. (2026). Impacto de la Tecnología en la Criminalidad en el Ecuador: Reflexión Crítica Sobre la Mutación del Fenómeno Delictivo y el Desafío de la Ciberseguridad Jurídica. El artículo examinó el rol dual de la tecnología en el fenómeno criminal ecuatoriano, tanto como instrumento delictivo —particularmente en el fraude informático y la suplantación de identidad— como herramienta

de control y prevención. Los autores identificaron a la cadena de custodia digital como el eslabón más débil del proceso penal contemporáneo, y sostuvieron que el marco jurídico vigente, pese a contar con normativa específica, carece de la velocidad y especialización necesarias para enfrentar una amenaza en constante evolución.

El señalamiento de la cadena de custodia digital como el punto más vulnerable del proceso penal resulta directamente relevante para la presente investigación, en la medida en que la solidez de dicha cadena determina, en gran medida, la posibilidad de acreditar los actos de disposición del dinero que la presente investigación identificó como el hecho discriminante entre el titular meramente registral y el titular con responsabilidad penal.

Catagua Zambrano, D. J., & Vera Navarrete, D. S. (2026). Análisis comparativo de herramientas digitales forenses con IA en el marco de los delitos informáticos en Ecuador. Mediante un diseño mixto, los autores compararon el rendimiento de tres herramientas forenses digitales potenciadas con inteligencia artificial, aplicadas al procesamiento de una imagen forense estandarizada, complementado con una encuesta a profesionales del sector. Encontraron diferencias relevantes en velocidad, automatización y capacidad de recuperación de evidencia entre las herramientas evaluadas, y advirtieron una brecha formativa crítica, pues el 75 % de los profesionales encuestados utiliza dichas herramientas solo ocasionalmente. Este antecedente aporta una perspectiva estrictamente técnica que enriquece la comprensión de las limitaciones periciales identificadas en la presente investigación, particularmente respecto de la categoría de elementos de convicción, evidenciando que la insuficiencia del desarrollo pericial informático observada en los procesos judiciales de Ayacucho no obedece únicamente a factores normativos, sino también a una brecha de capacitación técnica generalizada en la región.

Alvear Richards, G. E., & Hernández Pesantes, E. A. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos.

Las autoras realizaron un análisis comparado entre la Ley Orgánica de Protección de Datos Personales del Ecuador y la legislación peruana equivalente, examinando la tipificación de los delitos informáticos en ambos países desde una perspectiva de seguridad de la información, y proponiendo recomendaciones orientadas a garantizar el cumplimiento normativo y la protección efectiva del titular del dato personal. El estudio permite contextualizar, desde el derecho comparado, el marco normativo peruano en el que se inserta el delito de fraude informático analizado en la presente investigación, evidenciando semejanzas y diferencias regulatorias con un país de la región que enfrenta desafíos estructuralmente similares en materia de ciberdelincuencia.

2.2.2. Antecedentes Nacionales

Becerra Cervera, N. A. (2025). Una mirada a la problemática de los delitos informáticos y su afectación directa sobre las cuentas digitales bancarias en el Perú, 2022.

El autor desarrolló una investigación de enfoque cualitativo, básico, descriptivo y fenomenológico, orientada a analizar la relación entre la regulación de los delitos informáticos y la protección de la sociedad frente a estos ilícitos, empleando la entrevista como técnica y aplicándola a profesionales del derecho penal y a integrantes de la división de delitos informáticos de la Policía Nacional del Perú. Concluyó que, pese a la existencia de tipos penales específicos, persiste ambigüedad en su regulación y penas insuficientes, lo que deriva en sentencias poco efectivas frente a la afectación del patrimonio personal a través de cuentas bancarias digitales. Este es el antecedente nacional más cercano a la presente investigación, tanto por su enfoque metodológico cualitativo basado en entrevistas a operadores jurídicos y policiales, como por su objeto de estudio centrado en la afectación de cuentas bancarias

mediante fraude informático. Sus hallazgos sobre la insuficiencia de la regulación vigente respaldan la necesidad de examinar, con mayor especificidad, los criterios judiciales concretos para atribuir responsabilidad penal al titular de la cuenta receptora, aspecto que dicho estudio no abordó en profundidad y que constituye el objeto central de la presente tesis.

Rosales Medina, R. M. (2025). Incremento de los delitos informáticos y su problemática con la impunidad delictiva en Lima, 2024. La investigación, de enfoque cuantitativo, no experimental y de tipo correlacional, tuvo como objetivo determinar la relación entre el incremento de los delitos informáticos y la impunidad delictiva en Lima. Mediante el coeficiente Rho de Spearman, la autora obtuvo un valor de 0.821, que evidenció una relación directa y positiva alta entre ambas variables, concluyendo que el carácter anónimo del ciberespacio constituye el factor preponderante que impide la individualización del sujeto activo y conduce al archivamiento de la mayoría de las denuncias. Aunque de enfoque cuantitativo, distinto al de la presente investigación, este antecedente resulta relevante porque acredita empíricamente, a nivel de Lima Metropolitana, que el anonimato propio del entorno digital constituye la causa estructural de la impunidad en los delitos informáticos. Dicho hallazgo refuerza la pertinencia de estudiar, específicamente, cómo los órganos jurisdiccionales logran superar dicho anonimato para atribuir responsabilidad penal al único sujeto identificable en la cadena delictiva: el titular de la cuenta receptora del dinero.

Chávez Martínez, I. F., & Ruiz Valer, A. M. (2026). Análisis de la individualización del imputado en la persecución del delito de proposiciones a menores con fines sexuales por medios tecnológicos en la fiscalía de Ciberdelincuencia de Arequipa 2023. Las autoras examinaron las dificultades que enfrenta la Fiscalía Especializada en Ciberdelincuencia de Arequipa para individualizar a los presuntos autores de proposiciones sexuales a menores cometidas a través de medios tecnológicos, atendiendo a la complejidad técnica y legal de la obtención de pruebas digitales y al anonimato que facilita la reiteración de estas conductas.

Formularon recomendaciones orientadas a fortalecer el marco institucional y técnico de dicha fiscalía especializada. Este antecedente, aunque referido a un tipo penal distinto, resulta metodológicamente análogo a la presente investigación por abordar, en un distrito judicial vecino y en el mismo periodo temporal, la problemática de la individualización del responsable en delitos cometidos mediante medios tecnológicos y bajo condiciones de anonimato digital. Ello confirma que la dificultad de individualización no es exclusiva del fraude informático, sino un obstáculo transversal a distintos tipos penales que se cometen a través de las tecnologías de la información en el sur y centro del país.

Quincho Laura, R. S., Aylas Dionicio, J. F., & Arcos Huayhua, J. (2025). Aplicación del convenio de Budapest en la ley de delitos informáticos del Perú, Cusco 2024. Mediante un enfoque mixto que combinó cuestionarios dirigidos a especialistas del Ministerio Público, la Policía Nacional y abogados penalistas de Cusco con entrevistas semiestructuradas, los autores compararon la aplicación del Convenio de Budapest con la Ley N.º 30096, identificando vacíos normativos relevantes, entre ellos una regulación insuficiente del fraude informático y la suplantación de identidad frente a los estándares internacionales, así como deficiencias en la cooperación internacional y en la preservación de pruebas digitales. El hallazgo específico sobre la regulación insuficiente del fraude informático frente a los estándares del Convenio de Budapest constituye un antecedente normativo directo para la presente investigación, en la medida en que evidencia que las dificultades probatorias identificadas en las sentencias de Ayacucho podrían estar vinculadas a limitaciones más amplias del propio diseño legislativo del tipo penal contenido en el artículo 8 de la Ley N.º 30096.

Ventura Quijano, M. A. (2021). La tipificación del Phishing, Smishing y Vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima,

2020. La autora analizó el origen y desarrollo de la Ley de Delitos Informáticos N.º 30096 y su modificatoria, la Ley N.º 30171, en el marco de su incorporación de los estándares del Convenio de Budapest mediante la Resolución Legislativa N.º 30913, examinando las modalidades de phishing, smishing y vishing como mecanismos frecuentes de obtención fraudulenta de datos informáticos y de suplantación de identidad.

Este antecedente resulta útil para la fundamentación normativa de la presente investigación, en la medida en que describe con precisión el mecanismo técnico del *phishing* —modalidad identificada en las cinco sentencias que integran la muestra documental del presente estudio— como antecedente fáctico habitual de las transferencias fraudulentas dirigidas a la cuenta del titular investigado.

Hidalgo Coronel, C. N., & Solano Vidal, G. S. (2021). El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. Propuesta de incorporación del artículo 7-A en la Ley de Delitos Informáticos 30096. Los autores identificaron modalidades específicas de phishing que no resultan subsumibles en ninguno de los tipos penales previstos actualmente en la Ley de Delitos Informáticos, lo que, a su criterio, genera espacios de impunidad y dificulta la labor persecutoria del Ministerio Público. A partir de dicho diagnóstico, formularon una propuesta legislativa orientada a incorporar un artículo específico que regule de manera integral las distintas modalidades de ejecución de esta conducta. Este antecedente aporta un análisis de lege ferenda que complementa la perspectiva eminentemente aplicativa de la presente investigación, permitiendo distinguir entre las dificultades derivadas de vacíos legislativos en la tipificación del phishing y las dificultades derivadas específicamente de la valoración judicial de la prueba para atribuir responsabilidad al titular de la cuenta receptora, que constituye el objeto central del presente estudio.

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. El autor examinó específicamente los delitos de fraude informático

y suplantación de identidad regulados en el artículo 8 de la Ley N.º 30096, en el contexto de la consolidación de las operaciones comerciales virtuales y las transferencias a través de monederos digitales, analizando su vinculación con la criminalidad económica y destacando el carácter pluriofensivo de estas conductas. Este antecedente constituye una fuente doctrinal directa sobre el tipo penal materia de la presente investigación, pues desarrolla con precisión los elementos típicos del fraude informático y su relación con las modalidades de phishing y pharming, fundamento dogmático indispensable para el análisis de la atribución de responsabilidad penal desarrollado en el presente estudio.

Leyva Serrano, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. La autora realizó un estudio dogmático-doctrinario orientado a establecer la realidad jurídica de los delitos informáticos en el Perú en armonía con la política criminal preventiva, protectora y garantista diseñada por la Constitución, recomendando reformular los fundamentos dogmáticos de estos delitos a partir de la doctrina y la experiencia nacional. Este antecedente aporta el sustento dogmático general sobre la tipificación de los delitos informáticos en el Perú y su relación con los convenios internacionales, marco conceptual necesario para situar adecuadamente el análisis específico sobre la atribución de responsabilidad penal desarrollado en la presente investigación.

2.2. Bases teóricas

2.2.1. El delito informático: concepto, naturaleza y características

2.2.1.1. Concepciones amplia, intermedia y restringida

La doctrina penal no ha alcanzado un consenso unívoco sobre el concepto de delito informático, existiendo distintas aproximaciones que reflejan la complejidad del fenómeno. Villavicencio Terreros (2014, como se citó en Vinelli Vereau, 2021) sostiene que la criminalidad informática comprende las conductas dirigidas a burlar los sistemas de seguridad mediante el acceso no autorizado a computadoras, correos o bases de datos a través de una clave de acceso, precisando que se trata de conductas típicas que únicamente pueden cometerse

mediante el uso de la tecnología. En un sentido amplio, esta definición abarca todas aquellas conductas en las que las tecnologías de la información y la comunicación constituyen el objetivo, el medio o el lugar de ejecución del hecho, con independencia del bien jurídico afectado.

Una segunda aproximación es ofrecida por Rayón Ballesteros y Gómez Hernández (2014, como se citó en Vinelli Vereau, 2021), quienes conciben el ciberdelito como cualquier infracción punible en la que interviene un equipo informático o internet, ya sea como instrumento para la comisión del delito o como objeto material de este. Por su parte, Davara (1993, como se citó en Vinelli Vereau, 2021) define los delitos informáticos como aquellas acciones que, reuniendo las características que delimitan el concepto general de delito, se ejecutan utilizando un elemento informático o vulnerando los derechos de su titular, ya sea a nivel de hardware o de software.

Frente a estas posiciones amplias, Morillas Fernández (2017, como se citó en Vinelli Vereau, 2021) distingue tres concepciones doctrinales: la concepción amplia, que considera delito informático a cualquier figura penal cometida mediante el empleo de una computadora; la posición intermedia, que exige que el sistema informático constituya el objeto material o el instrumento del delito; y la concepción restringida, que define el delito informático como todo acto ilegal que exige el conocimiento de la tecnología informática para su perpetración, investigación y persecución, otorgándole así una autonomía típica frente a los delitos comunes cometidos por medios tecnológicos.

Para efectos de la presente investigación, se adopta la concepción restringida del delito informático, en la medida en que el fraude informático regulado en el artículo 8 de la Ley N.º 30096 exige, precisamente, un conocimiento técnico específico para la manipulación del sistema informático de la entidad financiera, lo que lo diferencia de otros delitos patrimoniales que simplemente emplean un medio tecnológico de manera incidental, como podría ocurrir con una estafa concertada por mensajería instantánea sin manipulación alguna del sistema.

2.2.1.2. Características propias de la criminalidad informática

Morillas Fernández (2017, como se citó en Vinelli Vereau, 2021) ha sistematizado un conjunto de características que distinguen a la criminalidad informática de la delincuencia tradicional. La primera de ellas es la ejecución a distancia, sin contacto físico entre el agresor y la víctima, lo que determina una separación temporal y espacial que dificulta la aprehensión

inmediata del responsable y exige mecanismos probatorios distintos a los empleados en los delitos de ejecución presencial.

Una segunda característica es la naturaleza transfronteriza de esta tipología criminal, inherente a la propia esencia de internet y del ciberespacio, lo que complica considerablemente las técnicas de investigación al requerir, en no pocos casos, mecanismos de cooperación judicial internacional. A ello se suma la ausencia de jerarquía en la red, que dificulta la verificación de la información que circula por este medio y la identificación de su origen.

Una tercera característica especialmente relevante para la presente investigación es el anonimato del perjuicio protegido y la facilidad para encubrir el hecho, derivada de la posibilidad de borrar huellas digitales sin dejar rastro perceptible tras la comisión del ilícito. Esta característica explica precisamente la recurrente alegación fiscal, en los procesos por fraude informático, de la intervención de sujetos no identificados que ejecutan materialmente la manipulación del sistema, mientras que la persecución penal se concentra en el titular identificable de la cuenta receptora.

Finalmente, Morillas Fernández (2017, como se citó en Vinelli Vereau, 2021) destaca la indeterminación de las víctimas, en la medida en que el sujeto activo puede ejecutar la acción ilícita sin conocer siquiera quiénes serán los destinatarios de esta, como ocurre característicamente en el phishing, modalidad que consiste en la búsqueda ilícita de datos personales mediante la suplantación de la identidad de una entidad financiera. Estas características, en conjunto, generan una elevada cifra negra de criminalidad y explican la complejidad probatoria que enfrentan los operadores jurídicos al momento de atribuir responsabilidad penal.

2.2.2. El delito de fraude informático en la legislación penal peruana

2.2.2.1. Regulación en la Ley N.º 30096 y su modificatoria, Ley N.º 30171

El ordenamiento jurídico peruano incorporó de manera expresa el delito de fraude informático a través del artículo 8 de la Ley N.º 30096, Ley de Delitos Informáticos, publicada en octubre de 2013, posteriormente modificado por el artículo 1 de la Ley N.º 30171, publicada en marzo de 2014. Dicha norma sanciona a quien, de manera deliberada e ilegítima, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción,

alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Ya desde una perspectiva histórica, Bramont-Arias Torres (1997) advertía, incluso antes de la promulgación de una legislación especial, que la utilización creciente de las computadoras en la sociedad moderna propiciaba el surgimiento de una nueva forma de delincuencia que representaba un reto para la concepción clásica del Derecho Penal, exigiendo su estudio en relación con figuras delictivas tradicionales como la estafa, los daños y la falsificación de documentos, antes de que dicha criminalidad fuera objeto de una tipificación autónoma en nuestro ordenamiento.

Leyva Serrano (2021), por su parte, destaca la necesidad de armonizar la tipificación de los delitos informáticos en el Perú con los convenios internacionales sobre la materia, sosteniendo que la política criminal preventiva, protectora y garantista diseñada por la Constitución exige una reformulación constante de los fundamentos dogmáticos de estos delitos a la luz de la experiencia nacional y del desarrollo doctrinal comparado, en la medida en que la legislación especial debe adaptarse a la evolución tecnológica de las modalidades delictivas.

La estructura normativa vigente distingue, además, un supuesto agravado en el segundo párrafo del artículo 8, que eleva la pena cuando el fraude informático afecta el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social, lo que evidencia una valoración diferenciada del legislador según el titular del bien jurídico patrimonial afectado, distinción que resulta ajena a los casos analizados en la presente investigación, en los que las víctimas son personas naturales o jurídicas de derecho privado.

2.2.2.2. Tipicidad objetiva y subjetiva del fraude informático

Desde el plano de la tipicidad objetiva, el delito de fraude informático configura un tipo penal de sujeto activo genérico, en la medida en que la norma no exige ninguna condición o cualidad específica en quien lo comete, pudiendo ser cometido por cualquier persona que cuente con los medios técnicos o la coordinación necesaria para manipular el sistema informático. De igual manera, el sujeto pasivo resulta genérico, siendo el titular del derecho patrimonial afectado por la operación fraudulenta, sea este una persona natural, una empresa o, en el supuesto agravado, el propio Estado.

La conducta típica exige la concurrencia de una manipulación informática entendida en sentido amplio, que comprende el diseño de plataformas fraudulentas, la introducción de datos falsos, la alteración o supresión de información legítima, o cualquier otra interferencia en el funcionamiento del sistema, orientada a procurar un provecho ilícito en perjuicio de un tercero. Esta amplitud típica permite subsumir modalidades de ejecución tan diversas como el phishing, el spoofing o la manipulación directa de plataformas bancarias, todas ellas presentes en la muestra documental de la presente investigación.

En cuanto a la tipicidad subjetiva, el delito de fraude informático se configura como un tipo eminentemente doloso, excluyéndose expresamente la modalidad culposa, que resultaría atípica. La norma exige, además, que el comportamiento esté orientado por un especial ánimo de lucro (*animus lucrandi*), lo que determina que el tipo penal se estructure como un delito de tendencia interna trascendente, en el que la obtención efectiva del provecho ilícito no forma parte del tipo objetivo, pero sí orienta subjetivamente la conducta del agente desde el inicio de su ejecución.

Esta estructura típica plantea, precisamente, el problema central que aborda la presente investigación: cuando la manipulación informática es ejecutada por un sujeto no identificado y el provecho ilícito se materializa en la cuenta bancaria de un tercero, resulta necesario determinar si dicho tercero actuó con el dolo y el ánimo de lucro exigidos por el tipo penal, o si, por el contrario, se limitó a ser el instrumento o incluso la víctima adicional de una manipulación de la que no tuvo conocimiento ni participación voluntaria.

2.2.2.3. Modalidades de ejecución: phishing, smishing, vishing y spoofing

Ventura Quijano (2021) explica que el phishing constituye la modalidad matriz de las técnicas de captación fraudulenta de información personal, mediante la cual el agente diseña páginas web o comunicaciones que imitan a una entidad legítima —típicamente una entidad bancaria— con la finalidad de inducir a la víctima a proporcionar sus datos personales, claves de acceso o información financiera, que posteriormente son empleados para consumir la transferencia fraudulenta de fondos.

A partir de esta modalidad matriz se han desarrollado variantes especializadas según el canal de comunicación empleado. El smishing, conforme señala Ventura Quijano (2021), es la modalidad mediante la cual el agente activo procura obtener información privada a través de

mensajes de texto (SMS) que dirigen a la víctima hacia un sitio web fraudulento o una llamada telefónica, término que resulta de la contracción entre las siglas SMS y la voz phishing.

El vishing, por su parte, se ejecuta mediante llamadas telefónicas o correos de voz en los que el agente suplanta la identidad de una entidad bancaria o de un familiar de la víctima, utilizando contestadores automáticos o mensajes robotizados para inducirla a proporcionar información confidencial o a realizar directamente una operación financiera (Ventura Quijano, 2021). Esta modalidad guarda especial relevancia para los casos de fraude informático en los que la víctima es inducida a error mediante una comunicación telefónica que aparenta provenir de su entidad financiera.

El spoofing o suplantación de identidad, modalidad técnica identificada expresamente en una de las sentencias que integran la muestra documental de la presente investigación, consiste en la creación de una página web con las mismas características visuales de la plataforma legítima que se pretende suplantar, de modo que la víctima, al ingresar sus datos, los transmite inadvertidamente a un tercero que los utiliza para consumir la transferencia fraudulenta. Hidalgo Coronel y Solano Vidal (2021) han planteado, precisamente, la necesidad de incorporar una tipificación específica para el phishing como conducta autónoma no regulada expresamente en la Ley N.º 30096, mediante la propuesta de un artículo 7-A que sancione la fase preparatoria de captación fraudulenta de datos, con independencia de que se consume o no la posterior transferencia patrimonial.

2.2.3. El Convenio de Budapest sobre la Ciberdelincuencia y su recepción en el ordenamiento peruano

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, suscrito en Budapest en el año 2001, constituye el instrumento internacional de mayor influencia en la armonización de las legislaciones penales frente a la criminalidad informática, estableciendo estándares mínimos para la tipificación de conductas como el acceso ilícito, la interferencia en datos y sistemas, y el fraude informático, así como directrices para la cooperación internacional en materia de obtención de evidencia digital.

Quincho Laura, Aylas Dionicio y Arcos Huayhua (2025) analizan la aplicación de dicho convenio en la Ley de Delitos Informáticos del Perú, identificando que, si bien la adhesión peruana al Convenio de Budapest en el año 2019 representó un avance significativo en la armonización normativa, persisten diferencias relevantes entre los estándares internacionales

exigidos y la regulación nacional vigente, particularmente en lo referido a los mecanismos de cooperación internacional expedita y a la conservación inmediata de datos informáticos.

Los autores citados destacan que la principal utilidad práctica del Convenio de Budapest para investigaciones como la que ocupa la presente tesis radica en sus disposiciones sobre conservación rápida de datos informáticos almacenados y sobre asistencia mutua para la obtención de pruebas en formato electrónico, mecanismos que resultan especialmente relevantes cuando la manipulación del sistema informático es ejecutada por sujetos no identificados que pueden operar desde plataformas o dominios registrados en el extranjero.

No obstante, la investigación de Quincho Laura et al. (2025) concluye que la implementación efectiva de dichos mecanismos en el distrito judicial peruano enfrenta todavía limitaciones operativas relacionadas con la falta de protocolos internos claros y con la escasa capacitación especializada de fiscales y jueces en el manejo de solicitudes de cooperación internacional, lo que en la práctica reduce las ventajas que el propio Convenio ofrece para la individualización del tercero no identificado que interviene en la manipulación del sistema informático.

2.2.4. La autoría, la participación y la atribución de responsabilidad penal en el fraude informático

2.2.4.1. Autoría, coautoría y complicidad en la criminalidad informática

La teoría de la autoría y participación, desarrollada por la dogmática penal a partir de los artículos 23 a 25 del Código Penal peruano, distingue entre el autor, quien realiza directamente el hecho punible o se sirve de otro para su ejecución; el coautor, quien interviene en la comisión conjunta del delito mediante un aporte esencial durante su ejecución conforme a un acuerdo previo; y el cómplice, quien colabora dolosamente en la realización del hecho sin ejecutar por sí mismo la conducta típica.

La aplicación de estas categorías a la criminalidad informática presenta particularidades relevantes, en la medida en que la ejecución del fraude informático suele estructurarse en una división funcional del trabajo criminal: un sujeto o grupo de sujetos ejecuta la manipulación técnica del sistema informático, mientras que otro sujeto —habitualmente el titular de la cuenta receptora— facilita el instrumento financiero necesario para materializar el provecho ilícito,

sin que necesariamente exista entre ambos un acuerdo previo pleno o un conocimiento recíproco de la totalidad de la operación.

En este escenario, la calificación del titular de la cuenta receptora como coautor exige acreditar que dicho sujeto tuvo un dominio funcional del hecho, es decir, que su aporte fue esencial para la consumación del delito y que actuó con pleno conocimiento del carácter ilícito de la operación en la que participaba, mientras que su calificación como cómplice exigiría un aporte de menor entidad funcional. La ausencia de acreditación de cualquiera de estos elementos subjetivos y objetivos impide, en cambio, atribuirle responsabilidad penal alguna, correspondiendo entonces valorarlo como un tercero ajeno al hecho o incluso como víctima adicional de la manipulación informática.

Esta distinción dogmática constituye el fundamento teórico central de la presente investigación, en la medida en que el problema de determinar si el titular de la cuenta receptora actuó como coautor, como cómplice, o si resultó ser un tercero de buena fe utilizado sin su conocimiento, no puede resolverse apelando únicamente a categorías abstractas de la teoría del delito, sino que exige el desarrollo de criterios probatorios específicos capaces de operacionalizar dichas categorías frente a la evidencia disponible en cada caso concreto.

2.2.4.2. La responsabilidad penal en la criminalidad organizada en entornos digitales

Rodríguez Pilco y Chimborazo Castillo (2026) sostienen que la criminalidad organizada ha experimentado una transformación profunda como consecuencia del desarrollo tecnológico, migrando de estructuras jerárquicas territoriales hacia redes transnacionales descentralizadas que operan en el ciberespacio con altos niveles de anonimato y sofisticación técnica, lo que ha incrementado su capacidad operativa y, correlativamente, la dificultad para identificar y sancionar a los responsables de los delitos cometidos.

Los autores citados identifican que este fenómeno pone a prueba las categorías tradicionales del derecho penal, especialmente en lo relativo a la imputación, la autoría, la participación y la asignación de responsabilidad dentro de sistemas organizados digitalizados, planteando una interrogante que resulta directamente aplicable a la presente investigación: si el sistema penal cuenta con un marco regulatorio, técnico e institucional adecuado para atribuir responsabilidad penal cuando la estructura delictiva se sostiene, precisamente, en el anonimato de sus ejecutores materiales.

Entre las principales limitaciones identificadas por Rodríguez Pilco y Chimborazo Castillo (2026) se encuentran la insuficiente regulación específica para conductas digitales complejas, las dificultades en el manejo y valoración de la evidencia digital, la escasez de operadores de justicia especializados, y la falta de protocolos claros frente al uso de tecnologías emergentes, debilidades que, en conjunto, generan obstáculos para la atribución efectiva de responsabilidad penal y favorecen escenarios de impunidad, particularmente respecto de quienes ejecutan materialmente la manipulación técnica del sistema informático.

La propuesta de dichos autores, orientada al fortalecimiento del sistema penal mediante reformas legales, capacitación especializada, mejora de los mecanismos probatorios y cooperación internacional, resulta plenamente trasladable al contexto peruano y, específicamente, al distrito judicial de Ayacucho, en la medida en que la presente investigación evidencia que la dificultad para individualizar a los sujetos no identificados que intervienen en la manipulación informática traslada, en la práctica, el peso íntegro de la persecución penal hacia el único sujeto plenamente identificable: el titular de la cuenta receptora.

2.2.4.3. La individualización del imputado en delitos cometidos por medios tecnológicos

Chavez Martinez y Ruiz Valer (2025), en su investigación sobre la individualización del imputado en delitos cometidos por medios tecnológicos en el distrito fiscal de Arequipa, sostienen que el carácter digital de estas conductas —marcado por el anonimato, la utilización de identidades ficticias y la intervención de servidores ubicados en distintas jurisdicciones— dificulta considerablemente la atribución precisa de responsabilidad penal, al punto que un número significativo de investigaciones culmina en disposiciones de archivo no por la inexistencia del hecho delictivo, sino por las limitaciones técnicas y probatorias para identificar al presunto autor.

Las autoras citadas destacan que la individualización del imputado constituye un presupuesto esencial del debido proceso, del principio de imputación necesaria y del ejercicio pleno del derecho de defensa, adquiriendo una trascendencia particular en el ámbito de los delitos cometidos mediante el uso de tecnologías de la información, en los que la ausencia de una adecuada individualización no solo debilita la eficacia del ius puniendi estatal, sino que también compromete la protección de los derechos fundamentales tanto de las víctimas como de terceros que podrían verse indebidamente involucrados en una investigación penal.

Si bien la investigación de Chavez Martinez y Ruiz Valer (2025) se circunscribe a un delito distinto —las proposiciones sexuales a menores de edad por medios tecnológicos—, sus hallazgos resultan plenamente relevantes para la presente investigación, en la medida en que evidencian una problemática estructural común a toda la criminalidad informática: la naturaleza volátil de la evidencia digital y el anonimato inherente al medio comisivo dificultan, en general, la individualización del ejecutor material del hecho, con independencia de la modalidad delictiva específica de que se trate.

Frente a esta dificultad estructural para individualizar al ejecutor material de la manipulación informática, la presente investigación plantea una vía distinta pero complementaria: en lugar de centrarse en la búsqueda de una individualización imposible del sujeto no identificado, examina los criterios que permiten atribuir válidamente responsabilidad penal al sujeto sí identificable —el titular de la cuenta receptora— sin que ello implique una vulneración del principio de imputación necesaria ni una responsabilidad objetiva desvinculada de su conocimiento y voluntad.

2.2.5. La cuenta bancaria receptora como elemento de conexión entre el hecho y su titular

2.2.5.1. La afectación de las cuentas digitales bancarias por delitos informáticos

Becerra Cervera (2025) examina la problemática de los delitos informáticos y su afectación directa sobre las cuentas digitales bancarias en el Perú, sosteniendo que la masificación de la banca digital ha convertido a las cuentas bancarias en el punto de convergencia obligado de prácticamente toda modalidad de fraude informático, en la medida en que el provecho ilícito perseguido por el agente exige, necesariamente, un instrumento financiero hacia el cual dirigir los fondos sustraídos de la víctima.

El autor citado destaca, entre los antecedentes de su investigación, el planteamiento de Rodríguez (2020, como se citó en Becerra Cervera, 2025), según el cual una parte relevante de los delitos informáticos que afectan cuentas bancarias se origina en descuidos atribuibles al propio consumidor frente a interfaces tecnológicas complejas, particularmente en el caso de adultos mayores, quienes olvidan contraseñas o datos de acceso, circunstancia que los ciberdelincuentes aprovechan para atentar contra su patrimonio digital.

Esta constatación resulta relevante para la presente investigación en un doble sentido: por un lado, evidencia que las cuentas bancarias afectadas por el fraude informático no se limitan a la cuenta de la víctima, de la que se sustrae el dinero, sino que se extiende necesariamente a la cuenta receptora, cuyo titular puede haber incurrido en un descuido similar —como el extravío de su tarjeta o de sus datos de acceso— que explicaría por qué su cuenta terminó siendo utilizada por terceros sin su conocimiento ni participación voluntaria.

Por otro lado, Becerra Cervera (2025) concluye que la falta de una regulación específica sobre los deberes de diligencia y las responsabilidades de las entidades financieras frente a estos hechos incide negativamente en la seguridad del patrimonio de las víctimas, lo que refuerza la necesidad de que los órganos jurisdiccionales examinen con especial rigor probatorio la posición del titular de la cuenta receptora, evitando tanto la impunidad de quien participó conscientemente en el fraude como la sanción injusta de quien resultó ser, él mismo, víctima adicional de la manipulación informática.

2.2.5.2. El titular registral y el titular con conocimiento y voluntad de participar en el fraude

A partir de la revisión de la literatura examinada, la presente investigación propone una distinción conceptual que no ha sido desarrollada de manera expresa en los antecedentes revisados, pero que se deriva necesariamente de la aplicación de la teoría de la autoría y participación al fraude informático: la diferenciación entre el titular meramente registral de la cuenta receptora y el titular con conocimiento y voluntad de participar en el fraude.

El titular meramente registral es aquella persona cuyo nombre figura formalmente como propietaria de la cuenta bancaria hacia la que se dirigió la transferencia fraudulenta, pero respecto de quien no se ha acreditado ningún elemento adicional —conocimiento del origen ilícito de los fondos, voluntad de participar en la operación, o disposición personalísima del dinero recibido— que permita superar dicha condición meramente formal y atribuirle responsabilidad penal por el hecho.

El titular con conocimiento y voluntad de participar, en cambio, es aquel respecto de quien sí se ha acreditado, mediante prueba directa o indiciaria, que tuvo conciencia del carácter ilícito de la operación y actuó con la voluntad de contribuir a su consumación, ya sea facilitando su cuenta a cambio de un beneficio, coordinando directamente con los ejecutores materiales de

la manipulación informática, o disponiendo del dinero recibido de manera consciente de su origen fraudulento.

Esta distinción conceptual, que constituye el eje categorial de la presente investigación, encuentra respaldo indirecto en los antecedentes revisados —particularmente en Becerra Cervera (2025) y en Rodríguez Pilco y Chimborazo Castillo (2026)— en la medida en que ambos reconocen que la sola constatación de un hecho objetivo (la titularidad de la cuenta, o la existencia de una estructura organizada) resulta insuficiente para fundar la responsabilidad penal, exigiéndose siempre la acreditación adicional del elemento subjetivo que vincule a la persona identificada con el conocimiento y la voluntad de participar en el hecho delictivo.

2.2.6. La prueba indiciaria y su aplicación a la criminalidad informática

2.2.6.1. El artículo 158.3 del Código Procesal Penal: pluralidad, concordancia y convergencia

El artículo 158, numeral 3, del Código Procesal Penal peruano establece los requisitos que debe reunir la prueba por indicios para sustentar válidamente una decisión judicial: que el indicio esté probado, que la inferencia esté basada en las reglas de la lógica, la ciencia o la experiencia, y que, cuando se trate de indicios contingentes, estos sean plurales, concordantes entre sí y converjan hacia una misma conclusión, no existiendo contraindicios consistentes que la enerven. Esta norma resulta de aplicación central en los procesos por fraude informático, en los que, según se ha desarrollado en el acápite 2.2.1.2, la propia naturaleza del delito dificulta la obtención de prueba directa sobre la manipulación técnica del sistema.

La teoría racionalista de la valoración de la prueba, desarrollada por autores como Ferrer Beltrán (2021) y Gascón Abellán (2005), sostiene que la prueba indiciaria exige una valoración individual de cada elemento de convicción, seguida de una valoración conjunta u holística orientada a determinar si la hipótesis inculpativa ha sido corroborada conforme al estándar de prueba exigido, el cual, en el proceso penal peruano, ha sido fijado con carácter vinculante como el estándar de "más allá de toda duda razonable" por la Sentencia Plenaria Casatoria N.º 1-2017/CIJ-433.

En el contexto específico del fraude informático, la aplicación de estos requisitos exige identificar los hechos indicadores relevantes —como la titularidad de la cuenta receptora, la recepción de los fondos y los actos posteriores de disposición— y verificar que su valoración

conjunta, conforme a las máximas de experiencia aplicables al funcionamiento habitual de las operaciones bancarias, permita descartar razonablemente las explicaciones alternativas compatibles con la inocencia del titular de la cuenta, tales como la pérdida de sus datos personales o la utilización no autorizada de su cuenta por parte de terceros.

La construcción de la regla de inferencia, conforme a la metodología argumentativa desarrollada por Toulmin (2019), exige que el juzgador explice no solo el hecho indicador y la conclusión que de él se extrae, sino también la garantía o máxima de experiencia que conecta ambos extremos y el grado de fuerza que dicha garantía confiere a la conclusión, exigencia argumentativa cuya ausencia constituye, precisamente, uno de los principales riesgos de motivación aparente en los procesos por fraude informático.

2.2.6.2. Contraindicios e hipótesis alternativas en el proceso penal

El contraindicio se define como todo hecho o circunstancia que, de resultar acreditado, debilita o neutraliza la fuerza incriminatoria del cuadro indiciario de cargo, mientras que la hipótesis alternativa es la explicación distinta a la responsabilidad penal del imputado que este o su defensa técnica proponen para justificar los mismos hechos acreditados. Ambas categorías cumplen una función de garantía dentro del proceso penal, en la medida en que obligan al juzgador a contrastar la solidez de la hipótesis incriminatoria frente a explicaciones alternativas igualmente plausibles antes de emitir un pronunciamiento condenatorio.

En el ámbito específico del fraude informático, las hipótesis alternativas más recurrentes planteadas por la defensa técnica del titular de la cuenta receptora son la pérdida de la tarjeta o de documentos de identidad, el préstamo voluntario de la cuenta a un tercero, la suplantación de identidad, y la utilización no autorizada del dispositivo o de las claves de acceso del titular, hipótesis que, conforme a la doctrina procesal penal, deben valorarse con el mismo rigor exigido para los indicios de cargo y no de manera meramente formal o retórica.

Ferrer Beltrán (2021) propone, en este sentido, que una hipótesis fáctica solo debe considerarse suficientemente probada cuando se hayan refutado todas las demás hipótesis explicativas de los mismos datos que resulten compatibles con la inocencia del imputado, excluidas las meras hipótesis ad hoc carentes de todo respaldo probatorio, criterio que exige del juzgador un análisis expreso y diferenciado de cada hipótesis alternativa planteada, y no su descarte genérico o presuntivo.

La aplicación de este estándar a los procesos por fraude informático adquiere una complejidad adicional derivada de la naturaleza técnica de las hipótesis alternativas planteadas, en la medida en que su verificación —por ejemplo, la determinación de si efectivamente existió un acceso no autorizado al dispositivo del titular— exige frecuentemente de conocimientos periciales especializados en informática forense de los que no siempre disponen oportunamente los operadores jurídicos, lo que refuerza la relevancia del aporte técnico pericial que se desarrolla en el siguiente acápite.

2.2.7. La evidencia digital y las herramientas forenses informáticas

2.2.7.1. Cadena de custodia y trazabilidad de la evidencia digital

La evidencia digital se caracteriza por su naturaleza volátil y su alta susceptibilidad a la alteración, pérdida o destrucción, lo que exige la aplicación rigurosa de protocolos de cadena de custodia desde el momento mismo de su identificación y aseguramiento, a fin de garantizar que dicha evidencia mantenga su integridad y autenticidad a lo largo de todo el proceso penal, desde la investigación preliminar hasta su valoración en juicio oral.

En los procesos por fraude informático, la trazabilidad de la evidencia digital comprende, fundamentalmente, dos vertientes complementarias: por un lado, la trazabilidad técnica del acceso al sistema informático manipulado, que incluye direcciones IP, registros de acceso y metadatos de conexión; y, por otro lado, la trazabilidad financiera del dinero sustraído, que comprende el seguimiento de las transferencias, retiros y conversiones sucesivas del monto defraudado hasta su destino final.

La oportuna preservación de esta evidencia resulta determinante para la individualización de los sujetos no identificados que intervienen en la manipulación informática, en la medida en que el retraso en el aseguramiento de los dispositivos electrónicos o en la solicitud de información a las entidades bancarias y proveedores de servicios de internet reduce considerablemente las posibilidades de rastrear el origen técnico de la manipulación, favoreciendo con ello los escenarios de impunidad advertidos por Rodríguez Pilco y Chimborazo Castillo (2026).

La ausencia de estándares uniformes para la preservación y provisión de esta información por parte de las entidades bancarias y las plataformas digitales constituye, conforme se evidencia en la propia práctica judicial analizada en la presente investigación, una

de las principales limitaciones estructurales para la individualización de los ejecutores materiales del fraude, lo que traslada, en la práctica, el peso probatorio íntegro hacia la conducta del titular de la cuenta receptora.

2.2.7.2. Herramientas forenses digitales potenciadas con inteligencia artificial

Catagua Zambrano y Vera Navarrete (2026) han realizado un análisis comparativo del rendimiento de herramientas forenses digitales potenciadas con inteligencia artificial, evaluando específicamente Autopsy, Magnet AXIOM y Belkasoft Evidence X sobre una imagen forense estandarizada, con el objetivo de identificar soluciones que fortalezcan las investigaciones digitales frente al incremento de la ciberdelincuencia en la región latinoamericana.

Los resultados de dicho estudio evidenciaron que Magnet AXIOM, gracias a su inteligencia artificial nativa integrada, procesó la evidencia forense en apenas cincuenta segundos, demostrando una notable eficiencia en velocidad y automatización, mientras que Belkasoft Evidence X sobresalió en la recuperación de evidencia mediante filtros semánticos visuales, identificando un mayor número de elementos multimedia relevantes para la investigación.

No obstante estos avances tecnológicos, Catagua Zambrano y Vera Navarrete (2026) identificaron una brecha formativa crítica: el 75% de los profesionales encuestados manifestó utilizar estas herramientas solo ocasionalmente, lo que evidencia una desconexión relevante entre el potencial tecnológico disponible y su aprovechamiento efectivo en la práctica cotidiana de la investigación de delitos informáticos, incluyendo el fraude informático objeto de la presente investigación.

Esta brecha formativa resulta directamente relevante para explicar una de las limitaciones identificadas en la práctica judicial de Ayacucho: la escasa profundidad del desarrollo pericial informático en la mayoría de los expedientes analizados, que contrasta con el potencial técnico que herramientas como las evaluadas por Catagua Zambrano y Vera Navarrete (2026) podrían ofrecer para determinar con mayor precisión si el titular de la cuenta receptora tuvo o no un rol activo en la manipulación del sistema informático.

2.2.8. Impunidad y desafíos institucionales frente a los delitos informáticos

Rosales Medina (2025) analiza la relación entre el incremento sostenido de los delitos informáticos y la problemática de la impunidad delictiva en Lima, sosteniendo que dicho incremento no encuentra una respuesta institucional proporcional por parte del sistema de justicia penal, lo que genera una creciente sensación de desprotección en la ciudadanía frente a esta modalidad delictiva de rápido crecimiento.

La autora identifica que, entre las principales causas estructurales de la impunidad en los delitos informáticos, se encuentran las limitaciones técnicas y logísticas de las unidades especializadas de investigación, la insuficiente capacitación de los operadores jurídicos en aspectos tecnológicos, y la dificultad práctica para obtener cooperación oportuna de las entidades financieras y de las plataformas digitales involucradas en los hechos investigados.

Esta problemática de impunidad, identificada por Rosales Medina (2025) a nivel general para todos los delitos informáticos, adquiere una dimensión particular en el fraude informático cuando se analiza desde la perspectiva de la presente investigación: la imposibilidad práctica de individualizar a los sujetos no identificados que ejecutan la manipulación técnica del sistema no debería derivar automáticamente en la impunidad total del hecho, en la medida en que el titular de la cuenta receptora, cuando concurren los elementos objetivos y subjetivos necesarios, puede y debe responder penalmente por su propia contribución al fraude.

En sentido inverso, la misma problemática de impunidad exige que los órganos jurisdiccionales eviten trasladar automáticamente hacia el titular de la cuenta receptora toda la responsabilidad penal por un hecho ejecutado predominantemente por terceros no identificados, pues ello generaría el riesgo simétricamente opuesto: sancionar penalmente a personas que resultaron ser, ellas mismas, víctimas adicionales de la sofisticación técnica de estas modalidades delictivas, sin haber tenido conocimiento ni voluntad de participar en el fraude.

2.2.9. Ciberseguridad y protección de datos personales

Alvear Richards y Hernández Pesantes (2023) desarrollan un análisis comparativo entre la Ley Orgánica de Protección de Datos Personales del Ecuador y la legislación peruana correspondiente, desde un enfoque de ciberseguridad y delitos informáticos, evidenciando que la adecuada protección de los datos personales de los usuarios de servicios financieros digitales

constituye una condición previa indispensable para la prevención de modalidades de fraude informático como el phishing, el smishing y el vishing.

Las autoras destacan que, si bien tanto el ordenamiento ecuatoriano como el peruano han incorporado disposiciones orientadas a la protección de datos personales, persisten diferencias relevantes en cuanto a los mecanismos de exigibilidad y a las sanciones administrativas aplicables frente al tratamiento indebido o la exposición negligente de dicha información, lo que incide directamente en la magnitud del riesgo de captación fraudulenta de datos que sustenta la comisión del fraude informático.

Esta perspectiva comparada resulta relevante para la presente investigación en la medida en que evidencia que la seguridad de las cuentas bancarias no depende únicamente de la conducta diligente o negligente de sus titulares, sino también del nivel de protección técnica y normativa que las propias entidades financieras y reguladores de datos personales están en capacidad de ofrecer, factor institucional que debe ser tomado en cuenta al momento de valorar la responsabilidad individual del titular de la cuenta receptora frente a un fraude informático sofisticado.

Alvear Richards y Hernández Pesantes (2023) concluyen que el fortalecimiento de la ciberseguridad jurídica exige una actualización normativa constante frente a la velocidad de la innovación tecnológica empleada por los agentes del fraude informático, conclusión que resulta plenamente aplicable al contexto peruano y que refuerza la pertinencia de investigaciones como la presente, orientadas a sistematizar los criterios judiciales que permitan una respuesta penal proporcional y jurídicamente sólida frente a esta modalidad delictiva en constante evolución.

2.3. Marco normativo

2.3.1. Constitución Política del Perú

La Constitución Política del Perú de 1993 constituye el marco de referencia primario de toda la investigación, en la medida en que el artículo 2, inciso 24, literal e, consagra el principio de presunción de inocencia, según el cual toda persona es considerada inocente mientras no se haya declarado judicialmente su responsabilidad. Este principio resulta determinante para la presente investigación, pues impide que la sola titularidad registral de una cuenta bancaria receptora del dinero fraudulentamente transferido pueda dar lugar, por sí sola, a una presunción de responsabilidad penal en contra de su titular, exigiéndose siempre la acreditación positiva de los elementos objetivos y subjetivos del delito.

El artículo 139, inciso 3, de la Constitución consagra, además, el derecho al debido proceso, que comprende, entre sus manifestaciones, el principio de imputación necesaria, conforme al cual toda persona sometida a un proceso penal tiene derecho a conocer con precisión, claridad y circunstancialidad los hechos que se le atribuyen. Este derecho adquiere una relevancia particular en los procesos por fraude informático en los que se alega la intervención de sujetos no identificados, pues exige que la imputación dirigida contra el titular de la cuenta receptora precise con exactitud cuál fue su aporte concreto al hecho delictivo, y no se limite a una fórmula genérica de coordinación con terceros no individualizados.

De igual manera, el artículo 139, inciso 5, de la Constitución establece el deber de motivación escrita de las resoluciones judiciales en todas las instancias, con mención expresa de la ley aplicable y de los fundamentos de hecho en que se sustentan, salvo los decretos de mero trámite. Este deber constitucional de motivación constituye el fundamento último de la exigencia, desarrollada en el marco teórico de la presente investigación, de que los órganos jurisdiccionales expliciten con claridad la regla de inferencia que conecta los hechos indicadores acreditados con la conclusión sobre el conocimiento y la voluntad del titular de la cuenta receptora.

Finalmente, el artículo 2, inciso 24, literal d, de la Constitución consagra el principio de legalidad penal, según el cual nadie puede ser condenado por acto u omisión que, al tiempo de cometerse, no esté previamente calificado en la ley como infracción punible. Este principio exige que la subsunción de la conducta del titular de la cuenta receptora en las categorías de autoría o participación se realice con estricto apego a los presupuestos típicos del artículo 8 de la Ley N.º 30096 y a las reglas generales sobre autoría y participación del Código Penal, sin que resulte admisible una extensión analógica de la responsabilidad penal fundada exclusivamente en la titularidad formal de la cuenta.

2.3.2. Código Penal peruano

El Código Penal peruano regula, en sus artículos 23 a 25, las formas de autoría y participación aplicables a todo delito, incluido el fraude informático. El artículo 23 establece que es autor quien realiza por sí o por medio de otro el hecho punible, y que los que lo cometan conjuntamente serán reprimidos con la pena establecida para el autor, disposición que sustenta la calificación de coautoría del titular de la cuenta receptora cuando se acredita que su aporte al hecho —facilitar la cuenta y disponer del dinero recibido— resultó esencial y estuvo articulado con la conducta del sujeto no identificado que ejecutó la manipulación informática.

El artículo 25 del Código Penal regula, por su parte, la complicidad, distinguiendo entre el cómplice primario, que dolosamente presta auxilio para la realización del hecho sin el cual no se hubiera perpetrado, y el cómplice secundario, que presta cualquier otro auxilio de menor entidad. Esta distinción resulta relevante para calificar jurídicamente los supuestos en que el aporte del titular de la cuenta receptora, aun siendo doloso, no alcanzó el grado de esencialidad exigido para la coautoría, como podría ocurrir en los casos de "alquiler" o préstamo remunerado de cuentas identificados como categoría emergente en la presente investigación.

El artículo IV del Título Preliminar del Código Penal consagra el principio de lesividad, según el cual la pena necesariamente precisa de la lesión o puesta en peligro de bienes jurídicos tutelados por la ley, principio que fue expresamente invocado en el expediente N.º 01342-2022-33 de la muestra documental para fundamentar el juicio de antijuridicidad de la conducta de la acusada. Asimismo, los artículos 45, 45-A y 46 regulan el procedimiento de individualización judicial de la pena mediante el sistema de tercios, exigiendo la consideración de las carencias sociales del agente, su cultura, sus costumbres y los intereses de la víctima, criterios que se aplicaron de manera recurrente en las sentencias analizadas para fijar la pena concreta impuesta a los titulares de las cuentas receptoras condenados.

Finalmente, los artículos 92 y 93 del Código Penal regulan la reparación civil derivada del delito, estableciendo que esta comprende la restitución del bien o, si no es posible, el pago de su valor, así como la indemnización de los daños y perjuicios, disposiciones que fundamentaron, en los expedientes condenatorios de la muestra documental, la orden de restitución del monto fraudulentamente transferido a favor de las víctimas, con independencia de la pena privativa de libertad impuesta a los titulares de las cuentas receptoras.

2.3.3. Código Procesal Penal (artículo 158.3)

El artículo 158 del Código Procesal Penal peruano regula, en su numeral 3, los requisitos que debe reunir la prueba por indicios para sustentar válidamente una sentencia condenatoria, exigiendo que el indicio esté probado, que la inferencia esté basada en las reglas de la lógica, la ciencia o la experiencia, y que, cuando se trate de indicios contingentes, estos sean plurales, concordantes y converjan hacia una misma conclusión, sin que existan contraindicios consistentes. Esta disposición constituye el fundamento normativo procesal central de la presente investigación, en la medida en que el fraude informático, por su propia naturaleza, rara vez cuenta con prueba directa sobre la manipulación técnica del sistema informático.

El artículo 393, numeral 2, del mismo cuerpo normativo complementa esta exigencia al disponer que el juez penal, para la apreciación de las pruebas, procederá primero a examinarlas individualmente y luego en conjunto con las demás, consagrando así el método de valoración probatoria de dos fases —individual y holística— desarrollado en la teoría racionalista de la prueba y aplicado expresamente en el expediente N.º 01342-2022-33 de la muestra documental de la presente investigación.

El artículo 394, numeral 3, del Código Procesal Penal exige que la sentencia contenga la motivación clara, lógica y completa de cada uno de los hechos y circunstancias que se dan por probadas o improbadas, con indicación del razonamiento que la justifique, disposición que sustenta la exigencia, desarrollada en el marco teórico, de que los órganos jurisdiccionales expliciten la regla de inferencia que conecta los hechos indicadores con la conclusión sobre el conocimiento y la voluntad del titular de la cuenta receptora, y no se limiten a una motivación aparente o a un salto inferencial no justificado.

Finalmente, el artículo 12, numeral 3, del Código Procesal Penal establece que la sentencia absolutoria o el auto de sobreseimiento no impiden al órgano jurisdiccional pronunciarse sobre la acción civil derivada del hecho punible válidamente ejercida, disposición que resultó aplicada expresamente en el expediente absolutorio N.º 00724-2020-83 de la muestra documental, en el que, pese a la insuficiencia de la prueba penal para sustentar la responsabilidad penal de la titular de la cuenta receptora, se declaró fundada en parte la pretensión civil por concepto de restitución del dinero indebidamente retenido en su cuenta.

2.3.4. Ley N.º 30096, Ley de Delitos Informáticos, y su modificatoria Ley N.º 30171

La Ley N.º 30096, Ley de Delitos Informáticos, publicada el 22 de octubre de 2013, constituye el cuerpo normativo especial que tipifica de manera autónoma las conductas delictivas ejecutadas mediante el uso de las tecnologías de la información y la comunicación, respondiendo a la necesidad, advertida por Bramont-Arias Torres (1997) y desarrollada en el marco teórico de la presente investigación, de una respuesta penal específica frente a una criminalidad que no encontraba adecuada subsunción en los tipos penales tradicionales del Código Penal.

El artículo 8 de dicha ley, modificado por el artículo 1 de la Ley N.º 30171, publicada el 10 de marzo de 2014, tipifica el delito de fraude informático, sancionando a quien de manera deliberada e ilegítima procura para sí o para otro un provecho ilícito en perjuicio de tercero

mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, con una pena privativa de libertad no menor de tres ni mayor de ocho años y de sesenta a ciento veinte días multa, elevándose dicho marco punitivo cuando se afecta el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

La exposición de motivos de la Ley N.º 30096 se sustentó, precisamente, en la necesidad de adecuar la legislación penal nacional a los estándares internacionales sobre ciberdelincuencia, particularmente a los establecidos por el Convenio de Budapest, evidenciando desde su origen una vocación de armonización normativa que resulta desarrollada con mayor detalle en el acápite siguiente del presente marco normativo.

La aplicación práctica de este tipo penal en las cinco sentencias que integran la muestra documental de la presente investigación evidencia que su formulación amplia —al no exigir una modalidad técnica específica de manipulación— permite subsumir tanto los supuestos de phishing y spoofing mediante páginas web falsas, como los supuestos de acceso directo no autorizado a plataformas bancarias legítimas, lo que otorga a la norma una flexibilidad típica adecuada para enfrentar la constante evolución de las modalidades de ejecución del fraude informático.

2.3.5. Convenio de Budapest sobre la Ciberdelincuencia

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, suscrito en Budapest el 23 de noviembre de 2001, constituye el primer instrumento internacional de carácter vinculante destinado a la armonización de las legislaciones penales nacionales frente a los delitos cometidos a través de sistemas informáticos, estableciendo en su artículo 8 la obligación de los Estados signatarios de tipificar como delito los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos, o mediante cualquier interferencia en el funcionamiento de un sistema informático con la intención de obtener un beneficio económico ilegítimo.

El Perú se adhirió formalmente al Convenio de Budapest mediante el Decreto Supremo N.º 010-2019-RE, ratificado por el Congreso de la República, incorporándose dicho instrumento al ordenamiento jurídico nacional conforme al artículo 55 de la Constitución Política, que reconoce a los tratados celebrados por el Estado y en vigor como parte del derecho

nacional, lo que dota a sus disposiciones de plena eficacia normativa interna en materia de cooperación internacional y armonización sustantiva frente a la ciberdelincuencia.

Además de la tipificación sustantiva del fraude informático, el Convenio de Budapest establece, en su Capítulo III, mecanismos de cooperación internacional de especial relevancia para la presente investigación, tales como la conservación rápida de datos informáticos almacenados y la asistencia mutua para la obtención de pruebas en formato electrónico, mecanismos que, conforme señalan Quincho Laura, Aylas Dionicio y Arcos Huayhua (2025), resultan indispensables cuando la manipulación del sistema informático es ejecutada por sujetos no identificados que operan desde plataformas o dominios registrados fuera del territorio nacional.

No obstante su plena vigencia normativa, la implementación operativa de estos mecanismos de cooperación en el distrito judicial de Ayacucho enfrenta las mismas limitaciones estructurales identificadas de manera general por Quincho Laura et al. (2025) para el ámbito nacional, relacionadas con la ausencia de protocolos internos expeditos y la escasa capacitación especializada de los operadores jurídicos, lo que en la práctica reduce el aprovechamiento de las herramientas de cooperación internacional que el propio Convenio pone a disposición del sistema de justicia penal peruano para la individualización de los ejecutores materiales del fraude informático.

2.3. Marco conceptual

- a. **Autoría.** Conforme al artículo 23 del Código Penal peruano, es autor quien realiza por sí o por medio de otro el hecho punible, así como quienes lo cometen conjuntamente. En el fraude informático, se atribuye la condición de autor a quien ejecuta materialmente la manipulación del sistema informático o interviene decisivamente en la consumación del provecho ilícito, distinguiéndose de la mera facilitación instrumental de una cuenta bancaria sin conocimiento del hecho.
- b. **Cadena de custodia.** Es el procedimiento destinado a garantizar la identidad, integridad y conservación de los elementos materiales de prueba desde el momento de su hallazgo o incautación hasta su valoración en el proceso penal, mediante el registro documentado de cada persona que tuvo contacto con dicho elemento y de las condiciones en que fue manipulado, trasladado o almacenado.
- c. **Coautoría.** Modalidad de intervención delictiva en la que dos o más personas, en virtud de un acuerdo previo o coetáneo, aportan de manera esencial a la ejecución del hecho

punible, de modo que cada interviniente domina funcionalmente una parte del suceso delictivo. En el fraude informático, la coautoría del titular de la cuenta receptora exige acreditar que su aporte —facilitar la cuenta y disponer del dinero recibido— resultó indispensable para la consumación del provecho ilícito perseguido conjuntamente con el sujeto que ejecutó la manipulación informática.

- d. **Complicidad.** Conforme al artículo 25 del Código Penal, consiste en el auxilio doloso prestado para la realización del hecho punible sin ejecutar la conducta típica, distinguiéndose entre complicidad primaria, cuando dicho auxilio resulta indispensable para la comisión del delito, y complicidad secundaria, cuando el aporte reviste una menor entidad funcional.
- e. **Contraindicio.** Todo hecho o circunstancia que, de resultar acreditado, debilita o neutraliza la fuerza incriminatoria del cuadro indiciario de cargo reunido en la investigación, exigiendo su valoración expresa por parte del órgano jurisdiccional antes de concluir la responsabilidad penal del imputado.
- f. **Convenio de Budapest.** Instrumento internacional suscrito en el año 2001 en el marco del Consejo de Europa, orientado a la armonización de las legislaciones penales nacionales frente a la ciberdelincuencia y al establecimiento de mecanismos de cooperación internacional para la investigación de estos delitos, al cual el Perú se adhirió formalmente en el año 2019 (Quincho Laura et al., 2025).
- g. **Elemento de convicción.** Medio de prueba concreto —de naturaleza documental, pericial o testimonial— incorporado legítimamente a la investigación penal, del cual se extrae la afirmación fáctica que constituye el hecho indicador empleado para sustentar o descartar una hipótesis de responsabilidad penal.
- h. **Fraude informático.** Delito previsto en el artículo 8 de la Ley N.º 30096, modificado por la Ley N.º 30171, que sanciona a quien, de manera deliberada e ilegítima, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión o clonación de datos informáticos, o mediante cualquier interferencia o manipulación en el funcionamiento de un sistema informático.
- i. **Hecho indicador.** Dato fáctico plenamente acreditado dentro del proceso a partir del cual el juzgador puede inferir, mediante un razonamiento lógico basado en las reglas de la experiencia, la ciencia o la lógica, la existencia de otro hecho que no ha sido objeto de prueba directa, como el conocimiento y la voluntad del titular de una cuenta receptora de participar en un fraude informático.

- j. **Hipótesis alternativa.** Explicación distinta a la responsabilidad penal del imputado, planteada por este o por su defensa técnica, para justificar los mismos hechos acreditados en la investigación, como la pérdida de la tarjeta o de documentos personales, el préstamo de la cuenta a un tercero, o la suplantación de identidad, cuya verosimilitud debe contrastarse con elementos objetivos disponibles en el expediente.
- k. **Individualización del imputado.** Presupuesto del debido proceso y del principio de imputación necesaria consistente en la identificación precisa de la persona a quien se atribuye la comisión de un hecho delictivo, cuya dificultad se incrementa considerablemente en los delitos informáticos por el anonimato y la dispersión geográfica propios del medio comisivo (Chavez Martinez & Ruiz Valer, 2026).
- l. **Motivación aparente / salto inferencial.** Defecto argumentativo de una resolución judicial o fiscal consistente en enunciar los hechos indicadores acreditados y concluir directamente la responsabilidad penal del imputado, sin desarrollar de manera explícita la máxima de experiencia o el razonamiento lógico que conecta ambos extremos, lo que vulnera el deber constitucional de motivación de las resoluciones judiciales.
- m. **Phishing.** Modalidad matriz de captación fraudulenta de datos personales mediante el diseño de páginas web o comunicaciones que imitan a una entidad legítima, habitualmente bancaria, con la finalidad de inducir a la víctima a proporcionar información confidencial que posteriormente es empleada para consumir una transferencia patrimonial no consentida (Ventura Quijano, 2021).
- n. **Préstamo o "alquiler" de cuentas receptoras.** Categoría emergente identificada en la presente investigación, referida a la modalidad mediante la cual el titular de una cuenta bancaria cede su uso a un tercero a cambio de una comisión económica, conociendo que facilita con ello una operación irregular, pero sin conocer necesariamente el origen ilícito específico de los fondos que recibirá, lo que la sitúa como una figura intermedia entre el titular plenamente consciente del fraude y el titular víctima de suplantación de identidad.
- o. **Prueba indiciaria.** Medio de prueba indirecto regulado en el artículo 158, numeral 3, del Código Procesal Penal, mediante el cual se acredita un hecho no probado directamente a partir de la inferencia lógica de otros hechos sí acreditados (indicios), exigiéndose que estos sean plurales, concordantes y convergentes, y que no existan contraindicios consistentes que enerven la conclusión incriminatoria.
- p. **Spoofing.** Modalidad técnica de suplantación de identidad digital que consiste en la creación de una página web con las mismas características visuales de la plataforma

legítima que se pretende imitar, de modo que la víctima transmite inadvertidamente sus datos personales a un tercero que los utiliza para ejecutar la transferencia fraudulenta.

- q. **Titular con conocimiento y voluntad de participar.** Categoría propia de la presente investigación referida a la persona respecto de quien se ha acreditado, mediante prueba directa o indiciaria, que tuvo conciencia del carácter ilícito de la operación realizada en su cuenta bancaria y actuó con voluntad de contribuir a su consumación, ya sea facilitando dicha cuenta a cambio de un beneficio, coordinando con los ejecutores materiales de la manipulación informática, o disponiendo conscientemente del dinero recibido.
- r. **Titular meramente registral.** Categoría propia de la presente investigación referida a la persona cuyo nombre figura formalmente como propietaria de la cuenta bancaria receptora del dinero fraudulentamente transferido, sin que se haya acreditado ningún elemento adicional —conocimiento del origen ilícito, voluntad de participar o disposición personalísima de los fondos— que permita superar dicha condición meramente formal y atribuirle responsabilidad penal por el hecho.
- s. **Vishing.** Modalidad de captación fraudulenta de información ejecutada mediante llamadas telefónicas o mensajes de voz en los que el agente suplanta la identidad de una entidad bancaria o de un familiar de la víctima, induciéndola a proporcionar información confidencial o a realizar directamente una operación financiera (Ventura Quijano, 2021).

CAPÍTULO III: CATEGORÍAS DE LA INVESTIGACIÓN

En las investigaciones de enfoque cualitativo, la categorización constituye la operación metodológica mediante la cual el investigador traduce sus problemas y objetivos específicos en unidades de análisis concretas, susceptibles de ser identificadas, descritas y comparadas dentro del material empírico examinado. Para efectos de la presente investigación, se optó por una categorización de tipo apriorística, construida a partir del marco teórico sobre autoría, participación y prueba indiciaria, y de los problemas secundarios previamente formulados, sin perjuicio de que, conforme a lo previsto por Hernández-Sampieri y Mendoza (2018), durante el análisis del material empírico pudieran emerger subcategorías adicionales no previstas inicialmente.

Las tres categorías apriorísticas que a continuación se desarrollan guardaron correspondencia directa con los tres problemas secundarios de la investigación: el valor jurídico-probatorio de la titularidad de la cuenta, la recepción de los fondos y los actos posteriores de disposición; la valoración de la intervención de sujetos no identificados y de las hipótesis alternativas planteadas por la defensa; y la construcción y motivación de la inferencia probatoria que permite distinguir al titular meramente registral de aquel que intervino con conocimiento y voluntad en el fraude informático.

Como se detalla al final del presente capítulo, durante el análisis de las entrevistas emergió efectivamente una subcategoría adicional no prevista en la matriz apriorística original, la cual fue incorporada a la Categoría 2 conforme al procedimiento de categorización emergente propio del enfoque cualitativo.

3.1. Matriz de categorización apriorística y emergente

Problema secundario	Categoría	Subcategorías	Indicadores

P.S.1	Valor jurídico- probatorio de la titularidad, la recepción de los fondos y los actos posteriores de disposición	• Titularidad formal de la cuenta receptora • Recepción efectiva de los fondos • Actos posteriores de disposición • Peso probatorio diferenciado atribuido a cada hecho	• Fecha de apertura de la cuenta en relación con la fecha del hecho; vigencia de la cuenta al momento de la transferencia; identidad entre el titular registral y el acusado. • Acreditación del ingreso del dinero a la cuenta mediante reporte bancario; monto y fecha exacta de la recepción; canal empleado para la transferencia. • Retiros en efectivo, transferencias a terceras cuentas, conversión en criptomonedas u otros activos; medio empleado para dicha disposición (tarjeta y clave personal, banca por internet, ventanilla). • Calificación expresa o implícita de cada hecho como indicio suficiente,
-------	--	--	--

			insuficiente o meramente complementario para sustentar la responsabilidad penal.
P.S.2	Valoración de la intervención de sujetos no identificados y de las hipótesis alternativas	• Tratamiento de la alegación fiscal sobre el tercero no identificado • Hipótesis alternativa de pérdida de tarjeta o documentos • Hipótesis alternativa de préstamo de la cuenta • Hipótesis alternativa de suplantación de identidad o uso no autorizado • Verificación objetiva de la hipótesis alternativa planteada • Subcategoría emergente: préstamo remunerado o	• Forma en que la imputación describe la intervención del tercero; relación funcional descrita entre dicho tercero y el titular de la cuenta. • Existencia de denuncia policial previa; oportunidad y coherencia temporal de la pérdida alegada respecto de la fecha del hecho. • Identificación de la persona a quien se habría prestado la cuenta; verosimilitud de dicho préstamo conforme a las reglas de la experiencia. • Elementos técnicos o testimoniales que acrediten o descarten el acceso no

		"alquiler" de la cuenta receptora (emergente)	autorizado al dispositivo o a la cuenta del titular. • Contraste de la hipótesis con elementos documentales u objetivos disponibles en el expediente; consecuencia de dicha verificación en el sentido del fallo. • Identificada durante el análisis de la entrevista al perito informático forense (PI-01), quien señaló que el titular puede haber cedido su cuenta a cambio de una comisión, conociendo que facilitaba una operación irregular pero sin conocer necesariamente el origen ilícito específico de los fondos. Esta subcategoría no formaba parte de la matriz apriorística inicial y fue incorporada conforme al procedimiento de
--	--	---	---

			categorización emergente descrito por Hernández-Sampieri y Mendoza (2018), en la medida en que aportó una figura intermedia entre el titular plenamente consciente del fraude y el titular víctima de suplantación de identidad.
P.S.3	Construcción y motivación de la inferencia probatoria entre el titular registral y el titular con conocimiento y voluntad	• Identificación del hecho indicador que revela conocimiento • Máxima de experiencia o razonamiento lógico aplicado • Diferenciación expresa entre titularidad formal y responsabilidad penal • Estándar de motivación exigido para la condena o la absolución	• Hecho específico que el juzgador emplea para inferir que el titular conocía el origen ilícito de los fondos (por ejemplo, retiro inmediato y personalísimo del dinero). • Enunciado general empleado para justificar el tránsito entre el hecho acreditado y la conclusión sobre el conocimiento y la voluntad del titular. • Referencia explícita en la motivación a que la sola titularidad no equivale a

			responsabilidad penal, y desarrollo de los elementos adicionales que la sustentan. • Nivel de suficiencia argumentativa exigido por el juzgador para considerar superada la duda razonable sobre la condición de mero titular registral.
--	--	--	---

3.2. Desarrollo de las categorías y subcategorías

3.2.1. Categoría 1: Valor jurídico-probatorio de la titularidad, la recepción de los fondos y los actos posteriores de disposición

Problema secundario relacionado: *¿Qué valor jurídico-probatorio se atribuye a la titularidad de la cuenta receptora, la recepción de los fondos y los actos posteriores de disposición para determinar la participación del titular en el fraude informático?*

Definición conceptual

Esta categoría examinó el peso probatorio diferenciado que los órganos jurisdiccionales otorgan a tres hechos que suelen presentarse de manera secuencial en el delito de fraude informático: la titularidad formal de la cuenta bancaria a la que se dirige la transferencia fraudulenta, la recepción efectiva de los fondos en dicha cuenta, y los actos posteriores mediante los cuales dichos fondos son retirados, transferidos a terceros o convertidos en otros activos. La categoría permitió determinar si estos tres hechos reciben un tratamiento probatorio

equivalente o si, por el contrario, los órganos jurisdiccionales atribuyen un valor incriminatorio creciente conforme se avanza de la titularidad formal hacia la disposición efectiva del dinero.

Subcategorías e indicadores

- a) **Titularidad formal de la cuenta receptora:** Fecha de apertura de la cuenta en relación con la fecha del hecho; vigencia de la cuenta al momento de la transferencia; identidad entre el titular registral y el acusado.
- b) **Recepción efectiva de los fondos:** Acreditación del ingreso del dinero a la cuenta mediante reporte bancario; monto y fecha exacta de la recepción; canal empleado para la transferencia.
- c) **Actos posteriores de disposición:** Retiros en efectivo, transferencias a terceras cuentas, conversión en criptomonedas u otros activos; medio empleado para dicha disposición (tarjeta y clave personal, banca por internet, ventanilla).
- d) **Peso probatorio diferenciado atribuido a cada hecho:** Calificación expresa o implícita de cada hecho como indicio suficiente, insuficiente o meramente complementario para sustentar la responsabilidad penal.

3.2.2. Categoría 2: Valoración de la intervención de sujetos no identificados y de las hipótesis alternativas

Problema secundario relacionado: *¿Cómo se valora la intervención de sujetos no identificados y las hipótesis alternativas de pérdida, préstamo, suplantación o utilización no autorizada de la cuenta receptora?*

Definición conceptual

Esta categoría analizó el tratamiento que los órganos jurisdiccionales otorgan, por un lado, a la alegación fiscal sobre la intervención de un tercero no identificado que habría ejecutado materialmente la manipulación del sistema informático, y, por otro lado, a las hipótesis alternativas que la defensa técnica del titular de la cuenta planteó para explicar su

desvinculación del hecho, tales como la pérdida de la tarjeta o de documentos personales, el préstamo voluntario de la cuenta a un tercero, la suplantación de su identidad, o la utilización no autorizada de sus datos o dispositivos.

Subcategorías e indicadores

- a) **Tratamiento de la alegación fiscal sobre el tercero no identificado:** Forma en que la imputación describe la intervención del tercero; relación funcional descrita entre dicho tercero y el titular de la cuenta.
- b) **Hipótesis alternativa de pérdida de tarjeta o documentos:** Existencia de denuncia policial previa; oportunidad y coherencia temporal de la pérdida alegada respecto de la fecha del hecho.
- c) **Hipótesis alternativa de préstamo de la cuenta:** Identificación de la persona a quien se habría prestado la cuenta; verosimilitud de dicho préstamo conforme a las reglas de la experiencia.
- d) **Hipótesis alternativa de suplantación de identidad o uso no autorizado:** Elementos técnicos o testimoniales que acrediten o descarten el acceso no autorizado al dispositivo o a la cuenta del titular.
- e) **Verificación objetiva de la hipótesis alternativa planteada:** Contraste de la hipótesis con elementos documentales u objetivos disponibles en el expediente; consecuencia de dicha verificación en el sentido del fallo.
- f) **Subcategoría emergente: préstamo remunerado o "alquiler" de la cuenta receptora**
[Subcategoría emergente]: Identificada durante el análisis de la entrevista al perito informático forense (PI-01), quien señaló que el titular puede haber cedido su cuenta a cambio de una comisión, conociendo que facilitaba una operación irregular pero sin conocer necesariamente el origen ilícito específico de los fondos. Esta subcategoría no formaba parte de la matriz apriorística inicial y fue incorporada conforme al

procedimiento de categorización emergente descrito por Hernández-Sampieri y Mendoza (2018), en la medida en que aportó una figura intermedia entre el titular plenamente consciente del fraude y el titular víctima de suplantación de identidad.

3.2.3 Categoría 3: Construcción y motivación de la inferencia probatoria entre el titular registral y el titular con conocimiento y voluntad

Problema secundario relacionado: *¿Cómo se construye y motiva la inferencia probatoria que permite distinguir al titular meramente registral del titular que intervino con conocimiento y voluntad en el fraude informático?*

Definición conceptual

Esta categoría examinó el razonamiento inferencial mediante el cual el órgano jurisdiccional transita desde la constatación de que una persona es la titular formal o registral de la cuenta receptora, hacia la conclusión de que dicha persona tuvo, además, conocimiento del origen ilícito de los fondos y voluntad de participar en el fraude informático, distinción que resultó determinante para diferenciar entre la responsabilidad penal y la condición de mero instrumento o víctima adicional del hecho.

Subcategorías e indicadores

- a) **Identificación del hecho indicador que revela conocimiento:** Hecho específico que el juzgador emplea para inferir que el titular conocía el origen ilícito de los fondos (por ejemplo, retiro inmediato y personalísimo del dinero).
- b) **Máxima de experiencia o razonamiento lógico aplicado:** Enunciado general empleado para justificar el tránsito entre el hecho acreditado y la conclusión sobre el conocimiento y la voluntad del titular.
- c) **Diferenciación expresa entre titularidad formal y responsabilidad penal:** Referencia explícita en la motivación a que la sola titularidad no equivale a responsabilidad penal, y desarrollo de los elementos adicionales que la sustentan.

- d) **Estándar de motivación exigido para la condena o la absolución:** Nivel de suficiencia argumentativa exigido por el juzgador para considerar superada la duda razonable sobre la condición de mero titular registral.

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1. Enfoque de investigación

La presente investigación se desarrolló bajo un enfoque cualitativo, siguiendo los lineamientos metodológicos propuestos por Hernández-Sampieri y Mendoza (2018) para la denominada "ruta cualitativa" de investigación. Este enfoque resultó pertinente porque el objeto de estudio —los criterios jurídicos y probatorios empleados para atribuir responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados— constituyó un fenómeno de naturaleza argumentativa e interpretativa, cuya comprensión exigió el análisis del significado que los propios operadores jurídicos atribuyeron a los hechos indicadores, y no la medición estadística de variables.

Conforme señalan Hernández-Sampieri y Mendoza (2018), la ruta cualitativa se orienta a comprender los fenómenos desde la perspectiva de los participantes, en su ambiente natural y en relación con su contexto, privilegiando la profundidad de significados sobre la generalización estadística. La presente investigación adoptó, además, un diseño de triangulación de fuentes, al recurrir simultáneamente al análisis documental de sentencias judiciales y a la entrevista semiestructurada aplicada a operadores jurídicos y a un perito informático forense, lo que permitió contrastar el patrón argumentativo efectivamente plasmado en las resoluciones judiciales con la experiencia y los criterios que los propios actores del sistema de justicia declararon emplear en su práctica profesional.

4.2. Tipo de investigación

La investigación fue de tipo básica o pura, en la medida en que su finalidad consistió en generar conocimiento sobre los criterios de atribución de responsabilidad penal al titular de la cuenta receptora, sin un propósito de intervención inmediata sobre la realidad estudiada, aunque sus resultados pueden orientar, de manera mediata, la formulación de recomendaciones de política judicial. Por su alcance, la investigación fue de tipo descriptivo-interpretativo, pues

no se limitó a describir el contenido de las sentencias y de las entrevistas, sino que buscó interpretar el sentido y la coherencia interna del razonamiento judicial empleado para diferenciar al titular meramente registral del titular con conocimiento y voluntad de participar en el fraude.

4.3. Diseño de investigación

El diseño de investigación correspondió al estudio de casos de tipo múltiple, en la modalidad de análisis de contenido de documentos judiciales, complementado con una guía de entrevista semiestructurada. Se optó por este diseño porque permitió examinar en profundidad un número reducido de unidades de análisis —cinco sentencias— seleccionadas por su relevancia y representatividad respecto del fenómeno estudiado, antes que por su cantidad, priorizando la riqueza descriptiva y la posibilidad de un análisis pormenorizado de cada resolución.

Conforme a lo señalado por Hernández-Sampieri y Mendoza (2018), en los diseños cualitativos la muestra no busca ser representativa en términos probabilísticos, sino que se selecciona por su capacidad de aportar riqueza, profundidad y calidad de información sobre el fenómeno estudiado. Por ello, la muestra documental de la presente investigación se integró deliberadamente con expedientes que presentaron variación relevante en las categorías de análisis: casos con y sin alegación de terceros no identificados, casos resueltos por conclusión anticipada y por juicio contradictorio, y casos con resultado condenatorio y absolutorio.

3.4. Escenario de estudio

El estudio se desarrolló en el ámbito del distrito judicial de Ayacucho, específicamente respecto de sentencias emitidas por los Juzgados Penales Unipersonales de la Corte Superior de Justicia de Ayacucho, con sede en la provincia de Huamanga, durante el periodo 2022-2024. Las entrevistas se aplicaron a operadores jurídicos y a un perito informático forense que se desempeñan o intervinieron en dicho distrito judicial.

4.5. Sujetos de estudio

4.5.1. Unidades de análisis documental

Criterio	Descripción
Unidad de análisis	Sentencias emitidas por los Juzgados Penales Unipersonales de la Corte Superior de Justicia de Ayacucho por el delito de fraude informático (artículo 8 de la Ley N.º 30096), en las que se atribuyó responsabilidad penal al titular de la cuenta receptora.
Población	Conjunto de sentencias emitidas por dicho delito en el distrito judicial de Ayacucho durante el periodo 2022-2024.
Muestra	Cinco sentencias, seleccionadas mediante muestreo intencional, que presentaron variación relevante en cuanto a la alegación de terceros no identificados (tres casos con dicha alegación y dos sin ella), la vía procesal (tres por conclusión anticipada y dos por juicio contradictorio) y el resultado (cuatro condenatorios y uno absolutorio).
Criterios de inclusión	Sentencias firmes o consentidas, emitidas por el delito de fraude informático previsto en el artículo 8 de la Ley N.º 30096, con acceso público a su contenido íntegro, en las que el titular de una cuenta bancaria fue procesado como imputado.
Criterios de exclusión	Resoluciones distintas a la sentencia (autos, disposiciones fiscales), y sentencias por modalidades delictivas informáticas distintas al fraude informático.

3.5.2. Participantes de la entrevista

Criterio	Descripción
Población	Jueces penales unipersonales, fiscales provinciales y adjuntos provinciales, abogados penalistas y peritos informáticos forenses del distrito judicial de Ayacucho con experiencia en procesos por fraude informático.
Muestra	Nueve participantes: tres jueces penales unipersonales, tres fiscales provinciales y adjuntos provinciales, dos abogados penalistas con experiencia en la defensa técnica de titulares de cuentas receptoras, y un perito informático forense, seleccionados mediante muestreo intencional.
Criterios de inclusión	Contar con experiencia mínima de tres años en el ejercicio de su función; haber intervenido directamente en al menos un proceso o investigación por fraude informático; aceptar voluntariamente su participación mediante consentimiento informado.
Criterios de exclusión	Operadores jurídicos o peritos sin experiencia previa en casos de fraude informático; personas que no otorgaron su consentimiento informado; participantes con intervención directa y vigente en un caso cuya información se encontraba sujeta a reserva.

4.7. Técnicas e instrumentos de recolección de datos

a) Análisis documental

Se empleó la técnica del análisis documental para el examen de las sentencias que conformaron la muestra, mediante el instrumento de la ficha de análisis documental, diseñada para registrar, respecto de cada sentencia, la titularidad y vigencia de la cuenta receptora, la existencia y naturaleza del acto de disposición del dinero, la alegación fiscal sobre terceros no identificados, las hipótesis alternativas planteadas por la defensa y su tratamiento judicial, y la estructura de la inferencia empleada para atribuir o descartar la responsabilidad penal del titular.

b) Entrevista semiestructurada

Se empleó la técnica de la entrevista semiestructurada para recoger la experiencia y los criterios de los operadores jurídicos y del perito informático forense, mediante el instrumento de la guía de entrevista, compuesta por nueve preguntas abiertas organizadas en las tres categorías apriorísticas antes señaladas, con preguntas complementarias de profundización formuladas durante su aplicación.

c) Validez y confiabilidad de los instrumentos

La validez de los instrumentos se sustentó en el juicio de expertos: tanto la ficha de análisis documental como la guía de entrevista fueron sometidas a la revisión de especialistas en derecho penal, derecho procesal penal y metodología de la investigación jurídica, quienes evaluaron la pertinencia, relevancia y claridad de cada ítem respecto de las categorías y los problemas de la investigación. Conforme señalan Hernández-Sampieri y Mendoza (2018), en la investigación cualitativa la confiabilidad no se sustenta en coeficientes estadísticos, sino en criterios de rigor propios de este enfoque —dependencia, credibilidad, transferencia y confirmación—, desarrollados en el apartado correspondiente del presente capítulo.

4.8. Procedimiento de recolección de datos

La recolección de la información se desarrolló en dos etapas. En la primera etapa se identificaron y solicitaron, a través de los canales institucionales correspondientes y de la información de acceso público disponible en el sistema de notificaciones electrónicas del Poder Judicial, las sentencias que conformaron la muestra documental, procediéndose a su lectura integral y al registro de la información pertinente en la ficha de análisis documental diseñada para tal efecto.

En la segunda etapa se contactó a los participantes seleccionados para las entrevistas, explicándoseles el objetivo académico de la investigación y solicitándoseles su consentimiento informado. Las entrevistas se aplicaron de manera presencial o virtual, según la disponibilidad de cada participante, con una duración aproximada de entre treinta y cinco y cuarenta y cinco minutos, y fueron registradas mediante notas y, previa autorización expresa, mediante grabación de audio, para su posterior transcripción y codificación.

4.9. Método de análisis de la información

La información obtenida a través de ambos instrumentos fue procesada mediante la técnica del análisis de contenido cualitativo, consistente en la codificación de los datos conforme a las categorías y subcategorías previamente definidas, lo que permitió identificar unidades de análisis, patrones recurrentes, coincidencias y diferencias tanto al interior de cada fuente de información como entre ambas fuentes.

Siguiendo el esquema de presentación de resultados propuesto por Williams, Unrau y Grinnell (2005) y desarrollado por Hernández-Sampieri y Mendoza (2018) para la ruta cualitativa, la narrativa de resultados se organizó por categorías, respaldando cada una con ejemplos de segmentos o citas textuales de los participantes, las anotaciones interpretativas del investigador, y las relaciones identificadas entre las distintas categorías. Una vez codificada la información, se procedió a la triangulación de los resultados obtenidos del análisis documental

y de las entrevistas, contrastando, categoría por categoría, los hallazgos provenientes de ambas técnicas.

4.10. Rigor científico

Criterio	Descripción
Dependencia	Se garantizó mediante el diseño de instrumentos estructurados a partir de una matriz de categorización apriorística clara y consistente, y mediante el registro sistemático del procedimiento seguido para la recolección y el análisis de la información, de modo que dicho proceso resultara auditable por otros investigadores.
Credibilidad	Se sustentó en la triangulación de fuentes (análisis documental y entrevistas) y de técnicas de recolección de información, así como en la revisión de los instrumentos por juicio de expertos, lo que permite sostener que los hallazgos reflejan de manera fidedigna el fenómeno estudiado.
Transferencia	Se procuró mediante la descripción detallada del contexto, de los participantes y de las condiciones en que se desarrolló la investigación, de modo que otros investigadores puedan valorar la posibilidad de transferir los hallazgos a contextos similares, sin que ello implique una generalización estadística de los resultados.
Confirmación	Se sustentó en el carácter documental y verificable de la principal fuente de información —las sentencias judiciales, de acceso público—, así como en la codificación sistemática de las entrevistas conforme a categorías predefinidas, minimizando la influencia de las apreciaciones subjetivas del investigador en la interpretación de los resultados.

4.11. Aspectos éticos

La presente investigación se desarrolló con estricto respeto a los principios éticos que rigen la investigación científica en ciencias sociales y jurídicas. Respecto de las sentencias analizadas, se trató de resoluciones judiciales de acceso público, por lo que su empleo no vulneró derecho alguno a la privacidad; no obstante, en la presentación de los resultados se procuró un uso estrictamente académico de la información, evitando cualquier juicio de valor sobre la actuación de los magistrados o las partes involucradas en los procesos analizados, y limitando el análisis a la estructura argumentativa de las resoluciones.

Respecto de las entrevistas, se garantizó la participación voluntaria de los entrevistados mediante la suscripción de un consentimiento informado, en el que se les explicó el objetivo

académico de la investigación, la confidencialidad de sus respuestas, y su derecho a abstenerse de responder cualquier pregunta o a retirarse de la entrevista en cualquier momento. La identidad de los participantes fue protegida mediante la asignación de códigos alfanuméricos, y en ningún momento se solicitó información que permitiera identificar casos concretos, personas investigadas, agraviadas o sentenciadas sujetas a reserva.

CAPÍTULO V: PRESENTACIÓN DE RESULTADOS

El capítulo presenta los resultados obtenidos mediante el análisis de cinco sentencias por fraude informático emitidas en el Distrito Judicial de Ayacucho entre 2022 y 2024 y de nueve entrevistas semiestructuradas realizadas a operadores jurídicos y a un especialista técnico. La exposición se organizó conforme a las tres categorías de la investigación: valor jurídico-probatorio de la titularidad, recepción y disposición de los fondos; valoración de la intervención de sujetos no identificados y de las hipótesis alternativas; y construcción de la inferencia que permite distinguir al titular meramente registral del titular que actuó con conocimiento y voluntad.

El análisis tuvo carácter cualitativo. Las frecuencias consignadas se emplearon únicamente como apoyo descriptivo para mostrar recurrencias dentro de la muestra y no como fundamento de generalización estadística. La interpretación se concentró en el contenido y alcance de los argumentos exteriorizados en las sentencias y en las coincidencias, diferencias y matices advertidos entre los perfiles entrevistados.

Para evitar una comparación metodológicamente incorrecta, se distinguieron las decisiones dictadas mediante conclusión anticipada de aquellas emitidas después de un juicio con actuación probatoria contradictoria. Las sentencias conformadas permitieron conocer la estructura de la imputación aceptada y los hechos admitidos; sin embargo, no fueron consideradas equivalentes a las sentencias contradictorias para evaluar la suficiencia de la prueba, el descarte de contraindicios o la respuesta a hipótesis alternativas.

5.2. Caracterización de las unidades de análisis

5.2.1. Muestra documental

La muestra documental estuvo conformada por cinco sentencias. Cuatro culminaron con condena y una con absolución. Tres condenas fueron emitidas mediante conclusión anticipada, mientras que la condena restante y la absolución se dictaron después de actuación

probatoria contradictoria. Esta distribución fue relevante porque la comparación entre las dos sentencias contradictorias permitió observar con mayor claridad los criterios que separaron la mera recepción del dinero de la intervención penalmente relevante.

Tabla 1
Caracterización de las sentencias analizadas

Código	Expediente y año	Tipo y decisión	Rasgos relevantes
S-01	00477-2023-59-0501-JR-PE-04 2024	Conclusión anticipada Condena	Cuenta abierta siete días antes; recepción de S/ 29 800; conversión casi inmediata en criptomonedas vinculadas al acusado.
S-02	00724-2020-83-0501-JR-PE-06 2022	Juicio contradictorio Absolución	Recepción de S/ 4 620 acreditada; no se individualizó a quien realizó la manipulación ni el retiro; ausencia de cámaras y ubicación del retiro.
S-03	01263-2019-33-0501-JR-PE-05 2024	Conclusión anticipada Condena	Dos receptores identificados; transferencias a sus cuentas y retiros en efectivo atribuidos a los titulares.
S-04	01342-2022-33-0501-JR-PE-04 2024	Juicio contradictorio Condena	Terceros no identificados; dos transferencias por S/ 9 725; retiros presenciales parciales con tarjeta y clave; cuenta luego bloqueada; pérdida no corroborada.
S-05	02815-2019-9-0501-JR-PE-06 2023	Conclusión anticipada Condena	Coordinación atribuida con sujetos no identificados; recepción de S/ 1 610; aceptación de cargos; fundamentación inferencial limitada por la conformidad.

En las cinco sentencias se acreditó que el dinero sustraído ingresó a una cuenta de titularidad de la persona procesada. No obstante, el comportamiento posterior fue diferente. En S-01 existió conversión del dinero en criptomonedas; en S-03 se consignaron retiros en efectivo; y en S-04 se acreditaron dos retiros presenciales por un total de S/ 710 mediante tarjeta y clave. En S-02 se sostuvo que el dinero había sido retirado, pero no se acreditó quién efectuó la operación. En S-05 la sentencia conformada reprodujo la imputación y la aceptación del acusado, sin desarrollar con igual precisión un acto posterior individualizado de disposición.

5.2.2. Muestra de entrevistados

La muestra personal estuvo integrada por nueve participantes seleccionados intencionalmente por su experiencia en el juzgamiento, investigación, defensa o análisis técnico de casos de fraude informático. Se entrevistó a tres jueces penales, tres fiscales penales, dos abogados penalistas y un perito informático forense. La pluralidad de perfiles permitió contrastar la perspectiva decisoria y acusatoria con la visión defensiva y la explicación técnica.

Tabla 2
Perfil de los participantes

Código	Perfil	Experiencia	Aporte al análisis
JP-01	Juez penal unipersonal	14 años	Experiencia en sentencias condenatorias y absolutoria con terceros no identificados.
JP-02	Juez penal unipersonal	11 años	Procesos con pluralidad de imputados y terceros no individualizados.
JP-03	Juez penal unipersonal	17 años	Juicios orales de fraude informático con ejecución colectiva.
FP-01	Fiscal provincial penal	13 años	Sustentación de acusaciones con terceros no identificados.
FP-02	Fiscal adjunto provincial	8 años	Elaboración de acusaciones contra titulares de cuentas receptoras.
FP-03	Fiscal adjunto provincial	6 años	Revisión y sustentación en etapa intermedia.
AP-01	Abogado penalista	15 años	Defensa de titulares de cuentas receptoras.
AP-02	Abogado penalista	9 años	Patrocinio en investigaciones por fraude informático.
PI-01	Perito informático forense	10 años	Pericias digitales en investigaciones con pluralidad de intervinientes.

5.2.3. Organización y tratamiento de la información

Las sentencias fueron codificadas como S-01 a S-05 y los participantes mediante códigos funcionales: JP para jueces penales, FP para fiscales penales, AP para abogados penalistas y PI para el perito informático. La información fue segmentada conforme a las

categorías y subcategorías apriorísticas. Posteriormente se efectuó una comparación intrafuente, entre sentencias y entre entrevistas, y una comparación interfuente para establecer convergencias, divergencias y vacíos.

En la fuente documental se examinó la diferencia entre hechos acreditados, imputaciones aceptadas y conclusiones inferidas. En la fuente testimonial se identificaron unidades de significado reiteradas: titularidad como punto de partida, disposición personal como indicador central, necesidad de vincular al tercero no identificado, verificación de explicaciones alternativas, importancia de la evidencia técnica y exigencia de motivación inferencial explícita.

5.3. Resultados de la categoría 1: Valor jurídico-probatorio de la titularidad, recepción y disposición

5.3.1. Titularidad formal de la cuenta receptora

El análisis documental mostró que la titularidad constituyó el punto común de las cinco decisiones. En todos los casos, los reportes bancarios permitieron identificar que la cuenta de destino se encontraba registrada a nombre del procesado. Este dato sirvió para iniciar la vinculación personal y reconstruir el recorrido financiero; sin embargo, su alcance para demostrar conocimiento y voluntad fue diferente según la presencia de otros hechos.

La sentencia S-02 estableció con particular claridad el límite de este dato. Aunque se acreditó que el dinero ingresó a la cuenta de la acusada, el juzgado consideró que ninguna prueba corroboró su participación en la transferencia ni permitió establecer quién retiró posteriormente los fondos. La titularidad permitió ubicar el destino del dinero, pero no individualizó al sujeto que efectuó la manipulación informática o la disposición.

En S-04, por el contrario, la titularidad se integró con retiros presenciales, el uso de tarjeta y clave y la ausencia de denuncia o bloqueo oportuno. Por ello, no operó como fundamento autónomo de la condena, sino como parte de una secuencia indiciaria. En las

sentencias conformadas S-01, S-03 y S-05, la titularidad se incorporó a los hechos aceptados, pero el reconocimiento de cargos redujo la necesidad de justificar contradictoriamente su alcance.

Las nueve entrevistas coincidieron en que la titularidad constituye un punto de partida, pero no prueba por sí sola la responsabilidad. JP-01 la calificó como “apenas el punto de partida del análisis”; FP-01 sostuvo que es un elemento “necesario pero no suficiente”; y PI-01 indicó que, desde la perspectiva técnica, la titularidad no informa quién ejecutó materialmente cada operación. Los abogados defensores acentuaron su neutralidad, mientras que jueces y fiscales reconocieron su utilidad para orientar la investigación.

5.3.2. Recepción efectiva de los fondos

La recepción fue acreditada documentalmente en las cinco sentencias mediante movimientos o información bancaria. Este hecho confirmó la ruta del dinero y la conexión objetiva entre la transferencia fraudulenta y la cuenta receptora. No obstante, los resultados demostraron que el ingreso del dinero no requiere necesariamente una acción del titular, pues puede ser producido unilateralmente por quien controla el acceso a la cuenta de origen o por un tercero que conoce los datos de la cuenta destino.

La relevancia de esta distinción se evidenció nuevamente en S-02: la materialidad del fraude y el destino de los fondos fueron acreditados, pero no la responsabilidad penal de la titular. El juzgado separó la prueba de la transferencia de la prueba de la intervención personal. Esta separación constituyó el principal fundamento de la absolución.

Los nueve entrevistados consideraron insuficiente la sola recepción cuando no existe un acto posterior atribuible al titular u otros indicios de coordinación. Los jueces y fiscales la caracterizaron como un indicio de valor intermedio o una imputación débil; los defensores la consideraron un hecho neutral; y el perito señaló que el ingreso de fondos no exige actuación

alguna del titular receptor. La diferencia fue de intensidad, no de conclusión: ningún participante sostuvo que la sola recepción fuera suficiente para condenar.

5.3.3. Actos posteriores de disposición

Los actos de disposición presentaron el mayor potencial diferenciador. En S-01, el dinero recibido fue destinado casi inmediatamente a la adquisición de criptomonedas vinculadas al acusado. La cercanía temporal, la apertura reciente de la cuenta y el uso posterior de los fondos conformaron una secuencia compatible con control consciente. Sin embargo, al tratarse de una sentencia conformada, la conclusión se apoyó también en la aceptación de la acusación.

En S-03, las transferencias fueron seguidas por retiros en efectivo atribuidos a los titulares de las cuentas receptoras. La sentencia consignó que uno de los imputados retiró S/ 1 490 y el otro realizó dos retiros por S/ 1 400 y S/ 80. Estos hechos fueron aceptados mediante conclusión anticipada y reforzaron la correspondencia entre recepción y aprovechamiento.

S-04 ofreció el desarrollo contradictorio más completo. El juzgado tuvo por acreditado que, luego de recibir una primera transferencia de S/ 715, la acusada realizó retiros por S/ 500 y S/ 210 mediante tarjeta y clave. La segunda transferencia, por S/ 9 010, no fue retirada porque la cuenta fue bloqueada. El valor incriminatorio no provino de que todo el dinero hubiera sido dispuesto, sino de la atribución personal de retiros parciales inmediatamente vinculados con la recepción.

En S-02, la acusación sostuvo que hubo retiro, pero no se produjo información sobre el lugar, la cámara del cajero o la identidad de la persona que dispuso de los fondos. El juzgado consideró que esa omisión impedía inferir participación o conocimiento. La comparación S-02/S-04 reveló que no basta la existencia contable de un egreso: resulta decisivo individualizar a quien ejecutó el acto de disposición.

Las entrevistas confirmaron esta gradación. Los nueve participantes asignaron mayor fuerza a los retiros presenciales acreditados mediante tarjeta, clave e imagen. Jueces y fiscales también destacaron la inmediatez y la conversión en criptomonedas como signos de premura y control. Los defensores aceptaron la relevancia del retiro solo cuando la autoría material estuviera plenamente demostrada. PI-01 explicó que las operaciones electrónicas requieren registros de IP, dispositivo y ubicación, mientras que los retiros presenciales pueden contar con imágenes de cajero o ventanilla.

5.3.4. Síntesis de la primera categoría

Tabla 3

Peso probatorio observado en la primera categoría

Hecho	Resultado documental	Resultado de entrevistas	Interpretación
Titularidad	Presente en 5/5; por sí sola no explicó el sentido del fallo.	9/9: punto de partida o dato neutral.	Identifica la cuenta, no necesariamente al ejecutor.
Recepción	Acreditada en 5/5; compatible tanto con condena como con absolución.	9/9: insuficiente sin corroboración adicional.	Demuestra destino del dinero, no conocimiento.
Disposición personal	Clara en S-01, S-03 y S-04; no individualizada en S-02; limitada en S-05.	9/9: indicador de mayor fuerza, con exigencia de atribución personal.	Aumenta la fuerza cuando existe proximidad temporal y respaldo técnico.
Control efectivo	Derivado de tarjeta, clave, cuenta reciente, retiros o conversión.	Consenso en vincularlo con medios de acceso y comportamiento posterior.	Conecta el dato registral con una conducta consciente.

En respuesta al primer objetivo específico, se determinó que la titularidad y la recepción tuvieron valor de vinculación inicial, mientras que los actos posteriores de disposición, siempre que fueran personalmente atribuibles, concentraron el mayor valor probatorio. La evidencia documental y testimonial no respaldó una regla automática según la cual la cuenta receptora convierte a su titular en responsable penal.

5.4. Resultados de la categoría 2: Valoración de la intervención de sujetos no identificados y de las hipótesis alternativas

5.4.1. Intervención de sujetos no identificados

La intervención de sujetos no identificados apareció expresamente en S-02, S-04 y S-05. En estos casos, la imputación distribuyó funciones: el tercero habría realizado la manipulación técnica y el titular habría facilitado o utilizado la cuenta receptora. En S-01 la acusación atribuyó al propio procesado la captación de datos y la operación, mientras que en S-03 existieron dos coimputados identificados. Esta diferencia mostró que la presencia de un tercero desconocido incrementó la necesidad de explicar el enlace entre la manipulación y el titular.

En S-02, la fórmula de actuación conjunta con un tercero no identificado no estuvo acompañada de comunicaciones, registros técnicos o prueba de retiro personal. El juzgado concluyó que la recepción del dinero no corroboraba mínimamente la coordinación imputada. En S-04, la intervención del tercero fue considerada compatible con la responsabilidad de la titular porque se integró con los retiros parciales y con el descarte de la explicación defensiva. En S-05, la coordinación fue aceptada dentro de la conclusión anticipada, razón por la cual la sentencia no exteriorizó el mismo nivel de comprobación autónoma.

Los entrevistados coincidieron en que la sola frase “en coordinación con sujetos no identificados” no debe funcionar como sustituto de la prueba. Los tres jueces exigieron elementos objetivos de vinculación; los tres fiscales indicaron que la acusación debe incorporar indicios adicionales, como apertura temporalmente cercana, patrones reiterados, comunicaciones o beneficios; los defensores advirtieron que la fórmula puede concentrar indebidamente la persecución en el único sujeto identificable; y el perito consideró técnicamente plausible que el tercero opere sin conocimiento del titular.

5.4.2. Pérdida de tarjeta o documentos y falta de bloqueo

La hipótesis de pérdida adquirió especial relevancia en S-04. La defensa sostuvo que la acusada había perdido la tarjeta en Lima. El juzgado contrastó esa afirmación con la falta de denuncia policial, la inexistencia de bloqueo oportuno y los retiros realizados con tarjeta y clave. La explicación fue descartada no solo por ausencia documental, sino por su incompatibilidad con el conjunto de hechos que el órgano jurisdiccional tuvo por acreditados.

En las entrevistas se observó una diferencia de enfoque. Los jueces y fiscales, seis participantes, asignaron importancia a la denuncia previa o inmediata y a la gestión de bloqueo. Consideraron que la omisión de ambas medidas debilita la hipótesis, especialmente cuando la explicación aparece recién durante el juicio. Los abogados defensores rechazaron que la denuncia sea el único criterio, pues su ausencia puede responder a desconocimiento o limitaciones del investigado. PI-01 propuso verificar registros de acceso, dispositivos y ubicaciones antes de aceptar o descartar técnicamente el uso no autorizado.

La triangulación permitió precisar que la ausencia de denuncia no fue entendida de manera uniforme. Para jueces y fiscales constituyó un contraindicio importante, pero no necesariamente autónomo. Para defensores y perito debía integrarse con el contexto personal y con evidencia técnica. El resultado emergente fue que convertir la falta de denuncia en prueba directa de culpabilidad implicaría trasladar al investigado una carga que corresponde inicialmente a la acusación.

5.4.3. Préstamo, suplantación y utilización no autorizada

Las sentencias no desarrollaron de forma uniforme estas hipótesis. S-02 mantuvo la posibilidad de intervención autónoma de un tercero porque la investigación no identificó al ejecutor ni al responsable del retiro. S-04 descartó la versión defensiva por los retiros atribuidos y la ausencia de respaldo objetivo. Las sentencias conformadas no ofrecieron un debate equivalente, debido a la aceptación de los hechos.

Los jueces y fiscales exigieron respaldo técnico o testimonial para considerar creíble la suplantación o el uso no autorizado. Los defensores enfatizaron que phishing y spoofing hacen técnicamente posible el uso de datos sin conocimiento del titular y solicitaron que la acusación descarte esa posibilidad. El perito señaló como datos relevantes los accesos desde dispositivos o lugares no habituales, los metadatos de conexión y las comunicaciones relacionadas con préstamos o alquileres de cuentas.

La diferencia entre perfiles se concentró en el punto de partida probatorio. La posición acusatoria exigió que la hipótesis defensiva presente soporte verificable; la defensa sostuvo que la plausibilidad técnica impide presumir la intervención consciente; y la perspectiva pericial propuso resolver la tensión mediante evidencia objetiva. A pesar de esa divergencia, todos coincidieron en que la hipótesis debe ser contrastada y no aceptada o rechazada mediante afirmaciones generales.

5.4.4. Síntesis de la segunda categoría

Tabla 4

Tratamiento de terceros no identificados e hipótesis alternativas

Aspecto	Sentencias	Entrevistas	Hallazgo
Tercero no identificado	Expreso en S-02, S-04 y S-05; resultado diferente según corroboración.	9/9 rechazaron que la mención genérica sea suficiente.	Debe probarse el vínculo funcional con el titular.
Pérdida de tarjeta	Desarrollada y descartada en S-04; vinculada a retiros y falta de denuncia/bloqueo.	Jueces y fiscales priorizan denuncia y bloqueo; defensa exige contexto.	La omisión es un dato de valoración, no prueba autónoma.
Uso no autorizado	Permaneció plausible en S-02; descartado en S-04.	Todos exigen contraste; PI-01 prioriza registros técnicos.	La evidencia técnica permite corroborar o refutar la alternativa.
Conclusión anticipada	S-05 aceptó coordinación sin debate probatorio exhaustivo.	Los participantes reclamaron motivación y corroboración.	No debe equipararse conformidad con comprobación contradictoria.

En respuesta al segundo objetivo específico, se estableció que la falta de identificación del ejecutor técnico no excluyó automáticamente la responsabilidad del titular, pero elevó la exigencia de acreditar el vínculo funcional. Las hipótesis alternativas fueron decisivas cuando permanecieron compatibles con la evidencia y no se individualizó el acto de disposición, como en S-02; fueron descartadas cuando existieron hechos contrapuestos, como en S-04.

5.5. Resultados de la categoría 3: construcción y motivación de la inferencia probatoria entre el titular registral y el titular con conocimiento y voluntad.

5.5.1. Hechos indicadores del conocimiento y la voluntad

La comparación documental permitió identificar una gradación. La titularidad fue el hecho inicial; la recepción confirmó el destino; el control efectivo y la disposición personal constituyeron los indicadores más cercanos al conocimiento y la voluntad. Otros datos reforzaron la inferencia: apertura de la cuenta pocos días antes, rapidez del retiro, conversión en criptomonedas, utilización de tarjeta y clave y ausencia de actuación compatible con una pérdida real.

S-04 exteriorizó la inferencia más desarrollada entre las decisiones condenatorias: cuenta a nombre de la acusada, recepción de dos transferencias, retiros parciales el mismo día con tarjeta y clave, falta de denuncia y de bloqueo y explicación defensiva no corroborada. S-02 mostró la inferencia negativa: acreditada la cuenta y la recepción, faltaron datos sobre el retiro, lugar, imágenes y participación en la manipulación; por ello, no fue posible pasar del hecho objetivo a la conclusión subjetiva.

Las sentencias conformadas presentaron una limitación estructural. En S-01 y S-03 existieron hechos posteriores fuertes, pero la aceptación de cargos redujo la controversia. En S-05, la sentencia afirmó coordinación y responsabilidad apoyándose en la conformidad, sin desplegar una regla inferencial comparable a S-04. Por ello, los resultados no permitieron afirmar que las cuatro condenas compartieran un mismo estándar de motivación.

5.5.2. Regla inferencial y valoración conjunta

La regla inferencial que emergió de las fuentes puede expresarse de la siguiente forma: cuando el titular mantuvo control efectivo de los medios de acceso y realizó personalmente actos de disposición cercanos a la recepción, sin que exista una explicación alternativa objetivamente respaldada, aumenta razonablemente la probabilidad de que conociera y quisiera participar en el circuito fraudulento. Esta regla no opera de forma automática y depende de la acreditación independiente de cada premisa.

Los tres jueces describieron una secuencia formada por control efectivo, acto personalísimo de disposición y descarte razonado de alternativas. Los fiscales reprodujeron la misma estructura para la acusación. Los defensores añadieron que debe acreditarse de manera indubitable la autoría material del acto de disposición. PI-01 sostuvo que los registros de acceso y metadatos deben complementar las inferencias derivadas del comportamiento bancario.

El consenso se situó en la estructura, mientras que la divergencia apareció en el nivel de corroboración requerido. Jueces y fiscales otorgaron fuerza a la combinación de tarjeta, clave, proximidad temporal y ausencia de denuncia; defensores y perito exigieron una atribución técnica más directa. Esta diferencia reflejó distintas funciones procesales, pero no alteró el acuerdo central: no es válido inferir conocimiento únicamente desde la titularidad.

5.5.3. Diferenciación entre titular registral y responsable penal

La distinción se encontró expresamente desarrollada en S-02, al separar el destino del dinero de la identidad de quien ejecutó la operación. En S-04 la diferenciación fue implícita, pues la condena se apoyó en datos adicionales. En las sentencias conformadas predominó la reproducción de los hechos aceptados, lo que impidió evaluar con igual profundidad si el órgano jurisdiccional había construido autónomamente la distinción.

Los nueve entrevistados afirmaron que la motivación debe explicar por qué el caso supera la mera titularidad. JP-03 distinguió entre el hecho objetivo de titularidad y el elemento

subjetivo de conocimiento y voluntad. FP-01 indicó que el requerimiento debe exponer el razonamiento que conecta ambos niveles. AP-02 reclamó que se descarte expresamente que el titular sea una víctima adicional. PI-01 propuso incorporar el análisis técnico de la plausibilidad de las hipótesis alternativas.

5.5.4. Suficiencia de la motivación

La suficiencia no dependió de la extensión de la sentencia, sino de la exteriorización del enlace entre los hechos. S-02 justificó la absolución al identificar las diligencias y datos ausentes. S-04 fundamentó la condena mediante una cadena de hechos convergentes, aunque parte de su razonamiento descansó en máximas relacionadas con el carácter personal de la tarjeta y la clave. Las sentencias conformadas presentaron menor desarrollo inferencial por la naturaleza del mecanismo procesal.

Las propuestas de los entrevistados se agruparon en cuatro ejes: protocolos o guías para diferenciar titularidad y responsabilidad; capacitación conjunta de jueces, fiscales y defensores; fortalecimiento de la pericia informática; y conservación oportuna de registros bancarios, imágenes, IP, dispositivos y metadatos. La recurrencia de estas propuestas evidenció que la principal dificultad no fue solamente normativa, sino también metodológica y operativa.

5.5.5. Síntesis de la tercera categoría

Tabla 5
Estructura inferencial identificada

Componente	Contenido identificado	Riesgo advertido	Exigencia resultante
Hecho inicial	Titularidad y recepción del dinero.	Confundir trazabilidad financiera con autoría.	No atribuir responsabilidad automática.
Hechos de enlace	Control de tarjeta/clave, retiro personal, rapidez, conversión, comunicaciones.	Atribuir al titular actos electrónicos ejecutables por terceros.	Individualizar el acto y su autor.

Hipótesis alternativa	Pérdida, préstamo, suplantación o uso no autorizado.	Invertir la carga de la prueba por falta de denuncia.	Contrastar con datos objetivos y contexto.
Regla de inferencia	Control + disposición personal + convergencia + descarte razonado.	Usar fórmulas genéricas o máximas no explicadas.	Exteriorizar el tránsito al conocimiento y voluntad.
Conclusión	Participación consciente o permanencia de duda razonable.	Equiparar condena conformada con valoración contradictoria.	Precisar el alcance procesal de cada sentencia.

En respuesta al tercer objetivo específico, se determinó que la inferencia válida requirió separar el hecho registral, los hechos de enlace y la conclusión subjetiva. La motivación resultó más controlable cuando identificó qué dato probaba el control, qué acto demostraba disposición y por qué las alternativas no explicaban razonablemente el conjunto.

5.6. Triangulación de los resultados

La triangulación mostró una convergencia sustancial entre documentos y entrevistas. La sentencia absolutoria S-02 confirmó la tesis compartida por los participantes de que la titularidad y la recepción no bastan. La condenatoria S-04 reflejó la secuencia defendida por jueces y fiscales: control, disposición personal y descarte de alternativas. La opinión pericial explicó por qué la falta de cámaras, IP, dispositivos o ubicación debilitó la atribución en S-02 y por qué un retiro presencial puede ofrecer mayor capacidad de individualización.

También se identificó una divergencia. En S-04, el juzgado atribuyó peso importante a la falta de denuncia y bloqueo. Jueces y fiscales respaldaron generalmente ese enfoque; los defensores cuestionaron que se convierta en requisito único; y PI-01 sostuvo que el centro debe estar en los registros técnicos. La síntesis resultante fue que la omisión defensiva puede debilitar una versión, pero no sustituye la prueba positiva del aporte y del conocimiento.

Tabla 6
Matriz de triangulación por categorías

Categoría	Hallazgo documental	Hallazgo testimonial	Resultado integrado
Titularidad, recepción y disposición	La diferencia entre S-02 y S-04 radicó en la individualización de la disposición.	Consenso de 9/9 sobre el valor creciente y la insuficiencia de la sola recepción.	La disposición personal corroborada es el principal hecho de enlace.
Terceros e hipótesis alternativas	La fórmula genérica no bastó en S-02; en S-04 se integró con otros indicios.	Todos exigen vinculación; difieren sobre denuncia y nivel técnico.	La intervención ajena debe analizarse como hipótesis real y contrastable.
Inferencia y motivación	S-02 y S-04 presentan cadenas opuestas; conformadas tienen menor debate.	Consenso sobre control, disposición y descarte razonado.	La motivación debe separar fuente, hecho, inferencia y conclusión.

5.7. Hallazgos emergentes

5.7.1. Asimetría entre trazabilidad financiera y atribución digital

El primer hallazgo emergente fue que la investigación financiera permitió identificar con facilidad el destino de los fondos, mientras que la atribución digital del acceso y de la manipulación presentó mayores vacíos. Esta asimetría explica por qué el titular de la cuenta se convierte en el sujeto visible del proceso, aun cuando el ejecutor técnico permanezca desconocido. La trazabilidad respondió dónde llegó el dinero, pero no siempre quién controló cada operación.

5.7.2. Diferencia entre egreso bancario y disposición personalmente atribuida

El segundo hallazgo consistió en distinguir la existencia contable de un retiro o transferencia posterior de su atribución personal. S-02 demostró que el egreso no identifica automáticamente al ejecutor. Los entrevistados, especialmente defensores y perito, señalaron que las operaciones electrónicas pueden realizarse remotamente y que los retiros requieren imágenes, ubicación u otros datos de corroboración.

5.7.3. Efecto metodológico de la conclusión anticipada

El tercer hallazgo fue la necesidad de clasificar las decisiones según su origen procesal. Las tres sentencias conformadas acreditaron la aceptación de cargos, pero no permitieron reconstruir del mismo modo el enfrentamiento entre hipótesis. Utilizarlas sin esta precisión

produciría una apariencia de uniformidad condenatoria y ocultaría que la diferencia probatoria más informativa se encontró en las dos sentencias contradictorias.

5.7.4. Riesgo de inversión de la carga probatoria

El cuarto hallazgo fue el riesgo de transformar la ausencia de denuncia, bloqueo o explicación documentada en prueba principal de culpabilidad. Tales omisiones pueden integrar la valoración de credibilidad, pero la presunción de inocencia exige que la imputación se apoye primero en hechos positivos. La debilidad de una hipótesis alternativa no completa por sí sola una inferencia acusatoria incompleta.

5.8. Resultado integrado respecto del objetivo general

El objetivo general consistió en analizar la forma en que se atribuyó responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados. Los resultados permitieron establecer que dicha atribución no se sustentó válidamente en un criterio único, sino en la combinación progresiva de hechos: titularidad registral, recepción, control efectivo, disposición personalmente atribuible, proximidad temporal, aprovechamiento y ausencia de una explicación alternativa compatible con los datos objetivos.

La muestra documental mostró dos respuestas opuestas en los procesos contradictorios. Cuando solo se acreditaron la titularidad y el destino del dinero, sin individualizar el retiro ni la manipulación, subsistió duda razonable y se absolvió. Cuando se acreditaron retiros presenciales con tarjeta y clave, se descartó la pérdida alegada y se integraron los hechos dentro de una secuencia convergente, se condenó. Las sentencias conformadas aportaron ejemplos de aceptación de imputaciones con conversión o retiro, pero su fuerza analítica para evaluar suficiencia fue menor.

Las entrevistas confirmaron que el criterio central fue el paso desde una relación registral hacia un comportamiento de control y disposición. Los nueve participantes rechazaron la responsabilidad automática por titularidad. Las diferencias se concentraron en el grado de

corroboración: jueces y fiscales valoraron la combinación de tarjeta, clave, inmediatez, denuncia y bloqueo; defensores y perito exigieron una individualización más estricta mediante imágenes, registros de acceso, dispositivos, IP y metadatos.

En consecuencia, se determinó que la responsabilidad penal del titular solo puede sostenerse cuando la acusación acredita hechos adicionales que revelen su aporte consciente y cuando la motivación explica por qué esos hechos son más compatibles con la participación que con la utilización no autorizada de la cuenta. La intervención de sujetos no identificados no elimina la posibilidad de responsabilidad, pero impide presumirla y eleva la exigencia de individualización y corroboración.

CAPÍTULO VI: DISCUSIÓN DE RESULTADOS

6.1. Discusión del resultado general

El resultado general de la investigación mostró que la responsabilidad penal del titular de la cuenta receptora no se derivó válidamente de la sola titularidad registral ni del ingreso de los fondos, sino de una construcción probatoria progresiva integrada por el control efectivo de la cuenta, la disposición personalmente atribuible, la proximidad temporal, el aprovechamiento económico y el contraste de explicaciones alternativas. Este hallazgo responde al objetivo general porque permite precisar que la cuenta receptora cumple inicialmente una función de trazabilidad financiera, pero solo adquiere significado incriminatorio cuando se conecta con conductas que exteriorizan conocimiento y voluntad. En consecuencia, la identificación del destinatario bancario no puede confundirse con la identificación del autor o coautor del fraude.

Este resultado coincide con Becerra Cervera (2025), quien advirtió que la existencia de tipos penales específicos no ha eliminado las dificultades para brindar una respuesta efectiva frente a la afectación de cuentas bancarias digitales. No obstante, la presente investigación especifica dónde se sitúa una de esas dificultades: no únicamente en la redacción del artículo 8 de la Ley N.º 30096, sino en el tránsito probatorio entre la ruta del dinero y la atribución subjetiva al titular. La contribución del estudio consiste, por tanto, en demostrar que el problema práctico no se resuelve constatando que el dinero llegó a una cuenta determinada, pues esa constatación solo acredita el destino patrimonial de la transferencia.

El hallazgo también guarda correspondencia con Rosales Medina (2025), quien identificó el anonimato del ciberespacio como un factor asociado a la impunidad en los delitos informáticos. Las sentencias analizadas permiten observar el efecto procesal concreto de ese anonimato: mientras el ejecutor técnico permanece oculto, el titular de la cuenta se convierte en el sujeto más fácilmente identificable. Sin embargo, la visibilidad registral no elimina el estándar de prueba. Precisamente, la sentencia S-02 mostró que la imposibilidad de individualizar a quien manipuló el sistema y retiró el dinero mantuvo la duda razonable; la sentencia S-04, en cambio, acreditó datos adicionales que permitieron atribuir personalmente la disposición. De este modo, el anonimato incrementa la dificultad investigativa, pero no autoriza a reducir el umbral probatorio.

Desde la teoría del delito informático, el resultado confirma las características descritas por Morillas Fernández (2017, como se citó en Vinelli Vereau, 2021): ejecución a distancia, anonimato, facilidad de ocultamiento y separación espacial entre intervinientes. Estas características explican la frecuente distribución de funciones entre quien obtiene las

credenciales, quien manipula el sistema y quien recibe o dispone de los fondos. Por ello, el fraude informático no debe ser analizado con una lógica simplificada de autor único. La atribución exige reconstruir el circuito funcional completo y determinar, respecto de cada interviniente, qué aporte realizó, si ese aporte fue consciente y qué evidencia permite sostenerlo.

Asimismo, el resultado es compatible con la concepción restringida del delito informático adoptada en la tesis, porque la manipulación tecnológica constituye un elemento propio de la modalidad prevista en el artículo 8 de la Ley N.º 30096. Sin embargo, el titular de la cuenta no siempre ejecuta esa manipulación. La consecuencia dogmática es relevante: su responsabilidad no puede fundarse en la mera vinculación patrimonial con el resultado, sino en la acreditación de un aporte objetivamente conectado con el plan común y subjetivamente doloso. De lo contrario, se introduciría una forma de responsabilidad objetiva contraria al principio de responsabilidad por el hecho propio y a la presunción de inocencia.

6.2. Discusión respecto del primer objetivo específico: criterios jurídicos para calificar la intervención del titular

El primer objetivo específico estuvo orientado a identificar los criterios jurídicos utilizados para calificar la autoría o coautoría del titular. Los resultados revelaron que las sentencias no desarrollaron esos criterios con igual intensidad. En las decisiones conformadas S-01, S-03 y S-05, la aceptación de cargos redujo la necesidad de confrontar hipótesis y de explicar exhaustivamente el dominio funcional del hecho. En las sentencias dictadas después de juicio contradictorio, la calificación dependió de la posibilidad de vincular al titular con actos de control y disposición. Esta diferencia obliga a evitar que la existencia de cuatro condenas dentro de la muestra sea interpretada como evidencia de un criterio jurisprudencial uniforme.

El hallazgo se relaciona con los artículos 23 a 25 del Código Penal, desarrollados en el marco teórico. La coautoría exige acuerdo común, aporte esencial y dominio funcional, mientras que la complicidad supone un auxilio doloso de diversa intensidad. En ese sentido, facilitar una cuenta puede constituir un aporte relevante, pero su significado jurídico depende del conocimiento del plan y de la función concretamente asumida. Una cuenta facilitada conscientemente para recibir y retirar dinero fraudulento puede integrar el dominio funcional; una cuenta prestada sin conocimiento del origen ilícito no satisface el dolo; y un aporte doloso no esencial podría requerir una calificación distinta de la coautoría. Por ello, la etiqueta procesal no puede sustituir la demostración de sus presupuestos.

Esta interpretación complementa el planteamiento de Rodríguez Pilco y Chimborazo Castillo (2026), quienes señalaron que la criminalidad organizada digital genera dificultades para atribuir responsabilidad dentro de estructuras tecnológicas complejas. La muestra de Ayacucho evidencia que esa complejidad puede presentarse incluso sin que se acredite formalmente una organización criminal: basta la fragmentación de tareas entre un ejecutor técnico desconocido y un titular visible. La respuesta jurídica debe individualizar el aporte de este último y evitar que la falta de identificación de los demás intervinientes sea suplida mediante una afirmación genérica de coordinación.

En particular, la expresión “en coordinación con sujetos no identificados” resultó insuficiente cuando no estuvo acompañada de comunicaciones, beneficios correlativos, patrones de apertura de cuentas, retiros personalmente atribuidos u otros datos objetivos. Esta constatación coincide con la exigencia dogmática de que el acuerdo común pueda inferirse de hechos externos, pero no presumirse por la sola convergencia causal del dinero en una cuenta. La fórmula acusatoria describe una hipótesis, no la prueba de esa hipótesis. Su uso sin respaldo puede producir una imputación circular: se afirma coordinación porque el dinero llegó a la cuenta y se atribuye significado incriminatorio al ingreso porque se presupone coordinación.

La subcategoría emergente relativa al préstamo remunerado o “alquiler” de cuentas confirma la necesidad de una calificación diferenciada. El dato de que una persona haya cedido su cuenta a cambio de una comisión puede demostrar conocimiento de una operación irregular, pero no necesariamente conocimiento del fraude informático específico ni dominio funcional de la manipulación. El hallazgo abre un espacio de análisis entre el titular plenamente consciente y el titular víctima de suplantación. La respuesta dogmática debe examinar el contenido del dolo, la esencialidad del aporte y el momento del acuerdo, sin convertir toda cesión imprudente o socialmente riesgosa en coautoría dolosa.

Por tanto, el primer objetivo específico permitió advertir que el criterio jurídicamente más consistente no es la titularidad, sino el aporte funcional consciente. La calificación de coautor exige justificar por qué el uso de la cuenta y la disposición de los fondos formaron parte de una división de funciones orientada al beneficio ilícito. Cuando ese enlace no se acredita, corresponde evaluar una forma distinta de participación o, si falta el conocimiento requerido, excluir la responsabilidad penal. Esta conclusión preserva la diferencia entre causalidad, contribución objetiva y atribución subjetiva.

6.3. Discusión respecto del segundo objetivo específico: elementos probatorios del conocimiento y la voluntad

El segundo objetivo específico buscó examinar los elementos probatorios capaces de acreditar conocimiento y voluntad. La comparación entre fuentes mostró una gradación estable: titularidad formal, recepción, control efectivo y disposición personalmente atribuible. La titularidad y la recepción se presentaron tanto en la condena como en la absolución, por lo que carecieron de capacidad discriminante suficiente. En cambio, los retiros presenciales con tarjeta y clave, la conversión inmediata en criptomonedas y el aprovechamiento de los fondos incrementaron la fuerza de la hipótesis acusatoria cuando pudieron ser atribuidos al procesado.

Este resultado es coherente con la teoría racionalista de la prueba desarrollada por Ferrer Beltrán (2021) y Gascón Abellán (2005). Un hecho indicador no posee valor incriminatorio por su mera existencia, sino por la relación que mantiene con la hipótesis y por su resistencia frente a explicaciones alternativas. La titularidad es compatible tanto con la participación consciente como con la utilización no autorizada; por ello, su capacidad confirmatoria es limitada. La disposición personal presenta mayor fuerza porque reduce el conjunto de explicaciones compatibles, aunque tampoco debe valorarse aisladamente: es necesario acreditar quién realizó la operación, cómo lo hizo y qué conexión temporal y funcional tuvo con la transferencia fraudulenta.

La diferencia entre S-02 y S-04 ilustra esta exigencia. En S-02 existió constancia del ingreso y posterior egreso, pero no se incorporaron imágenes, ubicación del retiro ni identificación del ejecutor; por ello, el egreso contable no probó la disposición personal. En S-04 se acreditaron retiros presenciales mediante tarjeta y clave, efectuados poco después de la recepción, y la explicación de pérdida no contó con respaldo objetivo. La divergencia entre ambos fallos no respondió únicamente a la existencia de un retiro, sino a su atribución personal y a la capacidad de la evidencia para excluir una actuación autónoma del tercero.

La importancia de la evidencia técnica coincide con Manobanda Guangasi y Chiriboga Sabando (2026), quienes identificaron la cadena de custodia digital como una debilidad del proceso penal contemporáneo, y con Catagua Zambrano y Vera Navarrete (2026), quienes advirtieron brechas de capacitación y diferencias en la capacidad de las herramientas forenses. Los entrevistados de Ayacucho confirmaron esas limitaciones al reclamar imágenes, registros de acceso, dispositivos, direcciones IP, ubicación y metadatos. La ausencia de estos datos no constituye un problema meramente tecnológico: afecta directamente la posibilidad jurídica de individualizar actos y superar la duda razonable.

Los resultados también guardan relación con Quincho Laura, Aylas Dionicio y Arcos Huayhua (2025), quienes identificaron deficiencias en la preservación de pruebas digitales y en la aplicación de los estándares del Convenio de Budapest. La conservación rápida de datos es decisiva porque los registros bancarios, videos, bitácoras de acceso y metadatos pueden perderse o dejar de estar disponibles con el transcurso del tiempo. Cuando la investigación se limita al reporte de titularidad y movimientos, reconstruye la ruta financiera pero no necesariamente la autoría de cada operación. La cooperación oportuna con entidades bancarias y proveedores resulta, por ello, una condición para una atribución individualizada.

El hallazgo relativo a la conversión en criptomonedas debe ser interpretado con la misma cautela. En S-01, la compra casi inmediata de activos vinculados al acusado reforzó el control y el aprovechamiento, pero la sentencia fue conformada. La conversión puede ser un indicador de premura u ocultamiento; sin embargo, su valor depende de que la cuenta o billetera de destino sea atribuida de manera fiable al titular y de que se descarte un acceso remoto. No es la naturaleza del activo la que prueba el dolo, sino la integración del acto dentro de una secuencia personalmente controlada.

En síntesis, el segundo objetivo específico confirmó que el conocimiento y la voluntad se prueban normalmente de manera indiciaria. La inferencia adquiere suficiencia cuando confluyen hechos independientes y concordantes: control de los medios de acceso, disposición personal, proximidad temporal, beneficio y ausencia de datos objetivos compatibles con un uso no autorizado. Ninguno de estos elementos debe transformarse en presunción absoluta; su fuerza depende de la corroboración de las premisas y de su valoración conjunta conforme al estándar más allá de toda duda razonable.

6.4. Discusión respecto del tercer objetivo específico: incidencia de los sujetos no identificados en la motivación

El tercer objetivo específico analizó la incidencia de la falta de individualización del ejecutor técnico en la motivación. Los resultados demostraron que esa falta no impide, por sí sola, atribuir responsabilidad al titular, pero eleva la exigencia argumentativa. Cuando la acusación distribuye funciones entre una persona desconocida que manipula el sistema y el titular que recibe o dispone, la sentencia debe justificar la existencia del enlace funcional. No basta demostrar la materialidad del fraude ni el destino del dinero; es necesario explicar por qué los hechos acreditados revelan una actuación coordinada y consciente.

Este resultado coincide con Chávez Martínez y Ruiz Valer (2026), quienes mostraron que la individualización constituye un obstáculo transversal en delitos cometidos mediante

tecnologías. La presente investigación añade que, cuando uno de los intervinientes sí es identificable, existe el riesgo de concentrar sobre él toda la imputación y reducir la investigación del componente digital. La falta de identificación del tercero no debe operar automáticamente a favor ni en contra del titular: debe ser incorporada como una circunstancia que exige mayor corroboración del aporte individual.

Desde la teoría de la argumentación, la exigencia se corresponde con Toulmin (2019): la decisión debe exponer los datos, la conclusión y la garantía que permite pasar de unos a otra. Aplicado al caso, no es suficiente afirmar que el acusado era titular, que recibió dinero y que, por tanto, conocía el fraude. La sentencia debe formular la máxima utilizada —por ejemplo, que quien conserva el control de tarjeta y clave y retira personalmente fondos inmediatamente después de su ingreso normalmente conoce y aprovecha la operación— y debe justificar por qué esa máxima resulta aplicable al caso concreto. Cuando se omite la garantía, aparece el salto inferencial o la motivación aparente.

La comparación entre S-02 y S-04 confirmó que la suficiencia de la motivación no depende de su extensión, sino de la transparencia del razonamiento. S-02 explicó qué información faltaba y por qué esas ausencias impedían individualizar la participación; S-04 integró titularidad, recepción, retiros con tarjeta y clave y falta de respaldo de la pérdida. Ambas decisiones fueron controlables porque exteriorizaron, con distinto resultado, la relación entre los hechos y el estándar probatorio. En contraste, las sentencias conformadas ofrecieron menor material para evaluar la calidad de la inferencia debido a la aceptación de cargos.

Este último punto constituye una precisión metodológica relevante. La conclusión anticipada acredita que el procesado aceptó la imputación y produce una decisión condenatoria dentro de un mecanismo consensual, pero no reproduce la misma intensidad de contradicción probatoria que un juicio. Por ello, no corresponde usar las sentencias conformadas como evidencia equivalente de un estándar judicial consolidado sobre suficiencia de indicios. Su valor para la investigación se encuentra en la estructura fáctica aceptada y en los actos posteriores descritos, no en un contraste exhaustivo de hipótesis.

La discusión sobre la falta de denuncia y bloqueo revela, además, una tensión con la presunción de inocencia. Jueces y fiscales los consideraron elementos que debilitan la explicación de pérdida, mientras defensores y perito reclamaron contextualización y verificación técnica. La posición integrada es que tales omisiones pueden funcionar como contraindicios dentro de un conjunto, pero no como prueba positiva autónoma del dolo. Si la acusación no demuestra el aporte consciente, la debilidad de la versión defensiva no completa

la hipótesis inculpativa. Sostener lo contrario trasladaría al procesado la carga de demostrar que no controló su propia cuenta.

La exigencia anterior encuentra respaldo en el artículo 2, inciso 24, literal e, y en el artículo 139, inciso 5, de la Constitución, así como en el artículo 394, numeral 3, del Código Procesal Penal. La presunción de inocencia requiere prueba de cargo suficiente; el deber de motivación exige un razonamiento claro, lógico y completo. En el marco de la Sentencia Plenaria Casatoria N.º 1-2017/CIJ-433, la condena solo resulta legítima cuando la hipótesis acusatoria supera la duda razonable. En consecuencia, la falta de individualización del tercero incrementa, y no disminuye, la necesidad de explicar la cadena inferencial.

6.5. Discusión de los hallazgos emergentes

La asimetría entre trazabilidad financiera y atribución digital fue el principal hallazgo emergente. Las entidades bancarias permiten establecer con relativa rapidez dónde llegó el dinero, pero esa información no siempre identifica quién accedió a la cuenta, retiró, transfirió o convirtió los fondos. Esta diferencia explica por qué la investigación tiende a detenerse en el titular registral. A la vez, demuestra la necesidad de ampliar la trazabilidad desde el plano contable hacia el plano técnico, incorporando canal, dispositivo, ubicación, autenticación y destino final de los fondos.

El segundo hallazgo emergente fue la diferencia entre egreso y disposición personalmente atribuida. Esta distinción tiene consecuencias metodológicas y jurídicas: un estado de cuenta acredita que los fondos salieron, pero no necesariamente que el titular realizó la operación. Las transferencias electrónicas pueden ejecutarse mediante acceso remoto; los retiros presenciales ofrecen mayores posibilidades de individualización, aunque requieren imágenes, ubicación y otros elementos. La investigación no debe confundir el registro de la operación con la identidad del operador.

El tercer hallazgo fue el efecto de la conclusión anticipada sobre la comparación de sentencias. La clasificación por vía procesal evitó interpretar las cuatro condenas como expresión de una pauta uniforme. La diferencia probatoria más informativa estuvo entre S-02 y S-04, ambas producto de juicio contradictorio. Este hallazgo confirma que, en estudios cualitativos de jurisprudencia, el sentido del fallo debe ser analizado junto con el mecanismo procesal que lo produjo y con el nivel de debate probatorio disponible.

El cuarto hallazgo fue el riesgo de inversión de la carga de la prueba. La ausencia de denuncia, bloqueo o documentos puede afectar la credibilidad de una explicación, pero no reemplaza la acreditación positiva de los elementos del delito. Esta precisión resulta

especialmente importante en contextos de desigualdad, donde el desconocimiento de trámites o la falta de acceso oportuno a servicios puede explicar la ausencia de actuaciones formales. La valoración debe atender al contexto y, sobre todo, a la evidencia técnica disponible.

Finalmente, la categoría emergente del alquiler de cuentas mostró que el fenómeno supera la dicotomía entre culpable y víctima absoluta. Pueden existir titulares que cedan el control a cambio de una comisión, conozcan el carácter irregular de la operación, pero no el origen concreto de los fondos o la modalidad técnica utilizada. Estos supuestos exigen profundizar el análisis del dolo y del aporte, y no pueden resolverse mediante la equiparación automática entre cesión de cuenta y coautoría en fraude informático.

6.6. Implicancias teóricas y prácticas de los resultados

En el plano teórico, los resultados proponen una secuencia de atribución compuesta por cuatro niveles: vínculo registral, recepción objetiva, control efectivo y disposición personalmente atribuible. Solo los dos últimos aproximan de manera significativa al conocimiento y la voluntad, y aun así deben integrarse con el contexto y el descarte razonado de alternativas. Esta secuencia permite ordenar la prueba indiciaria y evita que hechos de distinto valor sean tratados como equivalentes.

En el plano dogmático, la investigación reafirma que la coautoría del titular requiere un aporte funcional consciente. La recepción de fondos puede formar parte del plan común, pero su relevancia depende del control y del aprovechamiento. La intervención del ejecutor técnico no identificado no impide reconocer coautoría, siempre que el acuerdo y la contribución esencial del titular se infieran de hechos probados. Si tales presupuestos no se acreditan, la responsabilidad debe excluirse o recalificarse conforme a la entidad real del aporte.

En el plano probatorio, los resultados justifican protocolos de obtención y conservación temprana de evidencia. La información bancaria debe incluir algo más que titularidad y movimientos: canal de operación, terminal o cajero, hora exacta, imágenes, mecanismos de autenticación, dirección IP, dispositivo asociado, ubicación disponible y cuentas o billeteras de destino. Esta necesidad se articula con el Convenio de Budapest y con las observaciones de Quincho Laura et al. (2025) sobre preservación rápida y cooperación.

En el plano jurisdiccional, la motivación debería organizarse distinguiendo el hecho fuente, el hecho indicador, la regla inferencial y la conclusión. También debería exponer por qué las hipótesis alternativas fueron corroboradas o descartadas. Esta estructura no pretende imponer una fórmula rígida, sino hacer controlable el razonamiento y reducir el riesgo de que la titularidad se transforme tácitamente en presunción de responsabilidad.

Las propuestas de capacitación formuladas por los entrevistados coinciden con Catagua Zambrano y Vera Navarrete (2026) respecto de la brecha técnica en informática forense. La mejora no depende únicamente de una reforma legislativa; requiere articulación entre fiscales, jueces, defensores, peritos y entidades financieras. La especialización permitiría formular diligencias pertinentes, interpretar correctamente los registros y distinguir entre plausibilidad técnica y mera especulación.

6.7. Limitaciones y alcance interpretativo

Los resultados deben interpretarse dentro de las delimitaciones del estudio. La muestra documental estuvo integrada por cinco sentencias de Ayacucho y solo dos provinieron de juicios con contradicción probatoria plena; las otras tres fueron sentencias conformadas. Por ello, el estudio no pretende establecer frecuencias estadísticas ni generalizar cuantitativamente sus conclusiones a todo el sistema judicial peruano. Su aporte es analítico: identificar patrones, diferencias y criterios útiles para casos con estructuras semejantes.

Asimismo, el análisis se sustentó en el contenido escrito de las sentencias y no en la totalidad de carpetas fiscales, expedientes judiciales, audiencias o archivos técnicos. Determinadas diligencias pudieron haberse realizado sin quedar desarrolladas con igual detalle en la resolución. Esta limitación refuerza la cautela con la que deben interpretarse las ausencias probatorias: el estudio evalúa la evidencia y el razonamiento exteriorizados en las decisiones, que son precisamente los elementos sometidos al deber de motivación.

Las entrevistas aportaron diversidad funcional, pero expresan criterios profesionales y experiencias situadas. Las diferencias entre jueces, fiscales, defensores y perito no constituyen defectos de la muestra, sino información relevante sobre el distinto umbral de corroboración que cada rol considera necesario. La triangulación permitió identificar el consenso mínimo — la titularidad no basta— y ubicar las divergencias en la valoración de la denuncia, el bloqueo y la evidencia técnica.

6.8. Síntesis de la discusión

La discusión permitió sostener que la atribución penal al titular de la cuenta receptora es jurídicamente legítima cuando la trazabilidad financiera se complementa con evidencia individualizadora y una motivación inferencial explícita. Los resultados coinciden con los antecedentes que identifican anonimato, deficiencias técnicas y problemas de preservación de evidencia como obstáculos de la ciberdelincuencia; y los precisan al demostrar que, en el fraude informático, el punto crítico es distinguir el destino del dinero de la identidad y del dolo de quien lo controla y dispone.

En consecuencia, la intervención de sujetos no identificados no genera impunidad automática ni habilita una condena por proximidad registral. Obliga a reconstruir la división de funciones, probar el aporte consciente del titular, individualizar los actos de disposición y contrastar explicaciones alternativas mediante evidencia objetiva. El estándar resultante puede resumirse así: titularidad y recepción orientan la investigación; control y disposición corroborados sostienen la inferencia; y la motivación debe explicar por qué el conjunto supera razonablemente la hipótesis de uso no autorizado.

CONCLUSIONES

- J) Respecto del objetivo general, se concluye que la responsabilidad penal del titular de la cuenta receptora no puede atribuirse válidamente a partir de la sola titularidad registral ni de la recepción del dinero fraudulentamente transferido. La atribución requiere una valoración progresiva y conjunta de hechos adicionales, como el control efectivo de la cuenta, la disposición personalmente atribuible de los fondos, la proximidad temporal entre su recepción y retiro, el aprovechamiento económico y la inexistencia de una explicación alternativa compatible con la evidencia. La trazabilidad financiera identifica el destino del dinero, pero no demuestra automáticamente quién participó con conocimiento y voluntad en el fraude informático.
- J) Respecto del primer objetivo específico, se concluye que los órganos jurisdiccionales de Ayacucho no desarrollaron de manera uniforme los criterios jurídicos empleados para calificar al titular de la cuenta como autor o coautor. En las sentencias conformadas predominó la aceptación de los cargos, por lo que no se realizó un examen contradictorio suficientemente desarrollado sobre el acuerdo común, el aporte esencial y el dominio funcional del hecho. En los procesos contradictorios, la coautoría se sostuvo cuando se acreditó que el titular controló la cuenta y dispuso personalmente de los fondos dentro de una distribución funcional de tareas. Por consiguiente, la afirmación de que el titular actuó “en coordinación con sujetos no identificados” no basta para demostrar la coautoría si no está respaldada por hechos objetivos que acrediten el acuerdo y el aporte consciente.
- J) Respecto del segundo objetivo específico, se concluye que el elemento probatorio con mayor capacidad para acreditar el conocimiento y la voluntad del titular fue el acto de disposición personalmente atribuible. Los retiros presenciales realizados con tarjeta y clave, la proximidad temporal, la conversión inmediata del dinero en criptomonedas y

el aprovechamiento efectivo incrementaron la fuerza de la inferencia cuando fueron debidamente corroborados. En cambio, la existencia contable de un retiro o transferencia posterior no permitió identificar automáticamente a su ejecutor. Para individualizarlo resultaron relevantes las imágenes de cajeros, la ubicación de la operación, los registros de acceso, la dirección IP, el dispositivo empleado, las comunicaciones y los metadatos.

- J) Respecto del tercer objetivo específico, se concluye que la falta de individualización de los sujetos que ejecutaron la manipulación informática no excluye automáticamente la responsabilidad penal del titular de la cuenta, pero incrementa la exigencia de corroboración y motivación. La sentencia debe explicar el vínculo funcional entre el tercero no identificado y el titular, identificar los hechos indicadores, formular la regla inferencial empleada y justificar por qué la hipótesis de participación consciente resulta más consistente que las hipótesis de pérdida, préstamo, suplantación de identidad o utilización no autorizada de la cuenta.
- J) La comparación entre las sentencias S-02 y S-04 permitió establecer que la diferencia decisiva entre la absolución y la condena no estuvo en la titularidad ni en la recepción de los fondos, presentes en ambos casos, sino en la individualización del acto de disposición. En S-02 no se acreditó quién manipuló el sistema ni quién retiró el dinero, por lo que permaneció la duda razonable. En S-04 se acreditaron retiros presenciales efectuados con tarjeta y clave, próximos a la recepción de los fondos, y se descartó razonadamente la pérdida alegada. Esto demuestra que el egreso bancario solo adquiere fuerza incriminatoria cuando puede atribuirse personalmente al procesado.
- J) La triangulación de las cinco sentencias y las nueve entrevistas permitió identificar una asimetría entre la trazabilidad financiera y la atribución digital. Las investigaciones lograron determinar con facilidad la cuenta a la que llegó el dinero, pero presentaron

mayores dificultades para identificar el dispositivo, la ubicación y la persona que ejecutó las operaciones. Esta asimetría concentra la persecución penal en el titular registral, por ser el sujeto visible, y genera el riesgo de establecer una responsabilidad objetiva basada únicamente en la vinculación bancaria.

-) Se concluye que la ausencia de denuncia policial, bloqueo de la tarjeta o explicación documentada puede debilitar la credibilidad de una hipótesis defensiva, pero no constituye prueba autónoma de culpabilidad. Estas omisiones deben valorarse conjuntamente con los hechos positivos de cargo y con las condiciones personales del investigado. Utilizarlas como fundamento principal de una condena trasladaría indebidamente al procesado la carga de demostrar su inocencia y vulneraría la presunción de inocencia.
-) Finalmente, el préstamo remunerado o “alquiler” de cuentas constituye una situación intermedia que no puede resolverse mediante la calificación automática de coautoría. En estos casos debe determinarse si el titular conocía el origen ilícito de los fondos, si comprendía que su cuenta sería utilizada en un fraude informático, cuál fue la entidad de su aporte y si tuvo dominio funcional del hecho. El conocimiento de que se participaba en una operación irregular no equivale necesariamente al conocimiento y voluntad de intervenir específicamente en un fraude informático.

RECOMENDACIONES

-)] Al Ministerio Público del Distrito Fiscal de Ayacucho, se recomienda implementar un protocolo especializado para investigar fraudes informáticos en los que se utilicen cuentas receptoras. El protocolo debe exigir la obtención temprana de información sobre el canal de operación, ubicación, cajero o terminal, mecanismos de autenticación, imágenes, direcciones IP, dispositivos asociados, metadatos, comunicaciones y destino posterior de los fondos.
-)] A los fiscales penales, se recomienda evitar que la imputación se limite a señalar que el titular actuó “en coordinación con sujetos no identificados”. El requerimiento acusatorio debe precisar los hechos que demuestran el acuerdo, la distribución de funciones, el aporte esencial del titular, el beneficio obtenido y el conocimiento del origen ilícito de los fondos, justificando expresamente si la conducta corresponde a autoría, coautoría o complicidad.
-)] A los jueces penales del Distrito Judicial de Ayacucho, se recomienda estructurar la motivación diferenciando: la titularidad registral, la recepción del dinero, los hechos que acreditan el control efectivo, la disposición personalmente atribuible, la regla inferencial utilizada, el tratamiento de las hipótesis alternativas y la conclusión sobre el conocimiento y la voluntad del titular. Esta estructura permitirá controlar el razonamiento y evitar saltos inferenciales.
-)] A la Policía Nacional del Perú y al Ministerio Público, se recomienda solicitar inmediatamente la conservación de videos de cajeros, registros bancarios, bitácoras de acceso, direcciones IP, dispositivos, datos de autenticación y metadatos. La demora en requerir esta información puede ocasionar su pérdida y limitar definitivamente la individualización de quien realizó las operaciones.

- J A las entidades financieras, se recomienda establecer procedimientos de respuesta rápida ante solicitudes fiscales y judiciales, así como conservar durante un periodo razonable la información técnica vinculada con transferencias y retiros sospechosos. También deben reforzar las alertas frente a cuentas recientemente abiertas, transferencias atípicas y retiros inmediatos, respetando la protección de los datos personales y el secreto bancario.
- J A la Corte Superior de Justicia y al Distrito Fiscal de Ayacucho, se recomienda desarrollar capacitaciones conjuntas para jueces, fiscales, defensores y peritos sobre fraude informático, prueba indiciaria, autoría y participación, cadena de custodia digital y valoración de registros electrónicos. Estas actividades deben incluir el análisis comparativo de sentencias condenatorias y absolutorias.
- J A los abogados defensores, se recomienda plantear desde las primeras etapas las hipótesis de pérdida, préstamo, suplantación o acceso no autorizado y solicitar diligencias objetivas para corroborarlas. Cuando sea posible, deben promover el examen del dispositivo, la obtención de registros de acceso, comunicaciones, ubicación y pericias informáticas, evitando que la defensa se reduzca a la sola negación de los hechos.
- J A los órganos jurisdiccionales, se recomienda no utilizar la falta de denuncia policial o de bloqueo como prueba autónoma de culpabilidad. Estas omisiones deben valorarse considerando el contexto del investigado y únicamente después de que la acusación haya presentado hechos positivos suficientes para acreditar el control y la disposición de los fondos.
- J Al Ministerio Público, se recomienda diferenciar los casos de utilización no consentida de la cuenta de aquellos en los que existe préstamo o alquiler remunerado. En estos últimos debe investigarse el contenido del conocimiento del titular, las comunicaciones

sostenidas, la comisión recibida, el tiempo de cesión, el control conservado sobre la cuenta y la finalidad que le fue comunicada, a fin de determinar correctamente la forma de intervención.

) A futuros investigadores, se recomienda ampliar la muestra mediante el análisis de carpetas fiscales, requerimientos acusatorios, sentencias de segunda instancia y resoluciones de otros distritos judiciales. Esto permitirá comparar los criterios empleados a nivel nacional y desarrollar estándares más uniformes para distinguir al titular registral, al titular que actúa dolosamente y al titular cuya cuenta fue utilizada sin autorización.

BIBLIOGRAFÍA

- Alvear Richards, G. E., & Hernández Pesantes, E. A. (2023). Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos [Tesis de maestría, Universidad Politécnica Salesiana]. Repositorio Institucional UPS.
- Becerra Cervera, N. A. (2025). Una mirada a la problemática de los delitos informáticos y su afectación directa sobre las cuentas digitales bancarias en el Perú 2022 [Tesis de pregrado]. Repositorio institucional.
- Bonifaz Muñoz, M. F. (2024). Los delitos informáticos y su regulación en el sistema penal: Un análisis de los nuevos desafíos en la era digital del distrito fiscal de Ica, año 2024 [Tesis de pregrado, Universidad Nacional "San Luis Gonzaga"]. Repositorio institucional.
- Bramont-Arias Torres, L. A. (1997). El delito informático en el Código Penal peruano (Biblioteca de Derecho Contemporáneo, Vol. 6). Fondo Editorial de la Pontificia Universidad Católica del Perú.
- Catagua Zambrano, D. J., & Vera Navarrete, D. S. (2026). Análisis comparativo de herramientas digitales forenses con IA en el marco de los delitos informáticos en Ecuador. Revista Científica de Informática ENCRYPTAR, 9(17). <https://doi.org/10.56124/encryptar.v9i17.007>
- Chavez Martinez, I. F., & Ruiz Valer, A. M. (2026). Análisis de la individualización del imputado en la persecución del delito de proposiciones a menores con fines sexuales por medios tecnológicos en la fiscalía de Ciberdelincuencia de Arequipa 2023-2024 [Tesis de pregrado, Universidad Católica de Santa María]. Repositorio institucional.
- Hidalgo Coronel, C. N., & Solano Vidal, G. S. (2021). El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. Propuesta de incorporación del artículo 7-A en la Ley de Delitos Informáticos 30096 [Tesis de pregrado, Universidad Nacional del Santa]. Repositorio institucional.
- Hurtado Falvy, J. M. (1999). Introducción a los delitos informáticos en la legislación peruana. Derecho & Sociedad, (14), 311-320.

- Leyva Serrano, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris et Investigatio*, 1(1), 29-48. <https://doi.org/10.15381/lucerna.v0i1.18373>
- Manobanda Guangasi, N. A., & Chiriboga Sabando, D. V. (2026). Impacto de la tecnología en la criminalidad en el Ecuador: Reflexión crítica sobre la mutación del fenómeno delictivo y el desafío de la ciberseguridad jurídica. *Revista Iberoamericana de Ciencias Sociales*, 5(1). <https://doi.org/10.63371/ic.v5.n1.a717>
- Quincho Laura, R. S., Aylas Dionicio, J. F., & Arcos Huayhua, J. (2025). Aplicación del convenio de Budapest en la ley de delitos informáticos del Perú, Cusco 2024 [Tesis de pregrado, Universidad Continental]. Repositorio institucional.
- Rodríguez Pilco, K. K., & Chimborazo Castillo, L. A. (2026). Responsabilidad penal por criminalidad organizada en entornos digitales. *Revista Científica Internacional Arandu UTIC*, 13(2), 128-144. <https://doi.org/10.69639/arandu.v13i2.2165>
- Rosales Medina, R. M. (2025). Incremento de los delitos informáticos y su problemática con la impunidad delictiva en Lima, 2024 [Tesis de pregrado, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú.
- Ventura Quijano, M. A. (2021). La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020 [Tesis de pregrado, Universidad Privada del Norte]. Repositorio de la Universidad Privada del Norte. <https://hdl.handle.net/11537/28903>
- Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius et Praxis*, (53), 95-110. <https://doi.org/10.26439/iusetpraxis2021.n053.4995>
- Davara, M. Á. (1993). Derecho informático. Aranzadi. (Citado en Vinelli Vereau, 2021).
- Ferrer Beltrán, J. (2021). Prueba sin convicción. Estándares de prueba y debido proceso. Marcial Pons. (Citado conforme a su desarrollo en la fundamentación del expediente N.º 01342-2022-33-0501-JR-PE-04, integrante de la muestra documental de la investigación).
- Gascón Abellán, M. (2005). Sobre la posibilidad de formular estándares de prueba objetivos. *Doxa. Cuadernos de Filosofía del Derecho*. <https://doi.org/10.14198/DOXA2005.28.10>

(Citado conforme a su desarrollo en la fundamentación del expediente N.º 01342-2022-33-0501-JR-PE-04).

Morillas Fernández, D. L. (2017). Los delitos de daños informáticos: perspectiva doctrinal, jurisprudencial y de derecho comparado. Dykinson. (Citado en Vinelli Vereau, 2021).

Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, (47), 209-234. (Citado en Vinelli Vereau, 2021).

Rodríguez, J. (2020). Factores asociados a los delitos informáticos que afectan las cuentas bancarias digitales. (Citado en Becerra Cervera, 2025).

Toulmin, S. E. (2019). Los usos de la argumentación (M. Morras & V. Pineda, Trads.). Marcial Pons. (Citado conforme a su desarrollo en la fundamentación del expediente N.º 01342-2022-33-0501-JR-PE-04).

Villavicencio Terreros, F. (2014). Delitos informáticos. Derecho PUCP, (73), 284-304. (Citado en Vinelli Vereau, 2021).

ANEXOS

ANEXO 1. MATRIZ DE CONSISTENCIA

Problemas	Objetivos	Categorías y subcategorías	Metodología
Problema general: ¿Cómo atribuyen los órganos jurisdiccionales penales del distrito judicial de Ayacucho responsabilidad penal al titular de la cuenta receptora del dinero fraudulentamente transferido, frente a la intervención de sujetos no identificados en la manipulación del sistema informático, en el delito de fraude informático, durante el periodo 2022-2024?	Objetivo general: Analizar la forma en que los órganos jurisdiccionales penales del distrito judicial de Ayacucho atribuyen responsabilidad penal al titular de la cuenta receptora del dinero fraudulentamente transferido, frente a la intervención de sujetos no identificados en la manipulación del sistema informático, durante el periodo 2022-2024.	Categoría 1: valor jurídico-probatorio de la titularidad, recepción y disposición. Categoría 2: intervención de sujetos no identificados e hipótesis alternativas. Categoría 3: construcción y motivación de la inferencia probatoria.	Enfoque: cualitativo. Tipo: básico. Nivel: descriptivo-interpretativo. Diseño: estudio de casos múltiples. Técnicas: análisis documental y entrevista semiestructurada. Instrumentos: ficha documental y guía de entrevista. Muestra: cinco sentencias y nueve participantes. Muestreo: intencional.
P.E.1: ¿Qué criterios jurídicos emplean los órganos jurisdiccionales penales de Ayacucho para calificar el grado de intervención delictiva -autoría o coautoría- del titular de la cuenta receptora cuando se alega la intervención de sujetos no identificados?	O.E.1: Identificar los criterios jurídicos empleados para calificar el grado de intervención delictiva -autoría o coautoría- del titular de la cuenta receptora.	C.1: titularidad formal; recepción efectiva; actos posteriores de disposición; peso probatorio diferenciado.	Fuente documental: sentencias. Fuente personal: jueces, fiscales, abogados penalistas y perito informático. Análisis: codificación temática, comparación intrafuente e interfuente.
P.E.2: ¿Qué elementos probatorios permiten acreditar el conocimiento y la voluntad del titular de participar en el fraude ante la falta de individualización del ejecutor material?	O.E.2: Examinar los elementos probatorios que permiten acreditar el conocimiento y la voluntad del titular de participar en el fraude informático.	C.2: tratamiento del tercero no identificado; pérdida de tarjeta o documentos; préstamo de cuenta; suplantación o uso no autorizado; verificación objetiva; alquiler remunerado de cuenta (emergente).	Rigor: dependencia, credibilidad, transferencia y confirmación. Triangulación de fuentes, técnicas y perfiles profesionales.
P.E.3: ¿Cómo incide la falta de individualización de los sujetos que manipularon el sistema en la motivación de la responsabilidad penal atribuida al titular?	O.E.3: Analizar la incidencia de la falta de individualización de los sujetos que manipularon el sistema en la motivación de la responsabilidad penal atribuida al titular.	C.3: hecho indicador; regla inferencial; diferenciación titular registral/responsable; valoración conjunta; suficiencia de motivación.	Ética: consentimiento informado, participación voluntaria, confidencialidad, codificación de participantes y uso académico de la información.

ANEXO 2. MATRIZ DE CATEGORIZACIÓN

Categoría	Subcategorías	Indicadores	Ítems de entrevista
1. Valor jurídico-probatorio de la titularidad, recepción y disposición	Titularidad formal; recepción efectiva; actos posteriores de disposición; peso probatorio diferenciado	Fecha de apertura y vigencia; identidad del titular; monto y fecha del abono; retiro, transferencia o conversión; canal, ubicación, tarjeta/clave, IP o dispositivo; proximidad temporal; atribución personal.	Preguntas 1, 2 y 3
2. Intervención de sujetos no identificados e hipótesis alternativas	Tercero no identificado; pérdida; préstamo; suplantación/uso no autorizado; verificación objetiva; alquiler de cuenta (emergente)	Descripción de funciones; indicios de coordinación; denuncia y bloqueo; coherencia temporal; identificación del prestatario; accesos no habituales; comunicaciones; metadatos; contraste judicial.	Preguntas 4, 5 y 6
3. Construcción y motivación de la inferencia	Hecho indicador; máxima de experiencia/regla lógica; diferenciación titular/responsable; valoración conjunta; suficiencia de motivación	Hechos positivos de enlace; regla inferencial; descarte de alternativas; explicación de conocimiento y voluntad; estándar de duda razonable; propuesta de mejora.	Preguntas 7, 8 y 9

ANEXO 3. FICHA DE ANÁLISIS DOCUMENTAL

Objetivo: registrar de manera uniforme los datos relevantes de cada sentencia vinculados con la atribución de responsabilidad penal al titular de la cuenta receptora.

Sección	Información por registrar
I. Identificación	Código de sentencia: ____ Expediente: ____ Órgano jurisdiccional: ____ Año: ____ Vía procesal: ____ Decisión: ____
II. Datos del hecho	Entidad financiera: ____ Monto transferido: ____ Cuenta receptora: ____ Fecha de apertura/vigencia: ____ Modalidad de manipulación descrita: ____
III. Intervención atribuida	Calificación jurídica: autor / coautor / partícipe. Aporte atribuido al titular: _____. Función del sujeto no identificado: _____. Elementos de coordinación: _____.
IV. Evidencia sobre disposición	Retiro / transferencia / conversión / sin disposición acreditada. Fecha y proximidad: _____. Canal y ubicación: _____. Tarjeta y clave: _____. Imagen, IP, dispositivo o metadatos: _____.
V. Hipótesis alternativa	Pérdida / préstamo / suplantación / uso no autorizado / otra: _____. Elementos de respaldo: _____. Actos de verificación: _____. Tratamiento judicial: _____.
VI. Inferencia y motivación	Hechos indicadores: _____. Regla inferencial o máxima aplicada: _____. Valoración conjunta: _____. Diferenciación entre titularidad y responsabilidad: _____. Razón de condena/absolución: _____.
VII. Observaciones	Vacíos probatorios: _____. Nivel de motivación: alto / medio / bajo. Observaciones del investigador: _____.

ANEXO 4. GUÍA DE ENTREVISTA SEMIESTRUCTURADA

Título de la investigación: La atribución de responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados en el delito de fraude informático en el distrito judicial de Ayacucho, 2022-2024.

Objetivo de la entrevista: recoger criterios jurídicos y técnicos sobre el valor de la titularidad, recepción y disposición; el tratamiento de terceros no identificados e hipótesis alternativas; y la motivación de la inferencia probatoria.

Datos generales: código: ____; perfil profesional: ____; institución/ámbito: ____; años de experiencia: ____; experiencia en fraude informático: ____.

- 1. ¿Qué valor probatorio diferenciado atribuye a la titularidad formal de la cuenta receptora, frente a la recepción efectiva del dinero y a los actos posteriores de disposición realizados por su titular?**

- 2. ¿Qué actos de disposición -retiros, transferencias o conversión en criptomonedas- considera más reveladores del conocimiento del titular sobre el origen ilícito de los fondos?**

- 3. ¿En qué supuestos la sola recepción de los fondos, sin un acto posterior de disposición atribuible al titular, resulta insuficiente para sustentar responsabilidad penal?**

4. ¿Cómo evalúa la alegación fiscal sobre la intervención de un tercero no identificado en relación con la responsabilidad atribuida al titular de la cuenta?

5. ¿Qué criterios utiliza para verificar hipótesis alternativas como pérdida de tarjeta o documentos, préstamo voluntario de la cuenta o alquiler de esta?

6. ¿Qué elementos deben concurrir para considerar creíble la suplantación de identidad o la utilización no autorizada de la cuenta?

7. ¿Cómo se construye la inferencia que permite pasar de la titularidad registral a la conclusión de que el titular actuó con conocimiento y voluntad?

8. ¿Qué diferencias debe explicitar la motivación judicial o el requerimiento acusatorio entre el mero titular registral y el responsable penal?

9. ¿Qué medidas o buenas prácticas propone para mejorar la motivación y la investigación de estos casos en Ayacucho?

ANEXO 5. CONSENTIMIENTO INFORMADO

Se le invita a participar en la investigación indicada. Su participación consistirá en responder una entrevista semiestructurada de aproximadamente 35 a 45 minutos sobre criterios jurídicos o técnicos aplicables a casos de fraude informático. La participación es voluntaria. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento, sin consecuencia alguna.

La información será utilizada exclusivamente con fines académicos. Su identidad será protegida mediante un código alfanumérico y no se incorporarán datos que permitan identificarlo ni información reservada de casos vigentes. La entrevista podrá ser registrada en audio únicamente con su autorización expresa. Los resultados serán presentados de manera agregada o mediante citas anonimizadas.

Declaro que he recibido información suficiente, que comprendí el propósito, procedimiento, tratamiento confidencial de los datos y mis derechos, y que acepto participar libremente.

Datos y manifestación	Registro
Código del participante	_____
Autorizo la participación	Sí () No ()
Autorizo la grabación de audio	Sí () No ()
Firma del participante	_____
Firma del investigador	_____
Lugar y fecha	_____

ANEXO 8. MATRIZ CONSOLIDADA DE ANÁLISIS DOCUMENTAL

Código	Titularidad/recepción	Disposición	Tercero no identificado	Resultado inferencial
S-01	Acreditadas	Conversión a criptomonedas vinculadas al acusado	No fue el eje central	Condena conformada; control y aprovechamiento aceptados.
S-02	Acreditadas	Egreso no individualizado	Expreso; coordinación no corroborada	Absolución por duda razonable; no se probó quién manipuló ni retiró.
S-03	Acreditadas	Retiros efectivos en atribuidos a ambos titulares	Coimputados identificados	Condena conformada; hechos admitidos.
S-04	Acreditadas	Retiros presenciales con tarjeta y clave	Expreso; ejecutor técnico no identificado	Condena por cadena convergente y descarte de pérdida no corroborada.
S-05	Acreditadas	No desarrollado con igual precisión	Expreso	Condena conformada; alcance inferencial limitado por aceptación.

ANEXO 9. RELACIÓN CODIFICADA DE PARTICIPANTES

Código	Perfil profesional	Experiencia
JP-01	Juez penal unipersonal	14 años
JP-02	Juez penal unipersonal	11 años
JP-03	Juez penal unipersonal	17 años
FP-01	Fiscal provincial penal	13 años
FP-02	Fiscal adjunto provincial penal	8 años
FP-03	Fiscal adjunto provincial penal	6 años
AP-01	Abogado penalista	15 años
AP-02	Abogado penalista	9 años
PI-01	Perito informático forense	10 años

La identidad de los participantes se mantiene confidencial. Los códigos JP, FP, AP y PI corresponden, respectivamente, a juez penal, fiscal penal, abogado penalista y perito informático.

ANEXO 10. MATRIZ DE TRIANGULACIÓN

Categoría	Resultado documental	Resultado testimonial	Resultado integrado
Titularidad, recepción y disposición	La diferencia entre S-02 y S-04 estuvo en la individualización de la disposición.	9/9 coincidieron en el valor creciente y la insuficiencia de la sola recepción.	La disposición personalmente corroborada es el principal hecho de enlace.
Terceros e hipótesis alternativas	La fórmula genérica no bastó en S-02; en S-04 se integró con retiros y descarte de la pérdida.	Todos exigieron vinculación; divergieron sobre denuncia y nivel de evidencia técnica.	La intervención ajena debe tratarse como hipótesis real, verificable y no retórica.
Inferencia y motivación	S-02 y S-04 desarrollaron cadenas opuestas; las conformadas ofrecieron menor contradicción.	Consenso sobre control, disposición y descarte razonado.	La motivación debe separar fuente, hecho, regla inferencial y conclusión.



UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

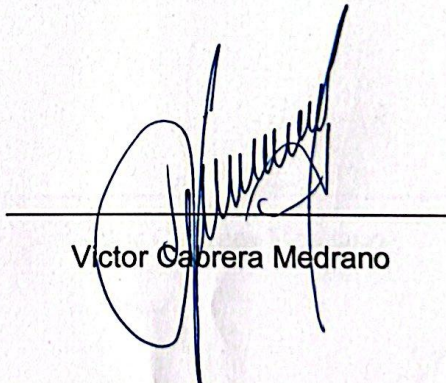
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

**ACTA DE SUSTENTACIÓN DE TESIS DE LA ASPIRANTE LUZ
ESPERANZA LIZANA TINCO**

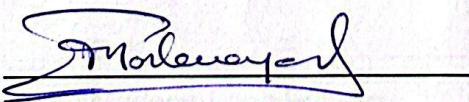
En la ciudad de Ayacucho, siendo las 6:00 pm del día 10 de setiembre de 2026 reunidos en la facultad de Derecho y Ciencias Políticas – UNSCH, los miembros del jurado examinador Victor Cabrera Medrano (Presidente), Marlene León Palacios, Jenny Juana Barraza Torres, Katherine Irma Quispe Vargas y Julio César Tello Jurado (Miembros). Para examinar la tesis de la aspirante Luz Esperanza Lizana Tinco titulado La atribución de responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados en el delito de fraude informático en el distrito judicial de Ayacucho, 2022-2024 .

Acto seguido se da lectura a la resolución decanal N°326-2026-UNSCH-FDCP-D de la fecha 03 de setiembre de 2026 y el artículo 25 del reglamento de grados y títulos, a continuación el presidente otorgó el uso de la palabra a la aspirante; una vez concluido se invita al aspirante y al público en general a salir del auditorio, y el jurado procede a deliberar.

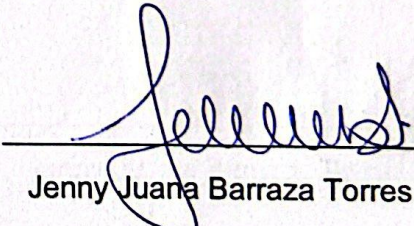
El jurado decidió **APROBAR** por unanimidad con la nota 12 (Doce) por lo que concluyó el acto académico con la firma del acta siendo las 7:45 pm del mismo.



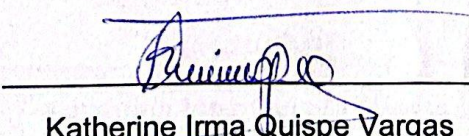
Victor Cabrera Medrano



Marlene León Palacios



Jenny Juana Barraza Torres



Katherine Irma Quispe Vargas



Julio César Tello Jurado

**UNSCH****FACULTAD DE DERECHO
Y CIENCIAS POLITICAS****ESCUELA PROFESIONAL DE
DERECHO****CONSTANCIA DE ORIGINALIDAD N° 01-2026-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:

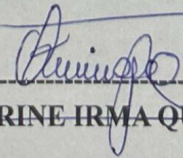
CONSTANCIA DE ORIGINALIDAD

Autor	Bach. LUZ ESPERANZA LIZANA TINCO
Para	Título profesional
Denominación de la tesis	La atribución de responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados en el delito de fraude informático en el distrito judicial de Ayacucho, 2022-2024.
Evaluación de Originalidad	8%
Numero de trabajo	3040323956
Fecha	23 de setiembre de 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, 23 de setiembre de 2026


KATHERINE IRMA QUISPE VARGAS

La atribución de responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados en el delito de fraude informático en el distrito judicial de Ayacucho, 2022-2024.

por LUZ ESPERANZA LIZANA TINCO

La atribución de responsabilidad penal al titular de la cuenta receptora frente a la intervención de sujetos no identificados en el delito de fraude informático en el distrito judicial de Ayacucho, 2022-2024.

INFORME DE ORIGINALIDAD

8%	8%	6%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unsch.edu.pe	2%
	Fuente de Internet	
2	repositorio.ucsm.edu.pe	1%
	Fuente de Internet	
3	hdl.handle.net	1%
	Fuente de Internet	
4	www.uticvirtual.edu.py	1%
	Fuente de Internet	
5	prcp.com.pe	<1%
	Fuente de Internet	
6	publicacionescd.ulead.edu.ec	<1%
	Fuente de Internet	
7	repositorio.upt.edu.pe	<1%
	Fuente de Internet	
8	www.coursehero.com	<1%
	Fuente de Internet	
9	Submitted to Universidad Tecnológica del Peru	<1%
	Trabajo del estudiante	
10	repositorio.unfv.edu.pe	<1%
	Fuente de Internet	
11	repositorio.continental.edu.pe	<1%
	Fuente de Internet	
12	Submitted to Universidad Nacional de San Cristóbal de Huamanga	<1%
	Trabajo del estudiante	
13	pirhua.udep.edu.pe	<1%
	Fuente de Internet	
14	www.icc-cpi.int	<1%
	Fuente de Internet	

15	Trabajo del estudiante	<1 %
16	tesis.ucsm.edu.pe Fuente de Internet	<1 %
17	vbook.pub Fuente de Internet	<1 %
18	revistasinvestigacion.unmsm.edu.pe Fuente de Internet	<1 %
19	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %
20	Submitted to Universidad Politécnica del Perú Trabajo del estudiante	<1 %
21	dspace.unach.edu.ec Fuente de Internet	<1 %
22	repositorio.udh.edu.pe Fuente de Internet	<1 %
23	revistas.unsaac.edu.pe Fuente de Internet	<1 %
24	Submitted to Integración Semipresencial Trabajo del estudiante	<1 %
25	Rivera Salazar, Gisela Giovanna. "Caracterización del proceso sobre desalojo por ocupación precaria, en el expediente N° 00267-2013-0-3207-JM-CI-03, del Distrito Judicial de Lima Este – Lima,2020", Universidad Católica los Ángeles de Chimbote (Peru) Publicación	<1 %
26	estudioderechoylibertad.com Fuente de Internet	<1 %
27	jalayo.blogspot.com Fuente de Internet	<1 %
28	repositorio.une.edu.pe Fuente de Internet	<1 %
29	Submitted to Corporación Universitaria Reformada Trabajo del estudiante	<1 %
30	Submitted to Unviersidad de Granada Trabajo del estudiante	<1 %

Excluir citas
Excluir bibliografía

Activo
Activo

Excluir coincidencias

< 30 words