UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

TESIS:

La trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático, Ayacucho, 2019 - 2025

Para optar el título profesional de:
ABOGADO

PRESENTADO POR:
Bach. Joseph Michael QUISPE ATAUQUI

ASESOR:
Mtro. Jesús Walter ESPINOZA ALTAMIRANO

AYACUCHO - PERÚ

2026

DEDICATORIA

A Dios, por ser luz en mi camino y fortaleza en cada paso; a mis padres, hermanos y familiares, por ser el abrazo que sostuvo mis sueños y la fuerza que me impulsó a continuar; y a todas aquellas personas que, de una u otra manera, dejaron una huella en este recorrido académico.

De manera especial, dedico estas páginas a la memoria de mi abuelo, cuya ausencia física nunca apagó su presencia en mi corazón. A él, que partió antes de verme culminar este sueño, le ofrezco este logro con la esperanza de que, desde la eternidad, pueda contemplarlo con orgullo. Porque hay seres queridos que se marchan de nuestra vista, pero permanecen para siempre en nuestros pasos; y quizá sea esa la forma más hermosa de permanecer: vivir en nuestros recuerdos, acompañar nuestros esfuerzos y convertirse, aun desde el silencio, en parte de cada meta que alcanzamos.

Esta tesis es, también, un homenaje a todos ellos y a la vida que me permitió llegar hasta aquí.

AGRADECIMIENTO

A mis docentes de pregrado.

ÍNDICE DE CONTENIDO

DEDICATORIA ..... **II**

AGRADECIMIENTO ..... **III**

ÍNDICE DE TABLAS ..... **X**

ÍNDICE DE FIGURAS ..... **XI**

RESUMEN ..... **XII**

ABSTRACT ..... **XIII**

INTRODUCCIÓN **95**

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA **99**

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA 99

1.2. FORMULACIÓN DEL PROBLEMA 103

1.2.1. Problema general *103*

1.2.2. Problemas específicos *104*

1.3. OBJETIVOS DE LA INVESTIGACIÓN 104

1.3.1. Objetivo general *104*

1.3.2. Objetivos específicos *104*

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN 105

1.4.1. Justificación teórica *105*

1.4.2. Justificación jurídica *105*

1.4.3. Justificación práctica *106*

1.4.4. Justificación metodológica *106*

1.4.5. Justificación social *107*

1.5. IMPORTANCIA DE LA INVESTIGACIÓN 107

1.6. DELIMITACIÓN DE LA INVESTIGACIÓN 108

1.6.1. Delimitación temática *108*

1.6.2. Delimitación espacial e institucional *108*

1.6.3. Delimitación temporal 108

1.6.4. Delimitación documental 109

1.6.5. Delimitación personal 109

1.7. LIMITACIONES Y VIABILIDAD 109

1.7.1. Limitaciones 109

1.7.2. Viabilidad 110

CAPÍTULO II: MARCO TEÓRICO 112

2.1. ANTECEDENTES DE LA INVESTIGACIÓN 112

2.1.1. Antecedentes internacionales 112

2.1.2. Antecedentes nacionales 113

2.2. BASES TEÓRICAS 115

2.2.1. Sociedad digital, criminalidad informática y economía del dato 115

2.2.2. Delitos informáticos: concepto y clasificación 115

2.2.3. Bien jurídico protegido 116

2.2.4. Fraude informático en el ordenamiento peruano 116

2.2.5. Diferencia entre fraude informático y estafa 117

2.2.6. Modalidades relevantes: phishing, smishing, vishing, pharming y suplantación 117

2.2.7. Evidencia digital 118

2.2.8. Autenticidad, integridad y cadena de custodia 118

2.2.9. Trazabilidad digital 119

2.2.10. Alcance y límites de los identificadores digitales 119

2.2.11. Trazabilidad financiera 120

2.2.12. Registros bancarios, secreto bancario y control judicial 121

2.2.13. Articulación de trazabilidad digital y financiera 121

2.2.14. Tratamiento fiscal de la trazabilidad 122

2.2.15. Imputación fiscal e imputación necesaria 122

2.2.16. Autoría, coautoría y participación en entornos digitales 122

2.2.17. Titular de cuenta, "mula financiera" y conductas neutrales 123

2.2.18. Prueba indiciaria e inferencia probatoria 123

2.2.19. Contraindicios e hipótesis alternativas 124

2.2.20. Motivación probatoria e inferencial del requerimiento acusatorio 124

2.2.21. Debido proceso, defensa y protección de datos 125

2.2.22. Cooperación interinstitucional e internacional 125

2.3. MARCO NORMATIVO 126

2.3.1. Constitución Política del Perú 126

2.3.2. Ley N.º 30096 y Ley N.º 30171 126

2.3.3. Código Procesal Penal 126

2.3.4. Convenio sobre la Ciberdelincuencia 126

2.3.5. Protección de datos personales y protocolos técnicos 127

2.4. MARCO JURISPRUDENCIAL 127

2.4.1. Prueba indiciaria y deber de exteriorización 127

2.4.2. Imputación y motivación de la acusación 127

2.4.3. Valoración de evidencia digital 128

2.5. MARCO CONCEPTUAL 128

CAPÍTULO III: CATEGORÍAS DE INVESTIGACIÓN 131

3.1. CATEGORÍAS DE ANÁLISIS 131

3.1.1. Categoría principal 131

3.1.2. Subcategoría de tratamiento fiscal de la trazabilidad digital 132

3.1.3. Subcategoría de tratamiento fiscal de la trazabilidad financiera 132

3.1.4. Subcategoría de articulación probatoria para sustentar la imputación 133

3.2. MATRIZ DE CATEGORIZACIÓN 134

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN 136

4.1. ENFOQUE DE LA INVESTIGACIÓN 136

4.2. TIPO DE INVESTIGACIÓN 136

4.3. NIVEL O ALCANCE DE LA INVESTIGACIÓN 137

4.4. DISEÑO DE LA INVESTIGACIÓN 137

4.5. MÉTODO DE INVESTIGACIÓN 138
4.5.1. Método inductivo 138
4.5.2. Método analítico-sintético 138
4.5.3. Método hermenéutico-jurídico 138
4.5.4. Método de estudio de caso 139
4.6. ESCENARIO DE ESTUDIO 139
4.7. POBLACIÓN, MUESTRA Y UNIDADES DE ANÁLISIS 139
4.7.1. Población 139
4.7.2. Muestra 139
4.7.3. U nidades de análisis 140
4.7.4. Criterios de inclusión documental 141
4.7.5. Criterios de exclusión documental 141
4.8. PARTICIPANTES 141
4.8.1. Muestra personal 141
4.8.2. Criterios de inclusión de los participantes 142
4.8.3. Criterios de exclusión de los participantes 142
4.9. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN 142
4.9.1. Análisis documental 142
4.9.2. Entrevista semiestructurada 142
4.9.3. Instrumentos de recolección de información 143
4.10. VALIDEZ DE LOS INSTRUMENTOS 143
4.11. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN 143
4.11.1. Procesamiento y análisis de la información 144
4.11.2. Organización del corpus 144
4.11.3. Codificación inicial 144
4.12. TRIANGULACIÓN 144
4.13. RIGOR CIENTÍFICO DE LA INVESTIGACIÓN 145
4.13.1. Credibilidad 145
4.13.2. Dependencia 145

4.13.3. Confirmabilidad *145*

4.13.4. Transferibilidad *145*

4.13.5. Saturación temática *145*

4.14. CONSIDERACIONES ÉTICAS 146

CAPÍTULO V: PRESENTACIÓN DE DATOS 147

5.1. PRESENTACIÓN DEL CAPÍTULO 147

5.2. CARACTERIZACIÓN DE LAS FUENTES DE INFORMACIÓN 147

5.2.1. Participantes *147*

5.2.2. Requerimientos acusatorios *149*

5.3. ORGANIZACIÓN Y CODIFICACIÓN DE LOS DATOS 149

5.4. DATOS DEL PRIMER OBJETIVO ESPECÍFICO SOBRE TRAZABILIDAD DIGITAL 151

5.4.1. Criterios expresados en las entrevistas *151*

5.4.2. Hallazgos consignados en el análisis documental *152*

5.4.3. Síntesis del primer objetivo *153*

5.5. DATOS DEL SEGUNDO OBJETIVO ESPECÍFICO SOBRE TRAZABILIDAD FINANCIERA 154

5.5.1. Criterios expresados en las entrevistas *154*

5.5.2. Hallazgos consignados en el análisis documental *155*

5.5.3. Síntesis del segundo objetivo *157*

5.6. DATOS DEL TERCER OBJETIVO ESPECÍFICO SOBRE ARTICULACIÓN DE LAS RUTAS 158

5.6.1. Criterios expresados en las entrevistas *158*

5.6.2. Hallazgos consignados en el análisis documental *160*

5.6.3. Síntesis del tercer objetivo *161*

5.7. PRESENTACIÓN INTEGRADA DE LAS FUENTES 161

CAPÍTULO VI: DISCUSIÓN DE RESULTADOS 164

6.1. PROPÓSITO Y ALCANCE DE LA DISCUSIÓN 164

6.1.1. Discusión del objetivo general *164*

6.1.2. Discusión del primer objetivo específico sobre trazabilidad digital *165*

6.1.3. Discusión de la fiabilidad y oportunidad de la información digital *166*

6.1.4. Discusión del segundo objetivo específico sobre trazabilidad financiera.....167

6.1.5. Discusión del tercer objetivo específico sobre articulación e imputación 168

6.2. APORTE DE LA INVESTIGACIÓN 169

CONCLUSIONES.....170

RECOMENDACIONES.....172

BIBLIOGRAFÍA.....174

ANEXOS 177

ÍNDICE DE TABLAS

Tabla 1 Componentes de la trazabilidad digital y pregunta probatoria asociada 119

Tabla 2 Niveles de análisis de la trazabilidad financiera y riesgos de inferencia 120

Tabla 3 Articulación de las rutas digital y financiera según el momento del hecho 121

Tabla 4 Estructura del razonamiento indiciario aplicada a la trazabilidad 124

Tabla 5 Matriz de categorización 134

Tabla 6 Distribución de la muestra personal por función y código 141

Tabla 7 Distribución de los participantes por función 147

Tabla 8 Composición del corpus documental 149

Tabla 9 Ejes de codificación utilizados 150

Tabla 10 Patrones documentales de trazabilidad digital 152

Tabla 11 Patrones documentales de trazabilidad financiera 156

Tabla 12 Patrones documentales de articulación probatoria 160

Tabla 13 Contraste entre entrevistas y requerimientos 161

ÍNDICE DE FIGURAS

Figura 1 Composición de la muestra personal por función 148

Figura 2 Relaciones identificadas en el tratamiento de la trazabilidad digital 153

Figura 3 Alcance de la reconstrucción financiera y posiciones diferenciadas 157

Figura 4 Articulación de las rutas para la imputación individualizada 162

RESUMEN

La investigación tuvo como objetivo analizar el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho, durante el periodo 2019-2025. Se desarrolló bajo un enfoque cualitativo, tipo básico, alcance descriptivo-interpretativo y diseño de estudio de caso documental; asimismo, se emplearon el análisis documental y la entrevista semiestructurada, considerando doce requerimientos acusatorios y ocho participantes: tres fiscales provinciales, tres fiscales adjuntos provinciales y dos asistentes en función fiscal. Los resultados evidenciaron que la trazabilidad financiera presentó mayor continuidad que la digital; sin embargo, no siempre permitió identificar al beneficiario final. La trazabilidad digital incorporó diversos identificadores técnicos, cuya eficacia dependió de la conservación de los datos, la oportunidad de las diligencias y su vinculación con usuarios determinados. Se concluyó que la titularidad de una cuenta receptora constituye un indicio relevante, pero no acredita por sí sola la autoría o participación delictiva. Por ello, resulta necesario articular ambas trazabilidades y fundamentar las inferencias probatorias, considerando la conducta individual, el conocimiento, la voluntad, los contraindicios y las hipótesis alternativas. Finalmente, se propone una matriz integrada que relacione las fuentes, los datos, los hechos acreditados, su fiabilidad, la conducta individual, la inferencia y la forma de intervención, con el propósito de fortalecer la fundamentación de la imputación fiscal.

Palabras clave: fraude informático, trazabilidad digital, trazabilidad financiera, imputación fiscal, evidencia digital.

ABSTRACT

The objective of this research was to analyze the legal treatment of digital and financial traceability to support the charges in the indictments for computer fraud filed by the Ayacucho District Attorney's Office during the 2019–2025 period. It was conducted using a qualitative, basic-level approach with a descriptive-interpretive scope and a documentary case study design; documentary analysis and semi-structured interviews were also employed, drawing on twelve indictments and eight participants: three provincial prosecutors, three deputy provincial prosecutors, and two prosecutorial assistants. The results showed that financial traceability exhibited greater consistency than digital traceability; however, it did not always allow for the identification of the ultimate beneficiary. Digital traceability incorporated various technical identifiers, the effectiveness of which depended on data retention, the timeliness of investigative procedures, and their linkage to specific users. It was concluded that ownership of a recipient account constitutes relevant evidence but does not, by itself, prove criminal authorship or participation. Therefore, it is necessary to coordinate both types of traceability and substantiate evidentiary inferences, taking into account individual conduct, knowledge, intent, counter-evidence, and alternative hypotheses. Finally, an integrated matrix is proposed that relates the sources, the data, the established facts, and their reliability, individual conduct, inferences, and the nature of involvement—to strengthen the substantiation of prosecutorial charges.

Keywords: computer-related fraud, digital traceability, financial traceability, prosecutorial attribution, digital evidence.

INTRODUCCIÓN

La expansión de la banca móvil, las billeteras digitales, el comercio electrónico y las plataformas de pago ha transformado la forma en que las personas realizan operaciones económicas. Esta transformación ha facilitado el acceso a servicios financieros, pero también ha generado nuevas oportunidades para la comisión de conductas orientadas a obtener beneficios ilícitos mediante la manipulación de datos o sistemas informáticos.

El fraude informático presenta una especial complejidad probatoria porque la operación puede ejecutarse a distancia, mediante identidades instrumentales y con la intervención de varias personas. El sujeto que crea una página falsa, obtiene las credenciales o accede al sistema no necesariamente coincide con el titular de la cuenta que recibe el dinero. También pueden intervenir personas encargadas de facilitar cuentas, retirar fondos, efectuar transferencias sucesivas o convertir el dinero en otros activos.

En estos casos, la investigación fiscal necesita reconstruir dos rutas relacionadas: la trazabilidad digital y la trazabilidad financiera. La primera comprende los registros que permiten examinar el mecanismo informático, como direcciones IP, dispositivos, líneas telefónicas, tarjetas SIM, códigos IMEI, comunicaciones, páginas falsas, datos de autenticación e informes técnicos. La segunda permite reconstruir el desplazamiento del dinero mediante cuentas de origen y destino, montos, fechas, canales, retiros y transferencias posteriores.

Aunque ambas rutas son complementarias, poseen alcances probatorios diferentes. La documentación financiera puede acreditar que el dinero ingresó a una cuenta determinada, pero la titularidad registral no demuestra necesariamente que su titular haya obtenido las credenciales, manipulado el sistema o ejecutado la transferencia. De manera similar, una dirección IP o una línea telefónica permite identificar una conexión o registro, pero no siempre individualiza a la persona que utilizó físicamente el dispositivo.

Por ello, el principal problema no consiste únicamente en determinar si la carpeta fiscal contiene información bancaria o digital. Es necesario analizar cómo dicha información fue tratada al formular la acusación, qué hechos se consideraron acreditados y qué inferencia permitió atribuir conocimiento, voluntad y una forma específica de intervención al acusado.

La Ley N.º 30096 regula el fraude informático y exige una conducta dirigida a obtener un provecho ilícito mediante la intervención sobre datos o sistemas, con perjuicio de un tercero. Asimismo, el Código Procesal Penal exige que la acusación contenga una relación clara y precisa del hecho y los elementos de convicción que la sustentan. Cuando la imputación se construye mediante indicios, el artículo 158.3 exige que estos se encuentren probados y que la inferencia responda a la lógica, la ciencia o las máximas de experiencia.

En este contexto, se formuló como problema general: ¿cómo se desarrolla el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025? Los problemas específicos se orientaron a examinar la ruta digital, analizar la reconstrucción financiera y determinar cómo ambas fueron articuladas para diferenciar la titularidad de una cuenta receptora de la autoría o participación.

El objetivo general fue analizar el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación. Los objetivos específicos consistieron en examinar la trazabilidad digital empleada para identificar y vincular al acusado con la manipulación del sistema; analizar la trazabilidad financiera utilizada para reconstruir el desplazamiento y destino del dinero; y determinar cómo ambas rutas fueron articuladas para construir una imputación individualizada.

La investigación se justificó teóricamente porque permitió sistematizar las relaciones entre evidencia digital, trazabilidad financiera, imputación fiscal y prueba indiciaria. Su justificación jurídica se vinculó con la necesidad de garantizar acusaciones

compatibles con la legalidad, la imputación necesaria, la presunción de inocencia, el principio de objetividad y el derecho de defensa. Desde una perspectiva práctica, buscó proporcionar criterios para ordenar la información y evitar que un identificador técnico o registral sea considerado automáticamente como prueba de autoría.

Metodológicamente, se desarrolló una investigación cualitativa, de tipo básico, alcance descriptivo-interpretativo y diseño de estudio de caso documental. Se aplicaron el análisis documental y la entrevista semiestructurada. La muestra documental estuvo integrada por doce requerimientos acusatorios por fraude informático, codificados como RA-01 a RA-12. La muestra personal estuvo conformada por tres fiscales provinciales, tres fiscales adjuntos provinciales y dos asistentes en función fiscal.

Los resultados mostraron que la trazabilidad financiera fue la dimensión más constante. Los requerimientos identificaron cuentas, titulares, montos y fechas, aunque el seguimiento del flujo no siempre alcanzó al beneficiario real. La trazabilidad digital presentó un desarrollo heterogéneo y estuvo condicionada por la disponibilidad de registros, la conservación de datos, la respuesta de los proveedores y la interpretación técnica.

También se determinó que la imputación fue más sólida cuando las rutas digital y financiera se integraron dentro de una cronología que relacionó el acceso, la transferencia, la recepción, el retiro y la disposición posterior. Sin embargo, algunos requerimientos presentaron mayor desarrollo en la enumeración de las fuentes que en la explicación del razonamiento utilizado para inferir conocimiento, voluntad y participación.

La investigación concluyó que la titularidad de una cuenta receptora constituye un punto inicial relevante, pero debe complementarse con control efectivo, actos de disposición, comunicaciones, coordinación, beneficio y demás hechos objetivos. Asimismo, se identificó la necesidad de diferenciar al ejecutor de la manipulación, el facilitador de cuenta, el receptor consciente y el beneficiario final.

La tesis se organiza en seis capítulos. El capítulo I desarrolla el planteamiento del problema, los objetivos, la justificación, la importancia, las delimitaciones y la viabilidad. El capítulo II presenta los antecedentes, bases teóricas, marco normativo, jurisprudencial y conceptual. El capítulo III desarrolla las categorías y subcategorías. El capítulo IV expone la metodología. El capítulo V presenta los resultados de las entrevistas y del análisis documental. Finalmente, el capítulo VI contiene la discusión de los resultados; a continuación, se presentan las conclusiones y las recomendaciones.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

A nivel internacional

La expansión de los servicios bancarios digitales, las aplicaciones móviles, las redes sociales y las plataformas de comercio electrónico ha transformado las formas de interacción económica y las modalidades de afectación del patrimonio. Las operaciones financieras pueden ejecutarse mediante dispositivos conectados a internet, aplicaciones bancarias, billeteras digitales y sistemas de autenticación remota. Paralelamente, estos recursos pueden ser utilizados para obtener información confidencial, suplantar identidades, manipular sistemas informáticos y realizar transferencias no autorizadas.

La investigación del fraude informático presenta dificultades derivadas de su posible dimensión transnacional. La conducta puede ejecutarse desde un país distinto de aquel donde se encuentra la víctima, mientras que los datos necesarios para esclarecer los hechos pueden permanecer en servidores administrados por proveedores extranjeros. Los responsables pueden utilizar identidades falsas, conexiones compartidas, redes privadas virtuales, páginas web clonadas y dispositivos que posteriormente son modificados o reemplazados. Estas circunstancias dificultan la identificación de los intervinientes y la reconstrucción de las operaciones.

Frente a esta problemática, el Convenio de Budapest constituye un marco internacional para abordar la ciberdelincuencia mediante disposiciones sustantivas, mecanismos procesales y cooperación entre Estados. Su relevancia para la investigación radica en que la obtención de información electrónica puede requerir la preservación de datos y la colaboración de autoridades y proveedores de servicios ubicados en diferentes jurisdicciones.

En este contexto, las investigaciones necesitan reconstruir dos rutas relacionadas: la trazabilidad digital y la trazabilidad financiera. La primera permite examinar el origen, desarrollo y control de las operaciones realizadas mediante sistemas informáticos, a partir de registros de acceso, direcciones IP, dispositivos,

comunicaciones y datos de autenticación. La segunda permite seguir el desplazamiento del dinero desde la cuenta afectada hasta las cuentas receptoras, transferencias posteriores, retiros, pagos o conversiones en otros activos.

La dificultad consiste en articular ambas rutas para individualizar la intervención de las personas investigadas. La identificación de una cuenta receptora no demuestra, por sí sola, quién obtuvo las credenciales o ejecutó la manipulación informática. Asimismo, una dirección IP, una línea telefónica o un dispositivo requieren corroboración para vincularlos con su usuario efectivo. Por ello, la reconstrucción de los hechos exige relacionar los datos tecnológicos y financieros con circunstancias temporales, comunicaciones y otros elementos que permitan sustentar la atribución de una conducta concreta.

A nivel nacional

En el Perú, el fraude informático se encuentra regulado principalmente por el artículo 8 de la Ley N.º 30096, Ley de Delitos Informáticos, con las modificaciones aplicables según el momento de realización de cada hecho. Su investigación exige identificar el mecanismo informático utilizado, el perjuicio patrimonial producido y la intervención atribuida a cada persona investigada. Esta exigencia adquiere especial relevancia cuando las operaciones se realizan mediante aplicaciones bancarias, billeteras digitales, páginas web o sistemas de autenticación remota.

Una de las principales dificultades consiste en establecer quién controló los medios utilizados para realizar la operación. Las líneas telefónicas pueden estar registradas a nombre de terceros; las cuentas bancarias pueden haber sido facilitadas por intermediarios; y los dispositivos pueden ser utilizados por varias personas. En consecuencia, la titularidad formal de estos recursos debe contrastarse con información sobre su uso efectivo, las comunicaciones entre los intervinientes y las circunstancias en las que se produjeron las operaciones.

La trazabilidad financiera puede demostrar que el dinero salió de la cuenta de la víctima e ingresó a una cuenta determinada. Sin embargo, este recorrido no acredita

necesariamente que el titular de la cuenta receptora haya diseñado una página falsa, obtenido las credenciales o ejecutado personalmente la transferencia. La cuenta puede haber sido utilizada por cesión voluntaria, engaño, acceso indebido o como parte de un mecanismo de recepción y dispersión del dinero. Estas posibilidades requieren ser examinadas al individualizar la conducta atribuida.

Por su parte, la evidencia digital exige procedimientos adecuados de identificación, recolección, preservación, documentación y análisis. Su alterabilidad hace necesario mantener la integridad y autenticidad de los datos desde su obtención hasta su utilización procesal. En este ámbito, el Manual para el recojo de la evidencia digital, aprobado mediante Resolución Ministerial N.º 848-2019-IN, proporciona criterios para su tratamiento (Ministerio del Interior, 2019).

La investigación fiscal también depende de información que se encuentra bajo el control de otras entidades. Los bancos pueden proporcionar datos sobre cuentas, operaciones, retiros y canales utilizados; las empresas operadoras, información sobre líneas telefónicas, tarjetas SIM y equipos; y las plataformas digitales, registros de acceso y comunicaciones. La oportunidad de los requerimientos y de las respuestas resulta relevante, porque la demora puede afectar la disponibilidad o utilidad de la información.

El Ministerio Público cuenta con mecanismos de apoyo especializado, como la Unidad Fiscal Especializada en Ciberdelincuencia y la plataforma UCIBER. No obstante, la disponibilidad de herramientas institucionales no permite asumir que su utilización se traduzca, en todos los casos, en una articulación suficiente de la información digital y financiera. Corresponde examinar cómo estos datos son incorporados y explicados en los requerimientos acusatorios.

Conforme al artículo 349 del Código Procesal Penal, el requerimiento acusatorio debe contener una relación clara y precisa del hecho atribuido, los elementos de convicción y la participación imputada, entre otros componentes. En los casos de fraude

informático, resulta necesario explicar cómo se relacionan el mecanismo tecnológico empleado, el desplazamiento del dinero y la conducta individual del acusado.

Por ello, la acusación requiere superar la mera enumeración de denuncias, estados de cuenta, cartas bancarias, reportes de operadoras, capturas de pantalla e informes técnicos. El razonamiento fiscal debe precisar qué aporta cada fuente y cómo su valoración conjunta sustenta la imputación. La cantidad de documentos no sustituye la explicación del vínculo entre el acusado y los hechos atribuidos.

A nivel local

En el Distrito Fiscal de Ayacucho, la presente investigación dispone de un corpus de doce requerimientos acusatorios por fraude informático correspondientes al periodo 2019–2025. Su revisión preliminar permite identificar modalidades relacionadas con páginas bancarias clonadas, captación de credenciales, sustitución de tarjetas SIM, llamadas de suplantación, transferencias por internet, cuentas receptoras, retiros mediante cajeros automáticos y utilización de criptomonedas.

Asimismo, en estos documentos aparecen informes bancarios, registros de operaciones, direcciones IP, capturas de comunicaciones, informes técnicos, información de operadoras y declaraciones de los intervinientes. La diversidad de estas fuentes permite analizar cómo la Fiscalía reconstruye las operaciones y qué razonamiento desarrolla para vincular los datos obtenidos con la participación atribuida a cada acusado.

El problema de investigación se centra en la articulación de la trazabilidad digital y financiera. Mientras que la ruta financiera permite seguir el dinero hasta las cuentas receptoras y sus movimientos posteriores, la ruta digital busca esclarecer quién controló los recursos empleados para obtener las credenciales o ejecutar las operaciones. Resulta necesario examinar cómo los requerimientos relacionan ambas rutas y qué elementos utilizan para diferenciar las posibles formas de intervención.

También corresponde analizar el tratamiento fiscal de las limitaciones técnicas. La falta de identificación del usuario de una dirección IP, la imposibilidad de recuperar

información eliminada, las dificultades para acceder a registros conservados en el extranjero o la ausencia de datos sobre el uso material de un dispositivo pueden restringir la reconstrucción de los hechos. Frente a estas circunstancias, interesa conocer qué diligencias se realizaron, qué resultados se obtuvieron y cómo se justificó la imputación con los elementos disponibles.

En consecuencia, la problemática no se limita a determinar si los requerimientos contienen documentación bancaria o información digital. Se busca comprender cómo la Fiscalía utiliza estas fuentes al construir la acusación: si presenta únicamente una descripción cronológica de operaciones o si desarrolla inferencias que explican el vínculo entre el acusado, el mecanismo informático y el desplazamiento del dinero.

El periodo 2019–2025 delimita el análisis documental de los requerimientos seleccionados. El estudio no pretende medir estadísticamente la totalidad de investigaciones por fraude informático del Distrito Fiscal de Ayacucho ni determinar la culpabilidad de las personas acusadas. Su alcance se concentra en el razonamiento exteriorizado en los documentos examinados y en la forma en que se utiliza la trazabilidad digital y financiera para sustentar la imputación.

Por tanto, resulta necesario analizar las diligencias y fuentes empleadas para reconstruir la ruta digital, los mecanismos utilizados para seguir el desplazamiento del dinero y la articulación de ambos componentes al atribuir una conducta penalmente relevante. Este análisis permitirá identificar criterios comunes, diferencias en el desarrollo argumentativo y aspectos que requieren fortalecimiento en los requerimientos acusatorios estudiados.

1.2. Formulación del problema

1.2.1. Problema general

¿Cómo se desarrolla el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025?

1.2.2. Problemas específicos

- ¿Cómo se desarrolla la trazabilidad digital para identificar y vincular al acusado con la manipulación del sistema informático en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025?
- ¿Cómo se desarrolla la trazabilidad financiera para reconstruir el desplazamiento y destino del dinero en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025?
- ¿Cómo se articulan la trazabilidad digital y financiera para sustentar la imputación y diferenciar la titularidad de una cuenta receptora de la autoría o participación en el fraude informático?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Analizar el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025.

1.3.2. Objetivos específicos

- Examinar el tratamiento de la trazabilidad digital para identificar y vincular al acusado con la manipulación del sistema informático en los requerimientos acusatorios por fraude informático.
- Analizar el tratamiento de la trazabilidad financiera para reconstruir el desplazamiento y destino del dinero en los requerimientos acusatorios por fraude informático.
- Determinar cómo se articulan la trazabilidad digital y financiera para sustentar la imputación y diferenciar la titularidad de una cuenta receptora de la autoría o participación en el fraude informático.

1.4. Justificación de la investigación

1.4.1. Justificación teórica

La investigación se justificó teóricamente por la necesidad de examinar las relaciones entre trazabilidad digital, trazabilidad financiera, evidencia electrónica e imputación fiscal en casos de fraude informático. El estudio permitió distinguir el seguimiento de una operación o de un flujo monetario de la individualización de la conducta de una persona. Esta distinción orientó el análisis del alcance de los identificadores técnicos y registrales utilizados en las acusaciones.

El aporte teórico consistió en organizar el análisis mediante la relación entre fuente de información, dato obtenido, hecho sustentado, fiabilidad, conducta atribuida, inferencia y forma de intervención. Este esquema permitió examinar cómo la Fiscalía pasó de la descripción de los registros a la formulación de una hipótesis de autoría o participación, así como identificar los aspectos del razonamiento que requerían mayor explicitación.

1.4.2. Justificación jurídica

La investigación se justificó jurídicamente por la relevancia de una imputación individualizada para el debido proceso, la presunción de inocencia y el derecho de defensa. El análisis se orientó a examinar la fundamentación de las conductas atribuidas, evitando equiparar la titularidad de una cuenta, línea o dispositivo con una conclusión automática de responsabilidad.

La Ley N.º 30096 y el Código Procesal Penal proporcionaron el marco para examinar el delito imputado y el contenido de las acusaciones. En particular, el artículo 349 permitió orientar la revisión de la claridad del hecho, los elementos de convicción y la participación atribuida. El Convenio sobre la Ciberdelincuencia complementó el contexto jurídico de preservación y cooperación para obtener información electrónica. La investigación examinó estos referentes atendiendo a su pertinencia para los casos y al periodo delimitado.

1.4.3. Justificación práctica

La investigación se justificó en el plano práctico porque examinó cómo fueron utilizados los informes bancarios, estados de cuenta, registros de operaciones, datos de telecomunicaciones, comunicaciones e informes técnicos al formular los requerimientos acusatorios. Su utilidad consistió en identificar las conexiones desarrolladas entre estas fuentes y los aspectos que permanecieron insuficientemente explicados en los documentos estudiados.

A partir del análisis se formuló una propuesta de matriz integrada de trazabilidad e imputación. Esta relacionó la fuente, el dato digital o financiero, la fecha y hora, la persona vinculada, las condiciones de fiabilidad, la conducta atribuida y la inferencia utilizada. Asimismo, incorporó el examen de limitaciones y explicaciones alternativas. La propuesta se planteó como una herramienta de organización y revisión; el estudio no evaluó su eficacia mediante una aplicación posterior.

1.4.4. Justificación metodológica

La justificación metodológica se sustentó en la complementariedad del análisis documental y la entrevista semiestructurada. El primero permitió examinar el razonamiento exteriorizado en doce requerimientos acusatorios; la segunda aportó los criterios y dificultades referidos por los ocho participantes consignados en la tesis. Ambas técnicas se organizaron en función de la trazabilidad digital, la trazabilidad financiera y su articulación para sustentar la imputación.

La comparación entre documentos, entrevistas y referentes jurídicos permitió examinar coincidencias y diferencias entre los criterios expresados y su formulación en las acusaciones. La ficha de análisis documental y la guía de entrevista facilitaron la organización de las fuentes y de las unidades de significado. El aporte metodológico correspondió a un procedimiento de análisis cualitativo del corpus seleccionado, sin pretensión de representatividad estadística.

1.4.5. Justificación social

La investigación se justificó socialmente por la afectación patrimonial que pueden producir las operaciones informáticas ilícitas y por las dificultades que enfrentan las víctimas para identificar a sus responsables. El tratamiento adecuado de la información digital y financiera resulta relevante para sustentar la persecución penal y evitar que la complejidad tecnológica impida esclarecer la intervención de las personas investigadas.

Asimismo, una atribución sustentada únicamente en datos registrales puede afectar a personas cuya intervención no ha sido suficientemente individualizada. El estudio abordó esta tensión mediante el examen del razonamiento fiscal, considerando tanto el interés en esclarecer los hechos como la protección de las garantías del imputado. Su contribución social se circunscribió a los criterios de análisis propuestos y no a la demostración de una reducción de la impunidad.

1.5. Importancia de la investigación

La importancia de la investigación radicó en el examen de la relación entre la operación informática, el desplazamiento del dinero y la conducta individual atribuida al acusado. El estudio permitió distinguir la incorporación de documentación del desarrollo de una explicación que conectara los datos con la imputación. Esta diferencia fue relevante para comprender el alcance argumentativo de los requerimientos acusatorios.

El análisis también permitió examinar las diferencias entre el receptor formal, quien controló la cuenta, el ejecutor de la manipulación y el eventual beneficiario final. Estas distinciones orientaron la revisión de casos que comprendieron cuentas facilitadas a terceros, negación de conocimiento, retiros posteriores, sustitución de tarjetas SIM y dificultades para identificar al usuario de un recurso técnico.

Los criterios sistematizados ofrecieron una base para revisar la claridad de las acusaciones y la exteriorización de sus inferencias. Su importancia se vinculó con la posibilidad de facilitar el control del razonamiento fiscal y la comprensión de la conducta imputada, dentro de los límites del corpus estudiado.

1.6. Delimitación de la investigación

1.6.1. Delimitación temática

La investigación se delimitó al tratamiento fiscal de la trazabilidad digital y financiera utilizada para sustentar la imputación en requerimientos acusatorios por fraude informático. La dimensión digital comprendió el examen de direcciones IP, registros de acceso, dispositivos, líneas telefónicas, tarjetas SIM, códigos IMEI, comunicaciones, capturas de pantalla, páginas falsas e información técnica mencionada en los documentos.

La dimensión financiera comprendió las cuentas de origen y destino, su titularidad, los montos, fechas, canales utilizados, retiros, transferencias posteriores y referencias a billeteras digitales o criptomonedas. La articulación de ambas dimensiones se examinó mediante la correspondencia temporal y funcional de los datos, la individualización de las conductas y las inferencias sobre conocimiento y voluntad.

El estudio no determinó la culpabilidad de los acusados ni examinó integralmente la pena, la reparación civil o todos los delitos previstos en la Ley N.º 30096. Su objeto fue el razonamiento fiscal expresado en las acusaciones seleccionadas.

1.6.2. Delimitación espacial e institucional

La investigación se desarrolló en el ámbito del Distrito Fiscal de Ayacucho y comprendió requerimientos acusatorios formulados por fiscalías provinciales penales corporativas pertenecientes a dicho distrito fiscal. La dimensión personal correspondió a fiscales provinciales, fiscales adjuntos provinciales y asistentes en función fiscal con experiencia vinculada con la investigación o tramitación de casos de fraude informático, según la muestra descrita en la tesis.

1.6.3. Delimitación temporal

El estudio comprendió el periodo 2019–2025, definido en función del año de emisión de los requerimientos acusatorios seleccionados. Este criterio se diferenció del año de comisión de los hechos o de apertura de las carpetas fiscales, que podía ser anterior al intervalo establecido.

El análisis normativo consideró la versión aplicable a los hechos examinados. La comparación entre los documentos tuvo en cuenta su contexto temporal, sin asumir que las herramientas técnicas e institucionales estuvieron disponibles de manera uniforme durante todo el periodo.

1.6.4. Delimitación documental

La muestra documental estuvo conformada por doce requerimientos acusatorios por fraude informático, identificados mediante los códigos RA-01 a RA-12. El análisis se concentró en los hechos imputados, las fuentes digitales y financieras mencionadas, la conducta individual atribuida y el razonamiento utilizado para relacionar los elementos de convicción.

La selección consideró la pertinencia temática y la legibilidad de los documentos. Se excluyeron duplicados y documentos cuyo contenido no permitía analizar los aspectos definidos. Cuando un requerimiento comprendió otros delitos, el examen se circunscribió a los extremos vinculados con el fraude informático. Los informes y anexos mencionados se analizaron únicamente en la medida en que su contenido fue reproducido o explicado en el material disponible.

1.6.5. Delimitación personal

La muestra personal estuvo conformada por ocho participantes: tres fiscales provinciales, tres fiscales adjuntos provinciales y dos asistentes en función fiscal. Sus aportes se delimitaron a los criterios y experiencias relacionados con la investigación, elaboración, revisión o tramitación de requerimientos acusatorios por fraude informático. La información fue interpretada conforme a la función de cada participante y al alcance cualitativo del estudio, sin extenderla a todos los integrantes del Ministerio Público.

1.7. Limitaciones y viabilidad

1.7.1. Limitaciones

La primera limitación correspondió a la naturaleza del corpus documental. Los requerimientos seleccionados pertenecieron a investigaciones que culminaron con una decisión fiscal de acusar. Por tanto, los resultados no comprendieron las

particularidades de casos archivados o sobreseídos ni permitieron evaluar la efectividad general de la investigación del fraude informático en el distrito fiscal.

La diversidad temporal constituyó una segunda limitación. Los documentos fueron emitidos entre 2019 y 2025, periodo en el que variaron las herramientas tecnológicas y los mecanismos institucionales disponibles. Esta circunstancia exigió interpretar las diferencias atendiendo al contexto de cada requerimiento y restringió las comparaciones que presuponían condiciones idénticas.

Una tercera limitación fue el alcance de la información exteriorizada. La mención de informes técnicos, anexos o diligencias no siempre permitió revisar íntegramente sus contenidos. Por ello, la ausencia de un dato en el requerimiento no fue equiparada, por sí sola, con la inexistencia de la diligencia o del documento en la carpeta fiscal. El análisis se circunscribió a lo verificable en el material disponible.

La heterogeneidad de las modalidades también condicionó la comparación. Los casos presentaron mecanismos operativos distintos, por lo que se compararon los componentes de trazabilidad y las estructuras de fundamentación, sin exigir que todos contuvieran los mismos identificadores o actuaciones técnicas.

La información de las entrevistas estuvo limitada a las experiencias y apreciaciones de los ocho participantes. Sus respuestas no sustituyeron la constatación documental ni permitieron afirmar que los criterios expresados fueran aplicados uniformemente en todas las investigaciones. Asimismo, el estudio no examinó si las acusaciones concluyeron en condena o absolución, por lo que no estableció una relación entre el tratamiento fiscal de la trazabilidad y el resultado judicial definitivo.

1.7.2. Viabilidad

La investigación fue viable documentalmente por la disponibilidad de doce requerimientos acusatorios con contenido pertinente para examinar los hechos imputados, las fuentes utilizadas y la fundamentación fiscal. Este acceso permitió delimitar un corpus concreto y desarrollar un análisis organizado de la información exteriorizada.

La viabilidad metodológica se sustentó en el uso de una ficha de análisis documental y una guía de entrevista semiestructurada. La organización por categorías, la comparación entre documentos y la integración de fuentes permitieron abordar los objetivos desde un enfoque cualitativo. La dimensión técnica no exigió reproducir pericias, porque el objeto consistió en examinar cómo sus resultados fueron incorporados y utilizados en las acusaciones.

El estudio se desarrolló con fines académicos y sin emitir pronunciamiento sobre la responsabilidad penal de las personas involucradas. La codificación de los documentos y participantes permitió orientar la presentación de la información hacia el razonamiento fiscal. Finalmente, la disponibilidad del material documental y de herramientas de procesamiento de textos hizo posible realizar el trabajo con los recursos del investigador.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Alzate Obando y Aponte Bedoya (2025), en el estudio “Garantías del debido proceso en delitos informáticos, municipio de Pereira durante los años 2020-2021”, examinaron la respuesta procesal frente al incremento de conductas informáticas. Las autoras destacaron que la eficacia investigativa no puede desligarse de las garantías de contradicción, defensa, legalidad y autenticidad de la evidencia. Su aporte para la presente tesis consiste en recordar que la trazabilidad no es únicamente una reconstrucción técnica: debe obtenerse por procedimientos legítimos, documentarse de modo verificable y ponerse en conocimiento de la defensa con posibilidad real de cuestionamiento.

Reyes Quezada y Palacios Rodas (2026), en el estudio “Marco jurídico ecuatoriano versus Convenio de Budapest: Análisis comparativo de la recolección de evidencia digital en phishing transfronterizo durante el período 2020-2024”, compararon el marco ecuatoriano con el Convenio de Budapest respecto de la recolección de evidencia digital en casos de phishing transfronterizo. Identificaron dificultades asociadas a la volatilidad de los datos, la ausencia de mecanismos suficientemente rápidos de conservación, la dispersión jurisdiccional y la coordinación interinstitucional. Aunque el estudio se publicó después del periodo documental 2019-2025, resulta útil como fuente teórica actual: demuestra que la pérdida de registros o la demora en requerirlos puede interrumpir el enlace entre el evento digital y el movimiento financiero.

Carriel Cagua et al. (2026) en el estudio “Responsabilidad penal en delitos informáticos: desafíos de la persecución penal en entornos digitales”, analizaron los desafíos de atribuir responsabilidad penal en entornos digitales. Su planteamiento resalta que la deslocalización, el anonimato, el uso de identidades instrumentales y la intervención de múltiples infraestructuras dificultan enlazar una conducta con una persona. Para esta investigación, dicho aporte permite sostener que la imputación no

puede descansar en un identificador aislado; requiere correlacionar datos de conexión, control del dispositivo, comunicaciones, operaciones económicas y actos posteriores.

Ramos Mera (2026) en el estudio “La funcionalidad informática como objeto de tutela penal: Bases dogmáticas para la comprensión del bien jurídico en los delitos informáticos”, desarrolló una propuesta dogmática sobre la funcionalidad informática como objeto de tutela penal. La tesis de la funcionalidad permite comprender que los ataques informáticos no solo lesionan patrimonio o privacidad, sino también la confiabilidad y disponibilidad de sistemas y datos. En el fraude informático peruano, este enfoque es complementario: el tipo penal protege el patrimonio frente a una transferencia o ventaja obtenida mediante interferencia o manipulación informática, pero la conducta se ejecuta necesariamente sobre funciones o datos de un sistema.

Monroy Sotomayor (2026), en el estudio “Evolución de la cibercriminalidad y desafíos del Derecho penal frente a los delitos informáticos”, estudió la evolución de la cibercriminalidad y los desafíos del Derecho penal. Señaló que la digitalización amplía la escala, automatización y transnacionalidad de las conductas, mientras las categorías tradicionales enfrentan problemas para identificar autores y preservar evidencia. Este antecedente doctrinal contextualiza la necesidad de una teoría de imputación adaptada a cadenas tecnológicas y financieras, sin abandonar los principios de responsabilidad por el hecho y culpabilidad.

2.1.2. Antecedentes nacionales

Herrera Figueroa (2026), en la tesis “La incidencia del delito de fraude informático y la protección efectiva del ciudadano, distrito judicial de Huánuco, 2022-2023”, examinó expedientes y actuaciones vinculadas con la investigación del fraude informático. Entre los aspectos abordados se encuentran la intervención policial, la especialización en recojo de evidencias, la suficiencia de la investigación fiscal, la identificación de autores y partícipes y la formulación de acusaciones. El trabajo es especialmente cercano a la presente investigación porque evidencia que la protección

penal efectiva depende de convertir información tecnológica y bancaria en elementos capaces de individualizar una intervención concreta.

Villacorta Saldaña (2026), en la tesis “La disposición de archivo preliminar en el delito informático y la inobservancia de los fines del proceso penal en la Segunda Fiscalía Corporativa de Huánuco, 2022-2023”, estudió carpetas archivadas y factores como la suficiencia de indicios, la imputación necesaria, la presencia de elementos de cargo y descargo, la especialización y la disponibilidad de peritos. El antecedente funciona como contraste con una muestra de requerimientos acusatorios: mientras estos últimos representan investigaciones que alcanzaron la etapa acusatoria, los archivos permiten advertir qué carencias impiden construir la trazabilidad o individualizar al responsable.

Vinelli Vereau (2021), en el artículo “Los delitos informáticos y su relación con la criminalidad económica”, analizó la relación entre delitos informáticos y criminalidad económica. El autor explicó la transformación de fraudes tradicionales a través de medios tecnológicos y examinó modalidades como phishing y pharming. Para la tesis, su contribución reside en vincular la manipulación informática con el desplazamiento patrimonial y en diferenciar el fraude informático de la estafa tradicional: en el primero, la afectación se produce por intervención en datos o sistemas y no necesariamente por un error inducido en una persona.

Ventura Quijano (2021), en la tesis “La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020”, estudió modalidades de fraude como phishing, smishing y vishing, destacando su combinación de ingeniería social, suplantación y operaciones financieras. El trabajo permite comprender que el requerimiento acusatorio debe reconstruir dos planos conectados: la captación o manipulación digital y la disposición patrimonial. La sola acreditación del engaño comunicacional no identifica a quien controló el destino de los fondos; a su vez, la titularidad de la cuenta receptora no prueba por sí misma quién ejecutó la intrusión o captación.

Estrada Salvador Ramírez (2024), en el artículo “La impunidad en los delitos informáticos. Una problemática de poco interés para legisladores, jueces y fiscales”, abordó la impunidad en los delitos informáticos y señaló como factor recurrente la dificultad para individualizar al ciberdelincuente. Destacó, además, que la respuesta fiscal depende de la cooperación oportuna de entidades financieras y empresas de telecomunicaciones. Este planteamiento se conecta directamente con el objeto de estudio: una acusación sólida requiere integrar registros que suelen estar bajo custodia de terceros y cuya utilidad disminuye cuando se obtienen tardíamente o sin información técnica suficiente.

2.2. Bases teóricas

2.2.1. Sociedad digital, criminalidad informática y economía del dato

La prestación de servicios financieros mediante aplicaciones, banca móvil, billeteras digitales y plataformas de pago ha reducido el tiempo entre acceso, orden y transferencia. Esa misma arquitectura produce registros técnicos: direcciones IP, sellos de tiempo, identificadores de sesión, características del dispositivo, autenticaciones, cuentas de origen y destino. La criminalidad informática aprovecha la velocidad y deslocalización del sistema, pero deja rastros distribuidos entre diferentes custodios. Por ello, investigar no consiste en hallar una única “huella digital”, sino en recomponer una secuencia fragmentada.

La cibercriminalidad comprende conductas en las que los sistemas o datos son objeto del ataque y conductas tradicionales potenciadas por tecnologías. El fraude informático pertenece al núcleo en el que el medio tecnológico integra la estructura típica: la ventaja o el perjuicio patrimonial se produce mediante diseño, introducción, alteración, borrado, supresión, clonación de datos o interferencia en el funcionamiento de un sistema. Esta característica exige una lectura dogmática y técnica coordinada.

2.2.2. Delitos informáticos: concepto y clasificación

Los delitos informáticos pueden definirse como conductas dolosas que lesionan o ponen en peligro bienes jurídicos mediante la afectación, utilización abusiva o

interferencia de sistemas y datos. Su nota distintiva no es simplemente el uso de un teléfono o computadora. La tecnología debe cumplir una función relevante en la ejecución, el objeto de protección o la producción del resultado.

Una clasificación útil distingue: a) delitos contra datos y sistemas, como acceso ilícito, atentados a integridad o interceptación; b) delitos patrimoniales ejecutados mediante manipulación informática, como el fraude informático; c) delitos relacionados con identidad, contenido o intimidad; y d) conductas conexas, como comercialización de credenciales, dispositivos o programas. La clasificación ayuda a precisar concursos y evita subsumir todo evento tecnológico bajo una sola figura.

2.2.3. Bien jurídico protegido

La doctrina debate si existe un bien jurídico informático autónomo. Ramos Mera (2026) propone la funcionalidad informática, entendida como confiabilidad, integridad, disponibilidad y funcionamiento de sistemas y datos. En cambio, los tipos patrimoniales mantienen como referente inmediato el patrimonio. Ambas perspectivas pueden coexistir: el fraude informático protege el patrimonio, pero la modalidad de lesión presupone una intervención indebida sobre la funcionalidad o los datos del sistema.

Esta precisión incide en la imputación. No basta acreditar que la víctima perdió dinero. Debe describirse el mecanismo informático relevante y su relación causal con la ventaja obtenida. De igual forma, no toda anomalía informática produce fraude consumado; puede tratarse de acceso ilícito, tentativa, acto preparatorio o una conducta atípica según el caso.

2.2.4. Fraude informático en el ordenamiento peruano

El artículo 8 de la Ley N.º 30096, modificado por la Ley N.º 30171, sanciona a quien procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante determinadas formas de intervención sobre datos o sistemas informáticos. La lectura del tipo exige identificar: el sujeto activo; la conducta informática desplegada; el nexo con el resultado o ventaja; el provecho ilícito; el perjuicio; y el dolo. En los casos del

periodo 2019-2025 debe aplicarse la versión normativa vigente al momento del hecho y observarse el principio de legalidad temporal.

El núcleo de injusto no se agota en recibir dinero de procedencia ilícita. La fiscalía debe explicar cómo la persona participó en la operación informática o, según la tesis de participación, cómo prestó un aporte doloso al hecho principal. Si la acusación se dirige contra el titular de una cuenta receptora, debe precisar si se le atribuye ejecución, coautoría, complicidad u otra forma de intervención y qué hechos demuestran conocimiento y voluntad.

2.2.5. Diferencia entre fraude informático y estafa

La estafa tradicional se estructura alrededor del engaño idóneo que genera error en una persona, conduce a una disposición patrimonial y produce perjuicio. En el fraude informático, la alteración patrimonial deriva de la manipulación o interferencia de datos o sistemas. La diferencia es relevante en modalidades híbridas: un mensaje de phishing puede engañar a la víctima para que entregue credenciales, pero la posterior operación no autorizada puede ejecutarse mediante el sistema. La calificación depende de la forma concreta en que se produjo la disposición y del dominio del curso causal.

La acusación debe evitar fórmulas genéricas como “mediante engaño informático”. Debe precisar quién recibió la comunicación, qué dato fue obtenido, cómo se utilizó, qué sistema procesó la orden, desde dónde se inició sesión, a qué cuenta se transfirió el dinero y qué intervención se atribuye a cada acusado.

2.2.6. Modalidades relevantes: phishing, smishing, vishing, pharming y suplantación

El phishing utiliza comunicaciones o sitios que aparentan pertenecer a una entidad confiable para captar credenciales. El smishing emplea mensajes de texto; el vishing, llamadas o comunicaciones de voz; el pharming redirige al usuario hacia un entorno falso; y la suplantación de SIM puede permitir recibir códigos de autenticación. Estas expresiones describen técnicas, no tipos penales autónomos. Su relevancia jurídica depende de la conducta finalmente acreditada.

Estas modalidades suelen distribuir funciones: creación del sitio, adquisición de dominios, envío masivo, obtención de credenciales, acceso a la banca, recepción de fondos, retiro o dispersión. La división operativa obliga a individualizar aportes y no presumir que todos los intervinientes realizaron cada acto. La trazabilidad debe ayudar a ubicar a cada persona dentro de la secuencia.

2.2.7. Evidencia digital

La evidencia digital es información con valor potencial para acreditar hechos y que se genera, procesa, almacena o transmite mediante sistemas electrónicos. Puede consistir en contenido —mensajes, archivos o imágenes— y en datos de contexto —metadatos, registros de acceso, direcciones IP, sellos de tiempo o identificadores de dispositivo—. Su significado surge de la relación con otras fuentes y no de su apariencia aislada.

Sus características principales son la volatilidad, duplicabilidad, alterabilidad, dependencia de herramientas de lectura y dispersión. Un registro puede ser retenido por un plazo limitado, utilizar una zona horaria distinta o requerir interpretación técnica. Por eso, la fiscalía debe solicitarlo oportunamente, conservar su formato original, documentar su obtención y asegurar que el perito explique alcance y limitaciones.

2.2.8. Autenticidad, integridad y cadena de custodia

La autenticidad responde a si el dato es lo que se afirma que es; la integridad, a si se mantuvo sin alteraciones relevantes; y la fiabilidad, a si el procedimiento de generación y obtención permite confiar en su contenido. La cadena de custodia registra quién obtuvo, recibió, trasladó, examinó y almacenó la evidencia. No reemplaza la valoración, pero permite controlar continuidad y detectar riesgos de contaminación.

En copias forenses, una función hash permite comparar estados del archivo o soporte. La coincidencia del valor respalda que el contenido no cambió entre dos momentos; no demuestra por sí sola quién creó el dato ni la veracidad de su contenido. Esta distinción debe aparecer en la motivación fiscal para no atribuir a una técnica de integridad un alcance identificador que no posee.

2.2.9. Trazabilidad digital

Para esta tesis, la trazabilidad digital es el proceso fiscal de identificar, ordenar, verificar y relacionar registros electrónicos que permiten reconstruir el origen, recorrido, transformación y destino de una actuación digital relevante. No equivale a una lista de documentos tecnológicos. Exige continuidad lógica y temporal, identificación del custodio, explicación del significado técnico y conexión con una persona o evento.

Toscano-Quispe et al. (2026) explican, en el ámbito de cadenas de suministro, que la fragmentación, falta de interoperabilidad y baja estandarización generan discontinuidades. Aunque su objeto no es penal, estas categorías son transferibles con cautela: una investigación también falla cuando los datos de banco, operador y proveedor se conservan en formatos incompatibles, con tiempos no normalizados o identificadores que no pueden cruzarse.

Tabla 1
Componentes de la trazabilidad digital y pregunta probatoria asociada

Componente	Ejemplos	Pregunta probatoria
Evento	Inicio de sesión, cambio de clave, transferencia, descarga.	¿Qué ocurrió y en qué momento?
Identificador	IP, IMEI, IMSI, número, usuario, token, dispositivo.	¿Qué sistema o recurso estuvo asociado al evento?
Custodio	Banco, operador, proveedor, plataforma, perito.	¿Quién generó y conservó el registro?
Contexto	Zona horaria, IP compartida, VPN, NAT, geolocalización aproximada.	¿Qué límites tiene la atribución?
Corroboración	Incautación, mensajes, cámaras, ubicación, reconocimiento.	¿Qué fuente independiente confirma el enlace personal?

Nota. Elaboración propia.

2.2.10. Alcance y límites de los identificadores digitales

Una dirección IP identifica una conexión o punto de salida en un momento determinado, no necesariamente a la persona que operó el dispositivo. Puede ser dinámica, compartida, traducida mediante NAT, utilizada por redes públicas o

encubierta con VPN. El IMEI identifica un equipo; el IMSI, una suscripción; el número telefónico, una línea asignada. Ninguno acredita automáticamente control físico, conocimiento o dolo.

La atribución se fortalece cuando convergen: asignación temporal del identificador; incautación del dispositivo; sesión activa; contenido relacionado; ubicación compatible; comunicaciones previas o posteriores; y movimientos financieros coordinados. También debe examinarse si hubo robo del equipo, duplicado de SIM, préstamo, acceso remoto o suplantación.

2.2.11. Trazabilidad financiera

La trazabilidad financiera es la reconstrucción documentada del origen, canal, secuencia, destino y disposición final de fondos relacionados con el hecho investigado. Incluye datos de la cuenta ordenante y receptora, fecha y hora, monto, canal, código de operación, beneficiario, cuentas intermedias, retiros, compras, transferencias posteriores y mecanismos de conversión.

Su finalidad probatoria no es solo demostrar el perjuicio. Permite identificar nodos, establecer proximidad temporal, detectar dispersión, vincular comunicaciones con operaciones y comprobar actos de aprovechamiento. Sin embargo, la titularidad registral de una cuenta no equivale necesariamente a control efectivo. Pueden existir cuentas cedidas, captadas, suplantadas o utilizadas por terceros.

Tabla 2
Niveles de análisis de la trazabilidad financiera y riesgos de inferencia

Nivel	Contenido mínimo	Riesgo de inferencia
Formal	Titular, apertura, datos declarados.	Confundir titularidad con autoría.
Operativo	Canal, dispositivo, IP, autenticación, agencia o cajero.	Omitir que el canal pudo ser usado por tercero.
Económico	Destino, retiro, consumo, dispersión, beneficiario final.	Detener el análisis en la primera cuenta receptora.
Subjetivo	Mensajes, contraprestación, patrón, ocultamiento, explicación.	Presumir conocimiento por el solo movimiento.

Nota. Elaboración propia.

2.2.12. Registros bancarios, secreto bancario y control judicial

La obtención de información financiera debe respetar la Constitución y las reglas procesales sobre secreto bancario, levantamiento y requerimiento de información. La legalidad de acceso condiciona su uso. El fiscal debe definir periodo, productos, personas y datos necesarios, evitando solicitudes indiscriminadas y asegurando que la información recibida corresponda al mandato autorizado.

El informe bancario debe ser interpretado junto con sus anexos originales. Un resumen elaborado por un analista puede orientar, pero la acusación debe permitir verificar las operaciones fuente. Cuando se utilicen términos técnicos —token, OTP, host, comercio, adquirente o pasarela— corresponde explicar su función y límites.

2.2.13. Articulación de trazabilidad digital y financiera

La hipótesis se robustece cuando ambas rutas se cruzan en tiempos, dispositivos, comunicaciones y actos de disposición. La ruta digital explica cómo se obtuvo o ejecutó la orden; la financiera muestra dónde ingresó y cómo se movilizó el beneficio. La convergencia no significa que un dato complete automáticamente al otro: cada hecho base debe acreditarse con una fuente fiable.

Tabla 3
Articulación de las rutas digital y financiera según el momento del hecho

Momento	Ruta digital	Ruta financiera	Resultado esperado
Preparación	Dominio, mensaje, contacto, cambio de SIM.	Apertura o captación de cuenta.	Contexto y planificación.
Ejecución	Acceso, sesión, autenticación, orden.	Cargo y abono correlativos.	Mecanismo y resultado.
Disposición	Mensajes de coordinación, ubicación, dispositivo.	Retiro, compra, dispersión.	Control y aprovechamiento.
Posterior	Borrado, bloqueo, cambio de línea.	Fraccionamiento o transferencia final.	Ocultamiento o explicación alternativa.

Nota. Elaboración propia.

2.2.14. Tratamiento fiscal de la trazabilidad

El tratamiento fiscal comprende decisiones de obtención, preservación, análisis, correlación y presentación de datos digitales y financieros. Tiene una dimensión investigativa —qué diligencias se ordenan y con qué oportunidad— y una dimensión argumentativa —cómo se transforma la información en hechos y cómo estos sustentan la imputación—. La tesis se concentra en lo exteriorizado en los requerimientos acusatorios, sin presumir razonamientos no documentados.

Un tratamiento adecuado debe: identificar la fuente; describir el dato relevante; justificar autenticidad y fiabilidad; normalizar fechas y zonas horarias; distinguir dato bruto de informe interpretativo; formular el hecho que se considera acreditado; relacionarlo con otros hechos; considerar contraindicios; y concluir sobre el aporte individual. La acumulación de anexos sin esa secuencia produce volumen documental, no necesariamente motivación.

2.2.15. Imputación fiscal e imputación necesaria

La imputación es la atribución concreta de un hecho penalmente relevante a una persona. En la acusación debe contener un componente fáctico, uno jurídico y uno probatorio. El primero describe qué hizo, cuándo, dónde, cómo y con qué intervención; el segundo identifica el tipo penal y la forma de participación; el tercero expone los elementos de convicción que sustentan cada proposición relevante.

La imputación necesaria impide fórmulas colectivas o ambiguas. En delitos ejecutados mediante cadenas, no basta afirmar que los acusados “se concertaron” o “realizaron transferencias fraudulentas”. Debe precisarse quién captó credenciales, quién accedió, quién proporcionó o controló la cuenta, quién retiró los fondos y qué conocimiento se atribuye. Si una función no pudo determinarse, la acusación debe expresar la inferencia que permite sostener la forma de intervención propuesta.

2.2.16. Autoría, coautoría y participación en entornos digitales

La autoría se determina por la realización del hecho típico o el dominio que corresponda según la teoría adoptada. La coautoría exige decisión común y aporte

esencial dentro de una división funcional. La complicidad supone un auxilio doloso al hecho principal. La presencia de infraestructura compartida o una relación personal no reemplaza la prueba de acuerdo, aporte y conocimiento.

En entornos digitales, la distribución de tareas puede ser remota y asincrónica. Esto no elimina los requisitos dogmáticos. La fiscalía debe distinguir entre el creador de la infraestructura, el operador, el receptor, el retirador y el beneficiario. La relevancia penal depende del aporte concreto y de la representación del plan delictivo, no de una etiqueta técnica.

2.2.17. Titular de cuenta, "mula financiera" y conductas neutrales

Una cuenta receptora constituye un punto de partida relevante, pero su titular puede ocupar posiciones distintas: operador consciente, facilitador remunerado, persona captada mediante engaño, víctima de suplantación o titular que perdió control. Para atribuir participación dolosa deben buscarse hechos adicionales: entrega deliberada de credenciales o tarjeta, recepción de comisión, coordinación, retiros inmediatos, reiteración, explicaciones falsas o disposición del dinero.

La teoría de las conductas neutrales exige cautela frente a actos cotidianos que pueden favorecer un delito. Abrir una cuenta, transferir dinero o prestar un teléfono no son por sí solos actos de complicidad. Adquieren relevancia cuando el contexto demuestra adaptación al plan delictivo y conocimiento del riesgo concreto. La acusación debe exteriorizar por qué descarta una actuación ordinaria, negligente o engañada.

2.2.18. Prueba indiciaria e inferencia probatoria

Debido a que la autoría informática rara vez se observa directamente, la imputación suele apoyarse en indicios. El artículo 158.3 del Código Procesal Penal exige que el indicio esté probado y que la inferencia responda a la lógica, ciencia o máximas de experiencia; cuando los indicios sean contingentes, deben ser plurales, concordantes y convergentes, sin contraindicios consistentes.

El Tribunal Constitucional, en el caso Llamoja Hilares (Exp. N.º 00728-2008-PHC/TC), destacó la necesidad de exteriorizar el razonamiento indiciario. La estructura

mínima comprende: fuente, hecho base acreditado, regla de inferencia y hecho consecuencia. En esta tesis, la trazabilidad funciona como soporte para organizar hechos base, pero la conclusión personal requiere una inferencia adicional y controlable.

Tabla 4
Estructura del razonamiento indiciario aplicada a la trazabilidad

Elemento	Ejemplo correcto	Salto que debe evitarse
Fuente	Reporte bancario con operación y anexos.	"El banco acredita al autor".
Hecho base	La cuenta X recibió y retiró el dinero en dos horas.	Confundir recepción con ejecución del fraude.
Inferencia	La proximidad, coordinación y control corroborado revelan aporte consciente.	Usar "por máxima de experiencia" sin explicar la regla.
Hecho indicado	La persona facilitó y controló la ruta de disposición.	Atribuir todos los actos del grupo.

Nota. Elaboración propia.

2.2.19. Contraindicios e hipótesis alternativas

Los contraindicios son hechos que debilitan o contradicen la hipótesis de cargo. En fraude informático pueden ser denuncia previa por pérdida del equipo, bloqueo de la cuenta, geolocalización incompatible, ausencia de control, suplantación acreditada o transferencias realizadas bajo engaño. El principio de objetividad exige incorporarlos y explicar su alcance.

La hipótesis fiscal no debe probar la imposibilidad absoluta de toda alternativa, pero sí confrontar las plausibles y apoyadas por información. La inferencia gana fuerza cuando explica mejor el conjunto que las hipótesis de error, negligencia, cesión inocente, apropiación por tercero o manipulación de identidad.

2.2.20. Motivación probatoria e inferencial del requerimiento acusatorio

La motivación probatoria explica qué aporta cada elemento de convicción. La motivación inferencial explica por qué los hechos acreditados permiten atribuir el delito y la forma de intervención. Un requerimiento puede contener cientos de páginas de

reportes y, aun así, presentar una inferencia débil si no distingue titularidad, control, ejecución y conocimiento.

El artículo 349 del Código Procesal Penal exige una relación clara y precisa del hecho, sus circunstancias y los elementos que fundamentan la acusación. Aplicado al fraude informático, ello demanda una narración cronológica y funcional, además de una matriz que vincule proposiciones fácticas con fuentes digitales y financieras.

2.2.21. Debido proceso, defensa y protección de datos

La investigación tecnológica puede afectar intimidad, secreto de comunicaciones y secreto bancario. El debido proceso exige legalidad, necesidad, proporcionalidad y control de las medidas, además de posibilidad de contradicción. La eficacia no legitima accesos informales ni recolecciones sin trazabilidad.

La defensa debe poder conocer el origen del registro, el método de extracción, las herramientas utilizadas y las limitaciones de interpretación. Cuando la fiscalía solo presenta capturas o transcripciones sin fuente verificable, disminuye la posibilidad de contradicción y aumenta el riesgo de descontextualización.

2.2.22. Cooperación interinstitucional e internacional

Bancos, operadores y proveedores conservan piezas distintas de la cadena. La respuesta tardía puede ocasionar pérdida de datos o imposibilidad de asignar una IP. El Convenio de Budapest promueve conservación expedita, producción de datos y cooperación transfronteriza. Su utilidad práctica depende de solicitudes claras, puntos de contacto activos y capacidad técnica para interpretar lo recibido.

La cooperación no exime al fiscal de controlar la pertinencia. Un reporte extranjero o privado debe incorporarse con información sobre origen, alcance, fecha, zona horaria y método de certificación. La interoperabilidad jurídica es tan importante como la técnica.

2.3. Marco normativo

2.3.1. Constitución Política del Perú

La Constitución reconoce la intimidad, el secreto e inviolabilidad de las comunicaciones y el secreto bancario, sujetos a los procedimientos constitucionalmente habilitados. Asimismo, el artículo 139 contiene garantías del debido proceso y la motivación; y el artículo 159 atribuye al Ministerio Público la conducción de la investigación del delito. Estas normas establecen una doble exigencia: investigar eficazmente y respetar los límites de obtención y uso de información personal.

2.3.2. Ley N.º 30096 y Ley N.º 30171

La Ley N.º 30096, Ley de Delitos Informáticos, organiza los tipos penales relacionados con datos, sistemas y otras conductas informáticas. La Ley N.º 30171 modificó diversos artículos para adecuarlos al Convenio de Budapest y precisar elementos típicos. El artículo 8 regula el fraude informático. Para el análisis documental debe identificarse la redacción vigente en la fecha del hecho, así como las agravantes que hayan sido expresamente imputadas.

2.3.3. Código Procesal Penal

El Código Procesal Penal regula la actividad probatoria, las medidas limitativas, la obtención de información protegida, la cadena de custodia y el contenido del requerimiento acusatorio. Son especialmente relevantes el artículo 158.3, sobre prueba indiciaria, y el artículo 349, sobre contenido de la acusación. Las disposiciones sobre comunicaciones e información bancaria deben aplicarse de acuerdo con la medida concreta y el control judicial requerido.

2.3.4. Convenio sobre la Ciberdelincuencia

El Convenio de Budapest proporciona categorías sustantivas, herramientas procesales para preservar y obtener datos y mecanismos de cooperación internacional. Para la trazabilidad son relevantes la conservación expedita de datos almacenados, la entrega de información, el registro y decomiso de datos y la cooperación. Estas herramientas responden a la volatilidad y deslocalización propias de la evidencia digital.

2.3.5. Protección de datos personales y protocolos técnicos

La Ley N.º 29733 y su normativa reglamentaria protegen datos personales y establecen principios de tratamiento. En investigación penal, la habilitación legal no elimina los deberes de seguridad, finalidad y proporcionalidad. Asimismo, los manuales y protocolos de evidencia digital orientan identificación, fijación, recojo, embalaje, extracción y conservación; su observancia contribuye a la fiabilidad, aunque su incumplimiento debe evaluarse según la afectación concreta y no mediante nulidades automáticas.

2.4. Marco jurisprudencial

2.4.1. Prueba indiciaria y deber de exteriorización

La sentencia del Tribunal Constitucional recaída en el Exp. N.º 00728-2008-PHC/TC, caso Llamoja Hilares, estableció que no basta invocar lógica o máximas de experiencia: el razonamiento debe exteriorizarse. Este criterio es aplicable al análisis de trazabilidad porque obliga a explicar por qué un registro conduce a un hecho base y por qué varios hechos permiten atribuir participación.

La jurisprudencia constitucional posterior ha reiterado que la prueba indiciaria exige hechos base acreditados y una inferencia expresamente controlable. En consecuencia, expresiones como “la IP acredita”, “la cuenta pertenece” o “el reporte demuestra” son insuficientes si no se expone el alcance del identificador, la corroboración y la regla inferencial.

2.4.2. Imputación y motivación de la acusación

La doctrina jurisprudencial sobre imputación necesaria exige una descripción suficientemente concreta para permitir defensa. En investigaciones complejas puede existir progresividad, pero al acusar la hipótesis debe estar consolidada. La narración debe separar hechos comunes y aportes individuales, precisar circunstancias y relacionar elementos de convicción pertinentes.

2.4.3. Valoración de evidencia digital

No existe una regla que otorgue valor automático a capturas, reportes o pericias. Su fuerza depende de autenticidad, integridad, método, corroboración y contradicción. La jurisprudencia general sobre prueba documental, pericial e indiciaria proporciona los criterios de valoración aplicables. La tesis, por ello, examina si los requerimientos justifican la fiabilidad y no únicamente si mencionan el documento.

2.5. Marco conceptual

Este apartado precisa el sentido con el que se emplean en la investigación los términos centrales. Las definiciones operativas propias de la tesis remiten a lo desarrollado en las bases teóricas; las demás se toman de las fuentes normativas y doctrinales indicadas.

Cadena de custodia: registro que documenta quién obtuvo, recibió, trasladó, examinó y almacenó la evidencia, y que permite controlar su continuidad. Respecto de la evidencia digital, Gonzáles Obando (2021) señala que esta «debe ser recabada con el procedimiento debido a través de la cadena de custodia» (p. 168).

Contraindicio: hecho que debilita o contradice la hipótesis de cargo, como la denuncia previa por pérdida del equipo, la suplantación acreditada o la ausencia de control sobre la cuenta; el principio de objetividad exige incorporarlo y explicar su alcance.

Control efectivo: poder material de acceso y disposición sobre una cuenta, línea o dispositivo, que puede no coincidir con su titularidad registral; se acredita mediante hechos como la posesión de tarjetas o claves, los retiros, las comunicaciones o el aprovechamiento de los fondos.

Datos informáticos: «cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función» (Consejo de Europa, 2001, art. 1).

Datos sobre el tráfico: datos informáticos relativos a una comunicación realizada por medio de un sistema informático, generados como elemento de la cadena de comunicación, «que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente» (Consejo de Europa, 2001, art. 1).

Dirección IP: identificador de una conexión o punto de salida en un momento determinado; no individualiza por sí misma a la persona que operó el dispositivo, pues puede ser dinámica, compartida o encubierta.

Evidencia digital: «cualquier información probatoria almacenada o transmitida en forma digital» (Gonzáles Obando, 2021, p. 168). Por su volatilidad, «se tiene que garantizar su inmutabilidad» (p. 170).

Fraude informático: delito previsto en el artículo 8 de la Ley N.º 30096, que sanciona la obtención de un provecho ilícito en perjuicio de tercero mediante formas de intervención sobre datos o sistemas informáticos. En la doctrina, Mayer Lux y Oliver Calderón (2020) lo describen como «la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos» (p. 156) y lo distinguen de la estafa porque no opera mediante el engaño de una persona.

Imputación necesaria: exigencia de describir de forma concreta qué hizo cada acusado, cuándo, dónde, cómo y con qué forma de intervención, de modo que pueda ejercer su defensa.

Phishing: técnica que utiliza comunicaciones o sitios que aparentan pertenecer a una entidad confiable para captar credenciales; sus variantes por mensajes de texto y por llamadas se denominan *smishing* y *vishing*. No constituye un tipo penal autónomo y, según Mayer Lux y Oliver Calderón (2020), suele corresponder a actos preparatorios del fraude informático.

Proveedor de servicios: toda entidad pública o privada que brinde a los usuarios la posibilidad de comunicarse por medio de un sistema informático, o que procese o almacene datos informáticos para dicho servicio o sus usuarios (Consejo de Europa, 2001, art. 1).

Prueba indiciaria: razonamiento que, a partir de hechos base probados, permite inferir un hecho consecuencia conforme a la lógica, la ciencia o las máximas de experiencia; cuando los indicios son contingentes, deben ser plurales, concordantes y convergentes (Perú, 2004, art. 158.3).

Requerimiento acusatorio: acto mediante el cual el fiscal formula acusación; debe contener, entre otros componentes, una relación clara y precisa del hecho atribuido, los elementos de convicción que la fundamentan y la participación que se imputa (Perú, 2004, art. 349).

Sistema informático: «todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa» (Consejo de Europa, 2001, art. 1).

Titularidad registral: condición de la persona a cuyo nombre figura una cuenta, línea o dispositivo según los registros de la entidad; constituye un punto de partida de la investigación, pero no acredita por sí sola control efectivo, conocimiento ni autoría.

Trazabilidad digital: proceso fiscal de identificar, ordenar, verificar y relacionar registros electrónicos que permiten reconstruir el origen, recorrido, transformación y destino de una actuación digital relevante.

Trazabilidad financiera: reconstrucción documentada del origen, canal, secuencia, destino y disposición final de los fondos relacionados con el hecho investigado.

CAPÍTULO III: CATEGORÍAS DE INVESTIGACIÓN

La investigación se desarrolló bajo un enfoque cualitativo, de tipo básico, alcance descriptivo-interpretativo y diseño de estudio de caso documental. Su propósito fue analizar el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019–2025. En correspondencia con este propósito, el análisis se organizó mediante una categoría principal y tres subcategorías vinculadas con los objetivos específicos.

3.1. Categorías de análisis

No se definieron variables independientes y dependientes, ni se asignaron escalas de medición, puntuaciones o coeficientes de correlación. La información se organizó en categorías de análisis que permitieron interpretar el contenido documental y los criterios de los participantes. Los indicadores se entendieron como referentes de lectura y codificación, no como medidas numéricas del fenómeno.

3.1.1. Categoría principal

Tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación.

Esta categoría comprendió los criterios y actuaciones fiscales dirigidos a obtener, incorporar, organizar, relacionar y valorar información digital y financiera para fundamentar la atribución de una conducta concreta en el requerimiento acusatorio. Su análisis abarcó tanto la identificación de las fuentes como la explicación de los hechos que estas sustentaron, sus limitaciones y el razonamiento utilizado para determinar la forma de intervención atribuida.

La presencia de documentos bancarios o registros electrónicos no se consideró, por sí sola, equivalente a una imputación suficientemente fundamentada. Se examinó la relación entre fuente, dato obtenido, hecho sustentado, conducta individualizada e inferencia fiscal, con atención a la información favorable y desfavorable a la atribución.

3.1.2. Subcategoría de tratamiento fiscal de la trazabilidad digital

Comprendió la reconstrucción de los eventos asociados con dispositivos, servicios de telecomunicaciones, plataformas y sistemas informáticos vinculados con el hecho investigado. Se examinó qué información fue obtenida, cómo se documentó su procedencia y conservación, qué operación permitió reconstruir y con qué alcance vinculó al acusado con el uso o la manipulación del sistema.

Los referentes de análisis incluyeron direcciones IP, registros de acceso y autenticación, dispositivos, líneas telefónicas, tarjetas SIM, IMEI, comunicaciones electrónicas, páginas falsas o clonadas, capturas de pantalla, informes técnicos y pericias. Estos referentes se examinaron según su pertinencia en cada caso; no se exigió su presencia conjunta en todos los requerimientos.

También se consideraron la autenticidad, integridad y conservación de la información, así como las limitaciones para identificar al usuario efectivo. Se distinguió la identificación de una conexión, línea o dispositivo de la atribución personal de la operación, atendiendo a las corroboraciones y explicaciones desarrolladas por el fiscal.

3.1.3. Subcategoría de tratamiento fiscal de la trazabilidad financiera

Comprendió la reconstrucción del desplazamiento de los fondos desde la operación cuestionada hasta su recepción, retiro, transferencia posterior o destino identificable. Se examinó el uso fiscal de informes bancarios, estados de cuenta y registros transaccionales para establecer la secuencia de movimientos y su relación con las personas involucradas.

Los referentes de análisis fueron la cuenta de origen y las cuentas receptoras, titularidad, fecha, hora, monto, canal de operación, retiros, transferencias sucesivas y destino del dinero. Las billeteras digitales y la conversión en criptomonedas se consideraron únicamente cuando resultaron pertinentes y estuvieron documentadas en el material analizado.

El examen diferenció la titularidad formal de la cuenta del control efectivo y de los actos de disposición de fondos. Se atendió a la información que permitió establecer

acceso, retiro, transferencia, aprovechamiento o beneficio, y a las limitaciones del seguimiento para identificar al destinatario final.

3.1.4. Subcategoría de articulación probatoria para sustentar la imputación

Comprendió el razonamiento mediante el cual el fiscal relacionó los datos digitales y financieros para atribuir una conducta y una forma de intervención a cada acusado. Se examinó la correspondencia temporal y funcional entre accesos, comunicaciones, transferencias, recepción y disposición del dinero, así como el aporte de cada fuente a la reconstrucción de los hechos.

Los referentes fueron la individualización de la conducta, las circunstancias de tiempo, modo y lugar, el control efectivo de los recursos utilizados, la inferencia sobre conocimiento y voluntad y la determinación de autoría o participación. Se examinó si el requerimiento explicó el tránsito entre los elementos de convicción y la conclusión atributiva, evitando equiparar automáticamente recepción del dinero con intervención consciente.

Asimismo, se analizó el tratamiento de los contraindicios y de las explicaciones alternativas plausibles presentes en las fuentes, como suplantación, pérdida de medios de acceso o utilización por terceros. El análisis valoró la explicación fiscal de estas circunstancias y su incidencia en la coherencia de la imputación, sin convertir la acusación en una declaración judicial de responsabilidad.

3.1.4.1. Definición operacional de la categoría

La categoría principal se examinó mediante el análisis de doce requerimientos acusatorios, codificados de RA-01 a RA-12, y las entrevistas semiestructuradas a ocho participantes: tres fiscales provinciales, tres fiscales adjuntos provinciales y dos asistentes en función fiscal. Los requerimientos constituyeron las unidades de análisis documental; las entrevistas aportaron criterios y explicaciones sobre el tratamiento de las fuentes y la construcción de la imputación.

La ficha de análisis documental permitió registrar las fuentes citadas, los datos relevantes, los hechos sustentados, las conexiones digitales y financieras y el

razonamiento de atribución. La guía de entrevista permitió examinar los criterios utilizados, las dificultades advertidas y las explicaciones sobre individualización y motivación. La información se organizó conforme a las tres subcategorías y se comparó entre fuentes.

El registro distinguió información expresamente desarrollada, aspectos mencionados sin explicación suficiente, elementos no identificados y referentes no aplicables al caso. La ausencia de un dato no se interpretó automáticamente como deficiencia: se examinó su pertinencia para el hecho atribuido y la disponibilidad que pudo identificarse en las fuentes. Lo no explicitado en el requerimiento no se presentó como inexistente en toda la carpeta fiscal.

3.2. Matriz de categorización

La matriz sintetiza la correspondencia entre los objetivos específicos, las subcategorías y los referentes utilizados para organizar el análisis. La categoría principal común es el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación.

Tabla 5
Matriz de categorización

Objetivo específico	Subcategoría	Referentes de análisis
Examinar el tratamiento de la trazabilidad digital para identificar y vincular al acusado con la manipulación del sistema informático.	Tratamiento fiscal de la trazabilidad digital.	Fuentes e identificadores; acceso y autenticación; comunicaciones; informes y pericias; autenticidad e integridad; conservación; usuario efectivo y límites atributivos.
Analizar el tratamiento de la trazabilidad financiera para reconstruir el desplazamiento y destino del dinero.	Tratamiento fiscal de la trazabilidad financiera.	Origen y recepción de fondos; titularidad; fecha, hora, monto y canal; retiros y transferencias posteriores; control efectivo; destino y beneficiario identificable.
Determinar cómo se articulan ambas trazabilidades para sustentar la imputación	Articulación probatoria para sustentar la imputación.	Correspondencia temporal y funcional; conducta individual; control y disposición; conocimiento y voluntad;

Objetivo específico	Subcategoría	Referentes de análisis
y diferenciar titularidad de autoría o participación.		forma de intervención; regla inferencial; contraindicios; alternativas y motivación.

Nota. Elaboración a partir de los problemas, objetivos y estructura metodológica del documento base.

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1. Enfoque de la investigación

La investigación se desarrolló bajo un enfoque cualitativo, debido a que estuvo orientada a comprender e interpretar el tratamiento fiscal de la trazabilidad digital y financiera utilizado para sustentar la imputación en los requerimientos acusatorios por fraude informático.

El estudio no buscó medir estadísticamente la frecuencia o efectividad general de las investigaciones fiscales, sino examinar la estructura, contenido y fundamentación del razonamiento exteriorizado en los requerimientos acusatorios. Asimismo, permitió conocer los criterios profesionales de fiscales y asistentes en función fiscal con experiencia en investigaciones por fraude informático.

El enfoque cualitativo resultó adecuado porque las categorías analizadas —trazabilidad digital, trazabilidad financiera y articulación probatoria— requerían identificar significados, criterios, relaciones, inferencias y formas de atribución individual que no podían ser comprendidas únicamente mediante datos numéricos.

4.2. Tipo de investigación

La investigación fue de tipo básico, porque tuvo como finalidad ampliar y sistematizar el conocimiento jurídico sobre el tratamiento fiscal de la trazabilidad digital y financiera en los requerimientos acusatorios por fraude informático.

El estudio no estuvo dirigido a implementar o evaluar experimentalmente una herramienta institucional. Sin embargo, sus resultados permitieron formular una propuesta práctica consistente en una matriz integrada para relacionar las fuentes digitales y financieras con los hechos acreditados, las inferencias y la forma de intervención atribuida.

También presentó una orientación jurídico-empírica, debido a que el análisis dogmático y normativo se complementó con el examen de requerimientos acusatorios y entrevistas a operadores fiscales. De esta manera, se contrastaron las exigencias jurídicas de la imputación con su aplicación en documentos concretos.

4.3. Nivel o alcance de la investigación

El alcance fue descriptivo-interpretativo.

Fue descriptivo porque permitió identificar cómo fueron incorporadas y desarrolladas las fuentes de trazabilidad digital y financiera en los requerimientos acusatorios. Se examinaron datos como direcciones IP, dispositivos, líneas telefónicas, tarjetas SIM, códigos IMEI, comunicaciones, registros de acceso, estados de cuenta, cuentas receptoras, retiros y transferencias posteriores.

Fue interpretativo porque no se limitó a constatar la existencia de dichos elementos. También analizó el significado probatorio que los fiscales les atribuyeron, las inferencias formuladas para vincularlos con el acusado y la forma en que se diferenciaron la titularidad registral, el control efectivo y la participación dolosa.

El estudio permitió interpretar la relación existente entre las rutas digital y financiera, así como determinar si su articulación sustentó una imputación individualizada o si permanecieron vacíos entre la descripción de la evidencia y la conclusión fiscal.

4.4. Diseño de la investigación

La investigación empleó un diseño de estudio de caso cualitativo sustentado en análisis documental y entrevistas semiestructuradas. El caso se delimitó por el ámbito institucional, el objeto de estudio y el periodo analizado, mientras que cada requerimiento constituyó una unidad de análisis documental.

El estudio de caso permitió examinar de manera contextualizada la práctica fiscal exteriorizada en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019–2025.

El diseño fue documental porque una de las principales fuentes de información estuvo constituida por doce requerimientos acusatorios. Estos documentos permitieron examinar directamente el razonamiento fiscal, la imputación, las fuentes digitales y financieras y la articulación probatoria.

Fue no experimental porque las categorías no fueron manipuladas. Los documentos fueron analizados tal como fueron formulados y las experiencias de los participantes fueron recogidas mediante entrevistas, sin intervenir en el desarrollo de las investigaciones fiscales.

El estudio tuvo una orientación retrospectiva, dado que examinó documentos correspondientes al periodo 2019–2025. El intervalo documental no se confundió con las fechas de recolección de entrevistas ni implicó un seguimiento longitudinal de los procesos.

4.5. Método de investigación

4.5.1. Método inductivo

El método inductivo permitió partir del contenido particular de los doce requerimientos acusatorios y de las respuestas proporcionadas por los ocho participantes para identificar patrones comunes sobre trazabilidad digital, trazabilidad financiera e imputación.

A partir de los datos se construyeron interpretaciones generales relacionadas con el predominio de la ruta financiera, el desarrollo heterogéneo de la evidencia digital, la diferencia entre titularidad y control efectivo y la motivación inferencial.

4.5.2. Método analítico-sintético

El método analítico permitió descomponer el tratamiento fiscal en sus principales componentes: fuente de información, dato obtenido, autenticidad, integridad, hecho acreditado, relación temporal, movimiento financiero, conducta individual, inferencia y conclusión.

El método sintético permitió integrar dichos componentes para determinar cómo las rutas digital y financiera fueron relacionadas para sustentar la imputación por fraude informático.

4.5.3. Método hermenéutico-jurídico

El método hermenéutico-jurídico fue utilizado para interpretar la Ley N.º 30096, el Código Procesal Penal, las garantías constitucionales, el Convenio de Budapest y los

criterios jurisprudenciales relacionados con la prueba indiciaria, la motivación y la imputación necesaria.

Este método permitió contrastar las exigencias normativas con el contenido efectivamente exteriorizado en los requerimientos acusatorios.

4.5.4. Método de estudio de caso

El método de estudio de caso permitió analizar de manera contextualizada el tratamiento fiscal desarrollado en el Distrito Fiscal de Ayacucho. La unidad institucional fue examinada mediante dos fuentes: documentos fiscales y entrevistas a operadores con experiencia directa.

4.6. Escenario de estudio

El escenario institucional estuvo constituido por el Distrito Fiscal de Ayacucho. El estudio se concentró en requerimientos acusatorios por fraude informático formulados durante el periodo 2019-2025 y en operadores fiscales con experiencia en la investigación, elaboración, revisión o tramitación de estos casos.

El análisis no comprendió todos los delitos informáticos, sino específicamente requerimientos en los que se atribuyó fraude informático y se utilizaron elementos relacionados con operaciones digitales o financieras.

4.7. Población, muestra y unidades de análisis

4.7.1. Población

El universo de interés estuvo constituido por los requerimientos acusatorios por fraude informático formulados en el Distrito Fiscal de Ayacucho durante el periodo 2019–2025. La investigación trabajó con el corpus accesible que cumplió los criterios de selección. No se estableció un tamaño total verificable del universo institucional ni se atribuyó representatividad estadística a la muestra.

4.7.2. Muestra

La muestra estuvo conformada por doce requerimientos acusatorios por fraude informático. La selección fue no probabilística, intencional y basada en criterios.

Los documentos fueron codificados como RA-01, RA-02, RA-03, RA-04, RA-05, RA-06, RA-07, RA-08, RA-09, RA-10, RA-11 y RA-12. La codificación permitió proteger la identidad de las personas involucradas y concentrar el análisis en el razonamiento fiscal.

Se analizaron íntegramente los doce documentos que integraron el corpus seleccionado. Esta revisión completa del corpus no equivalió a un censo de todos los requerimientos emitidos en el Distrito Fiscal durante el periodo, pues la selección estuvo condicionada por el acceso documental y los criterios temáticos.

4.7.3. U nidades de análisis

La unidad documental estuvo constituida por cada requerimiento acusatorio seleccionado, correspondiente a las investigaciones por el delito de fraude informático en el Distrito Fiscal de Ayacucho, durante el periodo 2019-2025.

La unidad de análisis documental fue la argumentación jurídico-probatoria utilizada para valorar los elementos de convicción relacionados con la trazabilidad digital y financiera y sustentar la imputación penal. Esta comprendió los segmentos referidos a los hechos indicadores, los elementos de convicción de naturaleza digital y financiera, la identificación del origen y destino de las operaciones económicas, la vinculación de las cuentas bancarias con los sujetos investigados, las inferencias probatorias, la valoración conjunta de los elementos de convicción, los contraindicios, las posibles explicaciones alternativas, la individualización de los presuntos autores o partícipes y la motivación de la atribución de responsabilidad penal.

En las entrevistas, la unidad de análisis estuvo constituida por los segmentos de respuesta de los participantes relacionados con las categorías y subcategorías de la investigación. Cada segmento fue considerado una unidad de significado susceptible de codificación, comparación e interpretación, con la finalidad de identificar las apreciaciones de los participantes sobre la obtención, valoración e integración de la información digital y financiera, así como su utilidad para sustentar la imputación penal en los requerimientos acusatorios por fraude informático.

4.7.4. Criterios de inclusión documental

Los criterios de inclusión fueron: requerimientos acusatorios por fraude informático pertenecientes al Distrito Fiscal de Ayacucho; emisión dentro del periodo 2019–2025; contenido completo y legible; imputación fáctica acompañada de elementos de convicción; e incorporación de información digital, financiera o ambas.

4.7.5. Criterios de exclusión documental

Los criterios de exclusión comprendieron disposiciones de archivo o formalización, requerimientos de sobreseimiento y sentencias judiciales; documentos incompletos, ilegibles o duplicados; requerimientos referidos exclusivamente a delitos distintos del fraude informático; y documentos que no permitieran examinar la fundamentación de la imputación.

4.8. Participantes

4.8.1. Muestra personal

La muestra personal estuvo integrada por ocho participantes:

Tabla 6
Distribución de la muestra personal por función y código

Participantes	Códigos	Cantidad
Fiscales provinciales	FP-01 a FP-03	3
Fiscales adjuntos provinciales	FAP-01 a FAP-03	3
Asistentes en función fiscal	AFF-01 a AFF-02	2
Total		8

Nota. Elaboración propia.

La selección fue no probabilística e intencional. Los participantes fueron elegidos por su experiencia directa en investigaciones por fraude informático y en la elaboración, revisión, sustentación o tramitación de requerimientos acusatorios.

La suficiencia del grupo se examinó en función de la pertinencia de la experiencia y la profundidad de las respuestas. La reiteración temática descrita en el

documento base constituyó un referente de suficiencia interpretativa, sin convertir el número de ocho participantes en un umbral automático de saturación.

4.8.2. Criterios de inclusión de los participantes

Se incluyeron fiscales provinciales, fiscales adjuntos provinciales y asistentes en función fiscal con experiencia en investigaciones por fraude informático o delitos informáticos patrimoniales y participación en la conducción, elaboración, revisión, sustentación o tramitación de acusaciones. También se consideraron la aceptación voluntaria y la autorización para utilizar académicamente sus respuestas de manera anonimizada.

4.8.3. Criterios de exclusión de los participantes

Se excluyeron operadores sin experiencia pertinente, personal dedicado exclusivamente a funciones administrativas, entrevistas no completadas y personas que no autorizaron el uso académico de sus respuestas.

4.9. Técnicas de recolección de información

4.9.1. Análisis documental

El análisis documental permitió registrar las fuentes digitales y financieras, los hechos sustentados, el tratamiento de autenticidad e integridad, la ruta del dinero, la conducta individual, la forma de intervención, las inferencias, los contraindicios y la motivación exteriorizada.

El análisis se concentró en el contenido exteriorizado. No se presumieron razonamientos, diligencias o elementos que no aparecieran en los documentos.

4.9.2. Entrevista semiestructurada

La entrevista semiestructurada permitió recoger los criterios, experiencias y dificultades de los ocho participantes. Esta técnica combinó una guía común de preguntas con la posibilidad de profundizar en las respuestas relevantes.

Las entrevistas abordaron las fuentes necesarias para reconstruir la ruta digital, su fiabilidad y las dificultades para obtenerlas; la información bancaria, la titularidad, el

control efectivo y el destino del dinero; y la correspondencia entre rutas, la individualización, los contraindicios y la motivación fiscal.

4.9.3. Instrumentos de recolección de información

4.9.3.1. Ficha de análisis documental

La ficha se estructuró conforme a la categoría y las tres subcategorías. Registró código, año y modalidad; fuente y dato digital; fuente y movimiento financiero; titularidad y control efectivo; destino; correspondencia temporal y funcional; conducta atribuida; forma de intervención; inferencia; contraindicios; alternativas y conclusión fiscal.

4.9.3.2. Guía de entrevista semiestructurada

La guía estuvo conformada por diez preguntas abiertas vinculadas con los tres objetivos específicos. Las preguntas fueron formuladas en lenguaje claro y permitieron que los participantes explicaran sus criterios y experiencias sin quedar limitados a respuestas afirmativas o negativas.

La profundización se adaptó al rol de cada participante. Los asistentes aportaron información sobre organización y tramitación documental; sus respuestas no se equipararon con la responsabilidad del fiscal en la decisión de acusar o en su fundamentación jurídica.

4.10. Validez de los instrumentos

La revisión de los instrumentos se orientó a evaluar su claridad, pertinencia con los objetivos, correspondencia con las subcategorías, coherencia metodológica y suficiencia para obtener información relevante. Se empleó la validación mediante juicio de expertos.

4.11. Procedimiento de recolección de información

El procedimiento comprendió la delimitación del problema, objetivos y categorías; identificación y selección documental; codificación de RA-01 a RA-12; lectura integral y registro en la ficha; selección de participantes; consentimiento informado y entrevistas; transcripción y codificación de respuestas; comparación entre

documentos y entrevistas; e interpretación de los hallazgos con apoyo en el marco teórico y jurídico.

4.11.1. Procesamiento y análisis de la información

El análisis siguió un procedimiento temático y comparativo.

4.11.2. Organización del corpus

Los requerimientos fueron codificados como RA-01 a RA-12. Los participantes fueron identificados mediante códigos funcionales: FP, FAP y AFF. Se eliminaron nombres, números de cuentas y demás datos que permitieran identificar a las personas involucradas.

Las unidades de significado comprendieron fragmentos del relato fáctico, enumeración y explicación de elementos de convicción, atribución individual y fundamentación fiscal, así como respuestas relevantes de las entrevistas. Cada registro conservó la referencia al código de origen para permitir la revisión del razonamiento interpretativo.

4.11.3. Codificación inicial

La codificación inicial identificó unidades de significado sobre identificación digital, fiabilidad, limitaciones tecnológicas, ruta financiera, control efectivo, destino final, correspondencia temporal, imputación personal, contraindicios y motivación inferencial.

4.12. Triangulación

La triangulación de fuentes se efectuó entre entrevistas y requerimientos acusatorios. Los antecedentes, las bases teóricas, la normativa y la jurisprudencia se utilizaron como referentes para interpretar y discutir los hallazgos; no se equipararon con datos empíricos obtenidos mediante entrevistas o documentos fiscales.

La convergencia entre las fuentes permitió fortalecer la interpretación. Las diferencias no fueron ocultadas, sino utilizadas para identificar la brecha entre los criterios profesionales y su exteriorización documental.

4.13. Rigor científico de la investigación

4.13.1. Credibilidad

La credibilidad se fortaleció mediante el empleo de dos técnicas de recolección de información, el análisis documental y la entrevista semiestructurada, cuya complementariedad permitió contrastar lo exteriorizado en los requerimientos con los criterios de los operadores. Esta estrategia se complementó con tres procedimientos: la selección de participantes con experiencia directa en investigaciones por fraude informático, el uso de testimonios representativos y la triangulación de las entrevistas con los documentos fiscales.

4.13.2. Dependencia

La dependencia se garantizó mediante la descripción del procedimiento, criterios de selección, instrumentos, códigos y etapas de análisis. Esto permite comprender cómo se obtuvieron las conclusiones.

4.13.3. Confirmabilidad

La confirmabilidad se aseguró vinculando las interpretaciones con unidades de significado y fragmentos documentales. Se procuró diferenciar los datos obtenidos de la interpretación realizada por el investigador.

4.13.4. Transferibilidad

La transferibilidad se favoreció mediante la descripción del contexto institucional, la muestra y las características de los documentos. Los resultados no son estadísticamente generalizables, pero pueden ser considerados en fiscalías con características semejantes.

4.13.5. Saturación temática

La reiteración de criterios sobre fuentes digitales, control efectivo, recorrido del dinero, correspondencia temporal, participación e hipótesis alternativas se consideró un indicio de suficiencia temática. Su alcance se circunscribió al corpus y al grupo entrevistado; no se sostuvo que hubieran sido agotadas todas las prácticas fiscales

posibles. La justificación de saturación debe poder vincularse con el registro de códigos y con la secuencia de entrevistas.

4.14. Consideraciones éticas

La investigación observó los principios de confidencialidad, voluntariedad, objetividad, integridad académica y respeto por los derechos de las personas involucradas. Los participantes fueron informados sobre el propósito del estudio, el uso académico de sus respuestas y su derecho a retirarse. Su intervención se formalizó mediante consentimiento informado.

Los requerimientos fueron anonimizados. Se eliminaron nombres, números de documentos, cuentas bancarias, direcciones, teléfonos y demás información sensible. Los códigos RA-01 a RA-12 fueron utilizados únicamente con fines académicos. El estudio no emitió pronunciamiento sobre la culpabilidad de las personas acusadas. El análisis se limitó al razonamiento fiscal exteriorizado y respetó la presunción de inocencia. Asimismo, se respetó la autoría intelectual mediante citas y referencias. Los resultados no fueron alterados para confirmar expectativas previas.

CAPÍTULO V: PRESENTACIÓN DE DATOS

5.1. Presentación del capítulo

El capítulo presenta los resultados sobre el tratamiento fiscal de la trazabilidad digital y financiera en doce requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho, correspondientes al periodo 2019–2025, y ocho entrevistas semiestructuradas. Los hallazgos se organizaron mediante tablas y figuras para facilitar la lectura de la composición de la muestra y de las relaciones identificadas entre las categorías de análisis.

La presentación responde al objetivo general de analizar el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático. Los resultados se organizaron según los tres objetivos específicos: tratamiento de la trazabilidad digital; tratamiento de la trazabilidad financiera; y articulación probatoria de ambas rutas para individualizar la conducta del acusado y diferenciar la titularidad de una cuenta receptora de la autoría o participación.

La exposición distingue los criterios expresados por los participantes, los patrones consignados en el análisis documental y la síntesis entre ambas fuentes. El análisis fue cualitativo: no se asignaron porcentajes a las recurrencias ni se utilizaron pruebas de hipótesis. Las diferencias entre requerimientos se examinaron según la modalidad del hecho y la disponibilidad de información pertinente, sin exigir que todos contuvieran los mismos registros técnicos.

5.2. Caracterización de las fuentes de información

5.2.1. Participantes

La muestra personal estuvo conformada por tres fiscales provinciales, tres fiscales adjuntos provinciales y dos asistentes en función fiscal. Los participantes declararon experiencia directa en la conducción, elaboración, revisión, sustentación o tramitación de investigaciones y requerimientos acusatorios por fraude informático.

Tabla 7

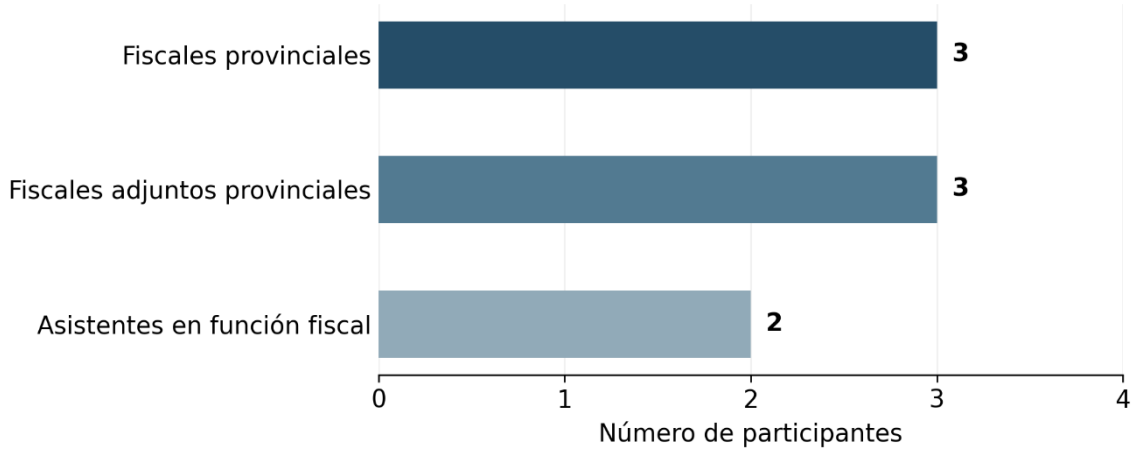
Distribución de los participantes por función

Función	Códigos	Cantidad
Fiscales provinciales	FP-01 a FP-03	3
Fiscales adjuntos provinciales	FAP-01 a FAP-03	3
Asistentes en función fiscal	AFF-01 a AFF-02	2
Total		8

Nota. Elaboración a partir de la sistematización de las entrevistas y del corpus documental. Se conservaron los códigos de identificación.

Los fiscales aportaron criterios sobre la conducción de las investigaciones y la elaboración o sustentación de acusaciones. Los asistentes aportaron información sobre tramitación de solicitudes, seguimiento de respuestas y organización de documentos. Esta diversidad funcional permitió comparar perspectivas, sin atribuir a los asistentes la responsabilidad decisoria de los fiscales.

Figura 1
Composición de la muestra personal por función



Nota. Elaboración a partir de la composición de la muestra personal (n = 8). Las cifras representan participantes, no frecuencias de respuestas.

La figura 1 mostró una participación equivalente de fiscales provinciales y adjuntos, con tres integrantes en cada grupo, y la inclusión de dos asistentes en función fiscal. Esta composición permitió recoger perspectivas relacionadas con las decisiones fiscales y con la tramitación de la información.

5.2.2. Requerimientos acusatorios

La muestra documental estuvo integrada por doce requerimientos acusatorios por fraude informático. Para preservar la confidencialidad, se asignaron códigos siguiendo el orden temporal aproximado del corpus.

Tabla 8
Composición del corpus documental

Código	Rasgo analítico predominante
RA-01	Página clonada, direcciones IP y transferencias
RA-02	Sustitución de SIM, comunicaciones y operaciones bancarias
RA-03	Cuentas receptoras y transferencias sucesivas
RA-04	Operación bancaria e informe técnico digital
RA-05	Transferencia por internet y retiro posterior
RA-06	Cuenta receptora y documentación bancaria
RA-07	Fraude informático asociado con actuaciones de suplantación
RA-08	Operación bancaria y vinculación del receptor
RA-09	Página bancaria falsa, captura de datos y transferencia
RA-10	Suplantación telefónica, comunicaciones y movimientos bancarios
RA-11	Capturas, información de operadoras y transferencia
RA-12	Pluralidad de intervinientes y documentación digital-financiera

Nota. Elaboración a partir de la sistematización de las entrevistas y del corpus documental. Se conservaron los códigos de identificación.

Los documentos contienen diversas modalidades operativas: clonación de páginas bancarias, captación de credenciales, suplantación mediante llamadas, sustitución de tarjetas SIM, transferencias no autorizadas, utilización de cuentas receptoras, retiros por cajeros y desplazamiento posterior del dinero. Esta diversidad hizo posible comparar qué componentes permanecieron constantes y cuáles dependieron de la disponibilidad técnica de cada caso.

5.3. Organización y codificación de los datos

Las respuestas de las entrevistas se organizaron conforme a la guía de diez preguntas y a los tres objetivos específicos. Se agruparon unidades de significado

relacionadas con las fuentes digitales, el recorrido financiero y el razonamiento de imputación, conservando los matices vinculados con la función de cada participante.

Los requerimientos fueron examinados mediante los mismos ejes. En cada documento se revisaron: fuente digital, dato obtenido, autenticidad e integridad, operación financiera, cuenta de origen y destino, secuencia temporal, destino posterior, conducta individualizada, inferencia sobre conocimiento y voluntad, contraindicios e hipótesis alternativas.

Tabla 9
Ejes de codificación utilizados

Eje	Contenido agrupado
Identificación digital	IP, dispositivo, línea, SIM, IMEI, registro y comunicación
Fiabilidad digital	Fuente, acta, cadena de custodia, método y conservación
Limitación tecnológica	Demora, pérdida de datos, IP compartida y proveedor extranjero
Ruta financiera	Origen, destino, fecha, hora, canal, retiro y transferencia posterior
Control efectivo	Posesión, acceso, retiro, disposición y explicación del titular
Destino final	Cuentas sucesivas, cajero, agente, billetera o criptomoneda
Correspondencia	Relación temporal y funcional entre acceso y transferencia
Imputación personal	Tiempo, modo, lugar, conocimiento, voluntad y forma de intervención
Contraindicio	Pérdida, suplantación, préstamo, engaño o acceso por terceros
Motivación inferencial	Fuente, hecho acreditado, inferencia y conclusión fiscal

Nota. Elaboración a partir de la sistematización de las entrevistas y del corpus documental. Se conservaron los códigos de identificación.

La síntesis se concentró en el razonamiento exteriorizado en los requerimientos. La falta de mención de un dato en la acusación no se consideró equivalente a su inexistencia en toda la carpeta fiscal. Tampoco se interpretó la repetición de criterios en las entrevistas como demostración automática de saturación de todas las prácticas institucionales.

5.4. Datos del primer objetivo específico sobre trazabilidad digital

El primer objetivo específico consistió en examinar el tratamiento de la trazabilidad digital para identificar y vincular al acusado con la manipulación del sistema informático.

5.4.1. Criterios expresados en las entrevistas

Los participantes destacaron que la vinculación digital requirió relacionar distintos datos: dirección IP, proveedor, dispositivo, línea telefónica, tarjeta SIM, IMEI, registros de acceso, comunicaciones, páginas falsas e informes técnicos. La identificación de uno de estos recursos no fue equiparada automáticamente con la identificación del usuario que realizó la operación.

En la síntesis atribuida a FP-01 se destacó la relación entre dirección IP, proveedor y registros de acceso; FP-03 resaltó la interpretación técnica de esos datos dentro de la secuencia investigada. Los fiscales adjuntos enfatizaron su organización para elaborar la acusación, mientras que los asistentes describieron la tramitación y sistematización de las respuestas institucionales.

La autenticidad fue relacionada con la identificación de la fuente de obtención. Los participantes distinguieron entre evidencia obtenida mediante incautación, exhibición voluntaria, visualización documentada y respuesta formal de una entidad proveedora.

La integridad fue asociada con las actas, la cadena de custodia y la conservación. FP-02 señaló que las actas deben describir adecuadamente la evidencia y que la cadena de custodia debe permanecer documentada. FAP-02 añadió que el soporte técnico debe permitir verificar que la información no fue alterada entre su obtención y análisis.

La fiabilidad fue vinculada con dos criterios: metodología técnica reconocible y correspondencia con otros elementos. En consecuencia, una captura aislada o un dato proporcionado informalmente no recibió el mismo valor que la información obtenida de la fuente original, documentada y corroborada.

Los participantes señalaron dificultades asociadas con demoras en las respuestas, eliminación de registros, direcciones IP compartidas, líneas a nombre de terceros, falta de incautación oportuna y proveedores extranjeros. Los fiscales adjuntos destacaron el impacto de los periodos de conservación; los asistentes describieron el seguimiento de oficios como una actividad frecuente.

5.4.2. Hallazgos consignados en el análisis documental

Los requerimientos mostraron un tratamiento heterogéneo. En RA-01 se incorporaron datos relativos a direcciones IP y constatación del equipo utilizado por la parte afectada. RA-02 desarrolló información sobre líneas telefónicas, sustitución de SIM, visualización de comunicaciones y dispositivos. RA-04 incluyó un informe técnico de análisis digital que examinó una posible modalidad de suplantación.

En RA-09, la imputación describió la utilización de una página bancaria falsa y la captura de credenciales. RA-10 incorporó comunicaciones y datos relacionados con la suplantación telefónica, mientras RA-11 presentó capturas e información remitida por entidades vinculadas con telecomunicaciones.

En otros requerimientos, la ruta digital apareció formulada principalmente desde la narración de la víctima o desde la afirmación de que existió manipulación del sistema. La identificación técnica del usuario que controló la página, línea, dispositivo o conexión no siempre alcanzó el mismo nivel de desarrollo que la descripción de la operación bancaria.

También se observó que la presencia de evidencia digital no implicó necesariamente una explicación de su autenticidad o metodología. Los documentos más desarrollados identificaron la fuente y el dato relevante; los menos desarrollados incorporaron capturas, comunicaciones o referencias técnicas sin exteriorizar completamente el criterio utilizado para atribuirles fiabilidad.

Tabla 10

Patrones documentales de trazabilidad digital

Aspecto examinado	Patrón descrito
Descripción del mecanismo informático	Presente en el relato de los hechos
Identificación de líneas y comunicaciones	Presente en diversos requerimientos
Direcciones IP y registros técnicos	Desarrollo selectivo según disponibilidad
Vinculación del dispositivo con el usuario	Explicación desigual
Autenticidad e integridad	Generalmente implícitas en actas u oficios
Pericia o interpretación técnica	Presente solo cuando se contó con informe especializado
Cooperación con plataformas extranjeras	Escasa exteriorización

Nota. Elaboración a partir de la sistematización de las entrevistas y del corpus documental. Se conservaron los códigos de identificación.

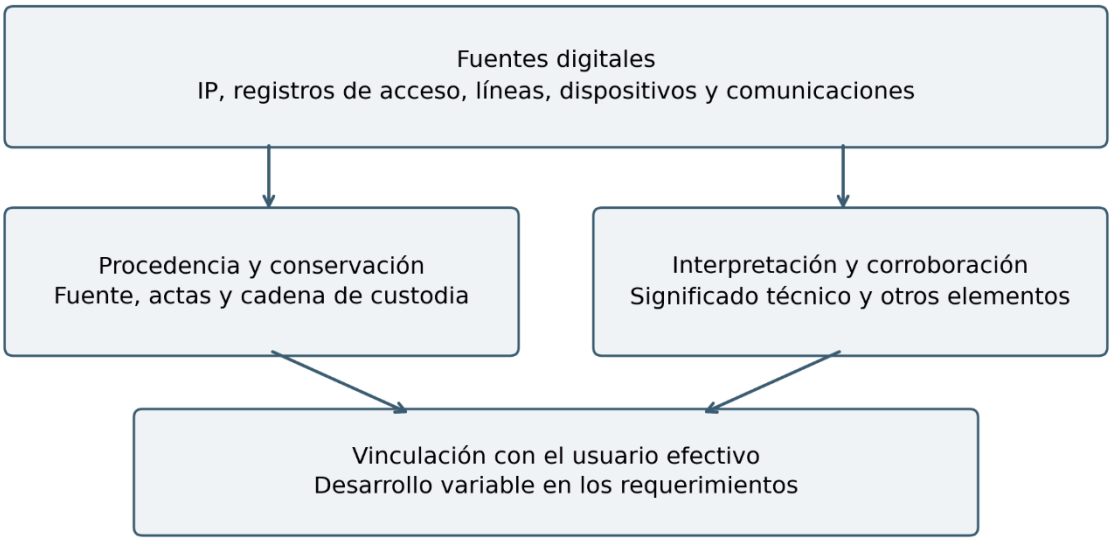
5.4.3. Síntesis del primer objetivo

Las entrevistas describieron un criterio de reconstrucción amplio, mientras que los requerimientos presentaron componentes digitales variables. La ruta digital permitió describir el mecanismo del fraude y, en determinados casos, reforzar la vinculación personal; su capacidad para identificar al usuario efectivo dependió del alcance de las fuentes y de la explicación técnica incorporada.

La diferencia central se ubicó entre identificar un recurso tecnológico y atribuir su utilización a una persona. El análisis reportó mayor desarrollo cuando el requerimiento precisó procedencia del dato, conservación, significado y conexión con la operación financiera. Estas características describieron diferencias del corpus, sin establecer una calificación numérica de cada acusación.

Figura 2

Relaciones identificadas en el tratamiento de la trazabilidad digital



Nota. Síntesis cualitativa de las entrevistas y del análisis documental. Las flechas representan relaciones analíticas; no expresan frecuencias, efectos causales ni una secuencia constatada en todos los casos.

La figura 2 sintetizó la relación entre la identificación de fuentes, su conservación y la interpretación técnica. El hallazgo central fue que la vinculación con el usuario efectivo presentó un desarrollo variable; la identificación de una dirección IP, línea o dispositivo no equivalió automáticamente a la individualización de la conducta.

5.5. Datos del segundo objetivo específico sobre trazabilidad financiera

El segundo objetivo específico fue analizar el tratamiento de la trazabilidad financiera para reconstruir el desplazamiento y destino del dinero.

5.5.1. Criterios expresados en las entrevistas

Los entrevistados coincidieron en la necesidad de obtener los estados de cuenta de la víctima y del receptor, informes de titularidad, fecha y hora, canal utilizado, retiros y transferencias posteriores. La trazabilidad fue entendida como una secuencia y no como la constatación aislada del abono.

La secuencia temporal cumple una función de conexión: permite comparar el momento de acceso no autorizado, la transferencia, el retiro y la dispersión. Según los participantes, la proximidad temporal puede constituir un dato relevante, pero necesita combinarse con control efectivo y disposición del dinero.

Los participantes diferenciaron la titularidad registral del control efectivo. Como datos adicionales señalaron posesión de tarjetas o claves, retiros, comunicaciones, relación con otros intervinientes y beneficio obtenido. La síntesis atribuida a FP-02 destacó la valoración conjunta de estos elementos, mientras que los asistentes explicaron la organización de documentación bancaria y de información complementaria.

Las respuestas también se refirieron a la explicación del titular sobre la operación. Este dato se presentó como parte del criterio declarado por los entrevistados y no como sustituto de los hechos objetivos que debían sustentar la atribución. No se equiparó el silencio del acusado con un indicio autónomo de participación.

Los entrevistados propusieron seguir la totalidad del flujo: cuentas sucesivas, cajeros, ventanillas, agentes, billeteras digitales y criptomonedas. El criterio común fue identificar quién recibió, retiró o dispuso de los fondos en cada etapa.

La conversión en criptomonedas fue mencionada en las entrevistas como un supuesto de seguimiento financiero que requirió conectar la cuenta, plataforma de intercambio y destino. Su inclusión como tema de entrevista no se interpretó como constatación de que esa modalidad estuviera presente en todos los documentos analizados.

5.5.2. Hallazgos consignados en el análisis documental

La trazabilidad financiera fue la dimensión más constante del corpus. Los doce requerimientos identificaron transferencias no autorizadas y utilizaron documentación bancaria para establecer cuentas de origen, cuentas receptoras, montos y fechas. En varios casos también se describieron retiros inmediatos, transferencias posteriores o movimientos realizados mediante cajeros.

RA-01 incorporó estados de cuenta y datos del proveedor sobre las direcciones vinculadas con las transferencias. RA-04 relacionó la transferencia con la cuenta receptora e incorporó información bancaria e informe técnico. RA-05 identificó el abono y el retiro posterior por cajero automático. RA-09 reconstruyó la transferencia hacia la cuenta receptora y la disposición posterior de los fondos. RA-10 incorporó información sobre establecimientos y reportes bancarios, mientras RA-11 organizó capturas, informes y movimientos financieros.

La documentación bancaria presentó generalmente origen institucional identificable. Sin embargo, el alcance de la ruta fue desigual. Algunos requerimientos siguieron el dinero hasta el retiro o transferencia posterior; otros concluyeron la reconstrucción en la primera cuenta receptora.

La titularidad de la cuenta tuvo un papel central en la imputación. En ciertos documentos se complementó con declaración, retiro, comunicación, relación previa o disposición del dinero. En otros, la conexión personal se construyó principalmente desde el ingreso del monto y el beneficio. Este patrón revela que la ruta financiera fue más completa para demostrar el resultado patrimonial que para explicar quién realizó la manipulación informática.

Tabla 11
Patrones documentales de trazabilidad financiera

Aspecto examinado	Patrón descrito
Cuenta de origen y destino	Identificación constante
Fecha, hora y monto	Presencia habitual en informes bancarios
Titularidad de la cuenta receptora	Eje central de vinculación
Canal utilizado	Desarrollo variable
Retiro o transferencia posterior	Presente en varios casos
Destino final del dinero	Seguimiento no uniforme
Billeteras y criptomonedas	Presencia excepcional
Beneficiario real	Individualización desigual

Nota. Elaboración a partir de la sistematización de las entrevistas y del corpus documental. Se conservaron los códigos de identificación.

5.5.3. Síntesis del segundo objetivo

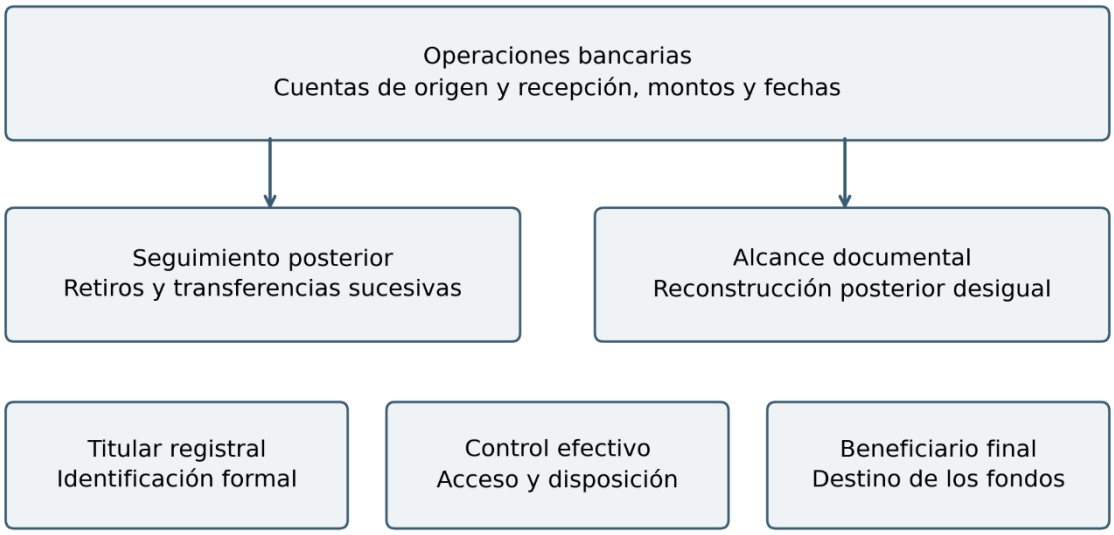
Las entrevistas y los documentos convergieron en considerar los informes bancarios como base de la reconstrucción financiera. La diferencia se presentó en la extensión de la ruta. Los participantes formularon un modelo que sigue el dinero hasta su destino final; los requerimientos mostraron que el rastreo frecuentemente se concentró en la primera cuenta receptora y, cuando fue posible, en el retiro posterior.

El resultado central es que la trazabilidad financiera permitió acreditar con mayor continuidad el perjuicio, el desplazamiento del dinero y la persona registrada como receptora. Su capacidad para demostrar participación consciente aumentó cuando se complementó con control de la cuenta, retiro, disposición, comunicaciones y explicación del titular.

La mayor continuidad documental se observó en la identificación inicial de operaciones, cuentas y titulares. El alcance del seguimiento posterior fue desigual; por ello, la persona registrada en la primera cuenta receptora no se presentó necesariamente como beneficiario final ni como ejecutor de la manipulación informática.

Figura 3

Alcance de la reconstrucción financiera y posiciones diferenciadas



Nota. Síntesis cualitativa del seguimiento financiero. Los recuadros inferiores representan posiciones analíticas distintas y no una sucesión obligatoria de intervinientes.

La figura 3 mostró la mayor continuidad de la documentación de las operaciones iniciales frente al alcance desigual del seguimiento posterior. También permitió distinguir al titular registral, a quien controló la cuenta y al beneficiario final, posiciones que no coincidieron necesariamente.

5.6. Datos del tercer objetivo específico sobre articulación de las rutas

El tercer objetivo consistió en determinar cómo se articulan la trazabilidad digital y financiera para sustentar la imputación y diferenciar la titularidad de una cuenta receptora de la autoría o participación.

5.6.1. Criterios expresados en las entrevistas

Los participantes coincidieron en que la articulación debe comenzar por la correspondencia temporal entre el acceso no autorizado y la transferencia. Luego deben relacionarse el dispositivo, la línea, la cuenta receptora y las actuaciones posteriores.

Los fiscales destacaron la individualización de las circunstancias de tiempo, modo y lugar y la valoración integrada de fuentes. En la síntesis atribuida a FAP-01 se advirtió la necesidad de explicar la conexión entre el relato digital y el movimiento bancario. Los asistentes describieron la utilidad de una cronología para detectar coincidencias, vacíos e incompatibilidades.

Este resultado introduce tres niveles analíticos: identificación registral, control material y participación dolosa. La identificación registral determina a nombre de quién figura la cuenta; el control material establece quién tuvo acceso y dispuso; y la participación dolosa exige inferir conocimiento y voluntad a partir de hechos acreditados.

Los participantes también diferenciaron al ejecutor de la manipulación de quien facilita la cuenta o dispersa el dinero. La forma de intervención debe corresponder a la conducta realmente individualizada y no a la denominación genérica de titular o beneficiario.

Los entrevistados mencionaron como explicaciones alternativas el préstamo de cuenta, la pérdida de tarjeta, la suplantación, el acceso no autorizado, la utilización mediante engaño, el desconocimiento del origen y el uso del dispositivo por terceros.

Las explicaciones alternativas se relacionaron con datos de contraste, como denuncias previas, movimientos, comunicaciones, posesión de medios de acceso y beneficio. Los fiscales adjuntos resaltaron el examen de alternativas plausibles, y los asistentes señalaron la organización de información favorable y desfavorable a la atribución.

Los participantes coincidieron en una estructura mínima: secuencia digital; secuencia financiera; correspondencia temporal y funcional; conducta individual; elementos de convicción; inferencia; forma de participación; y respuesta a contraindicios.

En las entrevistas se distinguió la descripción de la información contenida en una fuente de la explicación de su significado para atribuir conocimiento, voluntad o

intervención. Esta distinción permitió organizar los datos sobre motivación probatoria e inferencial.

5.6.2. Hallazgos consignados en el análisis documental

Los documentos con mayor articulación relacionaron el acceso o engaño digital, la transferencia, la cuenta receptora, el retiro y las comunicaciones dentro de una misma secuencia. RA-02 presentó datos sobre sustitución de SIM, comunicaciones, intervención y operaciones bancarias. RA-01 conectó página clonada, direcciones IP y cuentas beneficiarias. RA-09 vinculó la página falsa, captura de credenciales, transferencia y utilización posterior de los fondos.

En otros requerimientos, la ruta financiera se encontraba detallada, pero la ruta digital permanecía atribuida a terceros no identificados o se describía mediante una fórmula general de manipulación. En esos supuestos, la imputación al titular de la cuenta se sustentó principalmente en recepción, retiro o beneficio. La acusación podía justificar una intervención vinculada con la disposición del dinero, pero no siempre diferenciaba con la misma precisión entre ejecutor de la manipulación, facilitador de cuenta y beneficiario.

La regla de inferencia apareció con desarrollo desigual. Algunos documentos explicaron que la proximidad temporal, el control de la cuenta y el retiro permitían inferir participación consciente. Otros pasaron de la titularidad y recepción a la conclusión sobre autoría sin exteriorizar suficientemente los pasos intermedios.

Los contraindicios y las hipótesis alternativas tuvieron menor desarrollo que los elementos de cargo. Las declaraciones en las que los acusados negaron conocer la transferencia o alegaron uso por terceros fueron incorporadas, pero no siempre se desarrolló una comparación expresa entre ambas hipótesis.

Tabla 12
Patrones documentales de articulación probatoria

Aspecto examinado	Patrón descrito
Cronología de operaciones	Generalmente identificable

Correspondencia digital-financiera	Desarrollo desigual
Individualización de la conducta	Mayor precisión en actos financieros
Diferencia titularidad-autoría	Reconocida, pero no uniforme
Conocimiento y voluntad	Inferencia principalmente contextual
Regla de inferencia	Expresa en algunos casos, implícita en otros
Contraindicios	Incorporación puntual
Hipótesis alternativas	Comparación no sistemática

Nota. Elaboración a partir de la sistematización de las entrevistas y del corpus documental. Se conservaron los códigos de identificación.

5.6.3. Síntesis del tercer objetivo

El contraste mostró coincidencia en el criterio de relacionar las rutas, pero diferencias en su exteriorización documental. La trazabilidad financiera reconstruyó movimientos y receptores formales; la digital aportó datos sobre mecanismo y recursos utilizados. La atribución individual presentó mayor explicación cuando se estableció correspondencia temporal y funcional y se precisó el aporte de cada persona.

La principal diferencia se encontró en la explicación del tránsito desde recepción o titularidad hacia conocimiento, voluntad y forma de intervención. Los contraindicios y las alternativas plausibles tuvieron un desarrollo documental menor que los elementos de cargo. Esta observación se limitó a la motivación escrita y no constituyó un pronunciamiento sobre responsabilidad penal.

5.7. Presentación integrada de las fuentes

Tabla 13
Contraste entre entrevistas y requerimientos

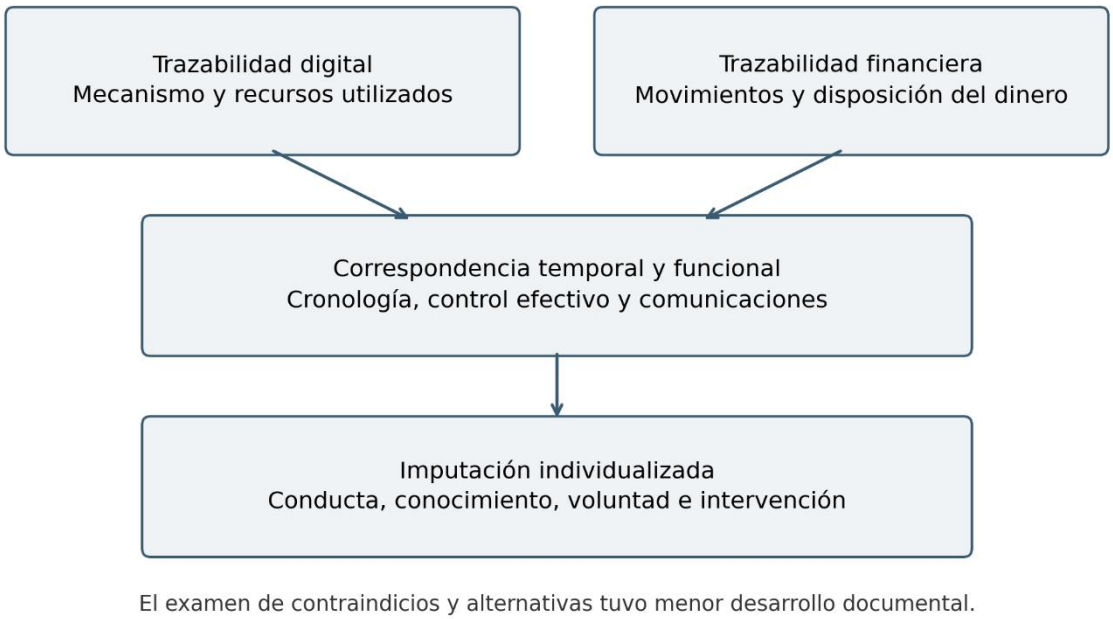
Aspecto	Criterio en entrevistas	Patrón documental
Identificación digital	Modelo amplio de IP, dispositivo, línea y registros	Disponibilidad variable
Autenticidad e integridad	Fuente, acta, cadena y método	Generalmente sustentadas mediante incorporación formal
Ruta financiera	Seguimiento hasta destino final	Fuerte hasta primera cuenta; variable después
Titularidad de cuenta	Insuficiente por sí sola	Eje frecuente de vinculación

Correspondencia	Coincidencia temporal y funcional	Presente con diferente profundidad
Forma de intervención	Debe individualizarse	Diferenciación desigual
Contraindicios	Deben verificarse objetivamente	Tratamiento puntual
Motivación	Fuente, hecho, inferencia y conclusión	Mayor descripción que explicación inferencial

Nota. Elaboración a partir de la sistematización de las entrevistas y del corpus documental. Se conservaron los códigos de identificación.

Las entrevistas y los documentos convergieron en la importancia de las fuentes identificables, el recorrido del dinero y la individualización. La diferencia consistió en la profundidad con que tales criterios se desarrollaron en los requerimientos. El contraste permitió identificar coincidencias y divergencias sin asumir que cada entrevistado hubiera elaborado cada documento del corpus.

Figura 4
Articulación de las rutas para la imputación individualizada



Nota. Síntesis de los hallazgos de articulación. Las flechas muestran conexiones analíticas y no demuestran, por sí mismas, autoría, participación o culpabilidad.

La figura 4 integró el aporte de ambas rutas y situó la correspondencia temporal y funcional como conexión entre los datos y la conducta individualizada. El desarrollo

de esa conexión fue desigual en los requerimientos, especialmente al explicar el conocimiento y la voluntad y al confrontar alternativas plausibles.

CAPÍTULO VI: DISCUSIÓN DE RESULTADOS

6.1. Propósito y alcance de la discusión

La discusión interpretó los resultados presentados sobre doce requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho, correspondientes al periodo 2019–2025, y ocho entrevistas semiestructuradas. Se organizó conforme al objetivo general y los tres objetivos específicos, relacionando los patrones documentales con los criterios profesionales y con los antecedentes y fundamentos jurídicos pertinentes.

El análisis se concentró en la forma en que la información digital y financiera fue utilizada para individualizar conductas. La comparación entre entrevistas y requerimientos permitió distinguir el criterio declarado de su exteriorización escrita. La coincidencia de respuestas no se consideró demostración de una práctica uniforme en todo el Distrito Fiscal, y las observaciones documentales no se extendieron a actuaciones de las carpetas que no estuvieron disponibles.

Los antecedentes se emplearon atendiendo a sus diferencias de objeto y metodología. Los estudios de alcance correlacional y las publicaciones doctrinales permitieron contextualizar los hallazgos, pero no se utilizaron para atribuir resultados estadísticos a esta investigación cualitativa. Las publicaciones posteriores a 2025 se incorporaron como referentes de discusión, sin tratarlas como normas aplicables retrospectivamente a los hechos del corpus.

6.1.1. Discusión del objetivo general

El objetivo general fue analizar el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación. El patrón principal fue una asimetría entre ambas rutas: la información financiera mostró mayor continuidad en la identificación de operaciones, cuentas, titulares, fechas y montos; la digital presentó un desarrollo variable en registros de acceso, direcciones IP, líneas, dispositivos y análisis técnico. Esta diferencia tuvo relevancia porque acreditar el desplazamiento de fondos y explicar

la intervención personal constituyeron tareas relacionadas, pero con exigencias argumentativas distintas.

La interpretación del corpus permitió advertir que la documentación bancaria facilitó reconstruir el resultado patrimonial, mientras que la información digital aportó datos sobre el mecanismo y los recursos utilizados. El ingreso de dinero a una cuenta explicó un tramo del recorrido económico, aunque no resolvió necesariamente quién obtuvo credenciales, controló un dispositivo o ejecutó la operación. Por ello, la integración entre rutas fue relevante para precisar el alcance de la conducta atribuida.

Vinelli Vereau (2021) examinó el fraude informático y la suplantación de identidad en su relación con la criminalidad económica. Su aporte doctrinal proporcionó un marco para interpretar conjuntamente la dimensión tecnológica y patrimonial. La investigación de Ayacucho añadió una precisión contextual: la identificación del receptor de fondos pudo estar más desarrollada que la vinculación del acusado con la operación informática. Esta precisión surgió del corpus analizado y no se presentó como un resultado empírico del artículo citado.

El aporte general consistió en ubicar la calidad de la imputación en la relación entre fuente, hecho sustentado e inferencia individual. La cantidad de documentos incorporados no permitió, por sí sola, evaluar esa calidad. La fundamentación adquirió mayor claridad cuando explicó qué aportó cada elemento, cómo se relacionó con los demás y qué conducta concreta se atribuyó a cada persona.

6.1.2. Discusión del primer objetivo específico sobre trazabilidad digital

El primer objetivo específico consistió en examinar el tratamiento de la trazabilidad digital para identificar y vincular al acusado con la manipulación del sistema informático. Las entrevistas describieron la necesidad de combinar identificadores y registros; los requerimientos mostraron una incorporación desigual de esos componentes. RA-01, RA-02 y RA-04 aportaron ejemplos de direcciones IP, información de telecomunicaciones o análisis técnico, mientras que RA-09, RA-10 y RA-11

describieron páginas falsas, comunicaciones o capturas. Estos ejemplos no implicaron que todos los documentos tuvieran igual capacidad de individualización.

La diferencia permitió distinguir dos funciones de la ruta digital. Una fue describir la modalidad del hecho; otra, relacionar una actuación con un usuario efectivo. La descripción de una página falsa o de una sustitución de SIM explicó el mecanismo investigado, pero la atribución de su control requirió una conexión adicional con personas, momentos y operaciones. Esta distinción fue central para evitar que la identificación de una modalidad sustituyera la individualización de su ejecución.

Estrada Salvador Ramírez (2024) abordó las dificultades de individualización en delitos informáticos y la necesidad de una respuesta especializada y coordinada. La coincidencia con los hallazgos se situó en la importancia de convertir información dispersa en una vinculación personal sustentada. La diferencia de alcance fue que su trabajo trató la problemática de la impunidad, mientras que esta investigación examinó documentos que ya habían alcanzado la decisión de acusar; por ello, no se dedujo una tasa de impunidad a partir del corpus.

La heterogeneidad documental no se interpretó automáticamente como falta de diligencia fiscal. Pudo estar relacionada con diferencias entre modalidades y con la disponibilidad de fuentes, aunque el diseño no permitió establecer causalmente el peso de cada factor. La observación relevante fue si el requerimiento explicó las limitaciones del dato disponible y evitó atribuirle una capacidad identificadora mayor que la sustentada.

6.1.3. Discusión de la fiabilidad y oportunidad de la información digital

Los resultados distinguieron procedencia, conservación e interpretación de la información. Esta separación permitió comprender que la incorporación formal de un oficio o acta no equivalió necesariamente a una explicación completa del alcance técnico de su contenido. El razonamiento fiscal requirió precisar qué dato fue obtenido, qué evento permitió reconstruir y qué limitaciones tuvo para identificar a una persona.

El Convenio sobre la Ciberdelincuencia contempla la conservación expedita de datos almacenados vulnerables a pérdida o modificación, y somete las facultades procedimentales a condiciones y salvaguardas (Consejo de Europa, 2001, arts. 15–16). Este marco permitió interpretar la preocupación expresada en las entrevistas por la pérdida de registros y las demoras. Su relevancia para el estudio consistió en diferenciar la preservación oportuna de la posterior obtención y valoración de información.

La disponibilidad de datos se entendió como una condición del análisis y no como una explicación causal comprobada del desarrollo desigual de las acusaciones. No se contaron con registros suficientes para comparar tiempos de respuesta, solicitudes frustradas o información eliminada en cada caso. En consecuencia, la discusión vinculó el problema con lo declarado por los participantes y con los límites visibles en el documento, sin cuantificar pérdidas ni atribuir incumplimientos específicos a proveedores.

6.1.4. Discusión del segundo objetivo específico sobre trazabilidad financiera

El segundo objetivo específico fue analizar el tratamiento de la trazabilidad financiera para reconstruir el desplazamiento y destino del dinero. Los datos reportados mostraron mayor continuidad en la identificación de la operación inicial y de la cuenta receptora, pero un seguimiento posterior desigual. La diferencia entre conocer el primer destino y reconstruir la disposición final permitió valorar el alcance real de la documentación bancaria.

RA-05 y RA-09 ilustraron el registro de abonos y actuaciones posteriores de disposición, mientras otros documentos concentraron el seguimiento en la primera cuenta. Estos ejemplos permitieron interpretar que la ruta financiera no tuvo una extensión uniforme. Cuando la reconstrucción terminó en el primer receptor, quedó limitado el conocimiento del beneficiario final; ello no eliminó el valor del abono documentado, pero restringió las conclusiones que podían derivarse de él.

Herrera Figueroa (2026) estudió la relación entre fraude informático y protección del ciudadano en Huánuco mediante diez casos fiscales con requerimiento acusatorio

y diez fiscales, bajo un diseño correlacional. Su resumen institucional relacionó los resultados con deficiencias en la respuesta de operadores. La cercanía con esta investigación radicó en el uso de casos que alcanzaron acusación; la diferencia estuvo en el propósito, pues aquí se interpretó la estructura de la trazabilidad y no se midió la protección ciudadana ni se reprodujeron sus coeficientes.

El aporte del segundo objetivo fue mostrar que la continuidad financiera favoreció la reconstrucción patrimonial, aunque no resolvió de manera automática el conocimiento del receptor ni su aporte al hecho. La discusión diferenció el registro institucional de titularidad, el acceso material a la cuenta y la disposición de los fondos. Estas posiciones debieron explicarse mediante hechos relacionados, especialmente cuando existió intervención de terceros.

6.1.5. Discusión del tercer objetivo específico sobre articulación e imputación

El tercer objetivo fue determinar cómo se articularon las rutas para sustentar la imputación y diferenciar titularidad de autoría o participación. El contraste mostró que los participantes describieron una valoración integrada, mientras los requerimientos desarrollaron esa relación con distinta profundidad. RA-01, RA-02 y RA-09 ofrecieron ejemplos de conexión entre mecanismo digital, transferencia, recepción y actuaciones posteriores, según los hallazgos consignados.

La correspondencia temporal permitió ordenar los eventos, pero su proximidad no se consideró una demostración autosuficiente de coordinación o conocimiento. La correspondencia funcional requirió explicar el papel del recurso tecnológico, la cuenta y los actos atribuidos dentro de una misma secuencia. La lectura integrada adquirió sentido cuando individualizó aportes y evitó que una cronología sustituyera el análisis de intervención.

El artículo 349 del Código Procesal Penal exige motivar la acusación y precisar hechos, elementos de convicción y participación atribuida. El artículo 158.3 establece requisitos para el razonamiento por indicios, entre ellos el sustento del hecho indicador y la racionalidad de la inferencia (Perú, 2004). Para esta discusión, el primero constituyó

el referente directo de contenido acusatorio; el segundo orientó el examen racional de enlaces inferenciales, sin convertir el requerimiento en una sentencia.

Esta distinción impidió trasladar automáticamente a la acusación el estándar de una condena. El estudio examinó la claridad de la pretensión fiscal y su respaldo en elementos de convicción, no la suficiencia definitiva de prueba actuada en juicio. La atribución de ejecución informática o de colaboración financiera requirió una explicación propia del aporte señalado, sin asumir que el receptor fuese necesariamente el ejecutor.

6.2. Aporte de la investigación

La investigación aportó una lectura conjunta de trazabilidad y razonamiento de imputación en el contexto documental seleccionado. Permitió distinguir el recurso digital del usuario, la titularidad del control y la primera recepción del destino final. Estas diferencias ofrecieron un criterio para interpretar acusaciones con división de funciones, sin imponer una lista única de registros a modalidades distintas.

Como implicancia práctica se planteó una matriz integrada que relacione fuente, dato, fecha, hecho sustentado, fiabilidad, limitación, persona vinculada, conducta, inferencia y alternativa relevante. Su finalidad fue facilitar la revisión de coherencia antes de formular la acusación. La propuesta no se implementó ni se evaluó experimentalmente, por lo que no se afirmó que hubiera reducido plazos, mejorado resultados judiciales o incrementado la eficacia institucional.

La matriz tampoco sustituyó la motivación escrita ni convirtió la valoración en una operación automática. Su utilidad propuesta consistió en detectar enlaces insuficientemente explicados y evitar atribuciones superiores al alcance del material. La revisión debió adaptarse a la conducta imputada y a las fuentes razonablemente disponibles en cada caso.

CONCLUSIONES

Primera. En relación con el objetivo general, se concluyó que el tratamiento fiscal de la trazabilidad digital y financiera en los doce requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho, correspondientes al periodo 2019–2025, se desarrolló mediante dos rutas complementarias con distinta continuidad documental. La ruta financiera permitió reconstruir con mayor uniformidad las operaciones, cuentas, montos y fechas; la digital presentó un desarrollo variable en la identificación de los recursos tecnológicos y de sus usuarios efectivos. La utilidad de ambas rutas para sustentar la imputación dependió de la explicación de su correspondencia y de la conducta atribuida a cada acusado. El contraste con las ocho entrevistas mostró coincidencia en los criterios profesionales de integración, aunque estos se exteriorizaron con diferente profundidad en los requerimientos. Este resultado se circunscribió a la muestra y al razonamiento escrito examinado, sin establecer la culpabilidad de las personas acusadas ni la eficacia general de la persecución fiscal.

Segunda. Respecto del primer objetivo específico, se determinó que la trazabilidad digital permitió describir el mecanismo del fraude y, cuando se contó con registros pertinentes y corroborados, reforzar la vinculación de una persona con la operación investigada. Los requerimientos incorporaron de manera heterogénea direcciones IP, líneas telefónicas, tarjetas SIM, dispositivos, comunicaciones, páginas falsas e informes técnicos. La identificación de estos recursos no equivalió automáticamente a la identificación de quien los utilizó. Los participantes destacaron la procedencia, conservación, integridad e interpretación técnica de los datos y señalaron dificultades relacionadas con demoras, pérdida de registros, identificadores compartidos y utilización por terceros. En los documentos, la explicación de la fiabilidad y del alcance atributivo fue desigual. Por ello, la principal limitación identificada fue el tránsito insuficientemente explicitado entre el recurso tecnológico y el usuario efectivo, sin que la ausencia de mención en la acusación demostrara la inexistencia del dato en toda la carpeta fiscal.

Tercera. En relación con el segundo objetivo específico, se estableció que la trazabilidad financiera presentó mayor continuidad para reconstruir el desplazamiento inicial del dinero. La documentación bancaria permitió identificar cuentas de origen y recepción, titulares, fechas y montos, y en determinados casos incorporó retiros o transferencias posteriores. Sin embargo, la extensión del seguimiento fue desigual y no siempre permitió reconstruir el destino final de los fondos. Las entrevistas plantearon un criterio de seguimiento más amplio que el exteriorizado en algunos requerimientos. El hallazgo permitió distinguir la titularidad registral, el control efectivo de la cuenta y la condición de beneficiario final, posiciones que no coincidieron necesariamente en una misma persona. En consecuencia, la recepción de fondos constituyó un dato relevante del recorrido financiero, pero su significado para atribuir una intervención consciente requirió relacionarlo con actos de acceso, disposición, comunicaciones u otros hechos objetivos.

Cuarta. Respecto del tercer objetivo específico, se concluyó que la articulación de las rutas adquirió mayor claridad cuando los requerimientos relacionaron cronológicamente el mecanismo digital, la transferencia, la recepción, el retiro o desplazamiento posterior y los actos atribuidos a cada interviniente. Su desarrollo fue desigual: algunos documentos integraron ambas secuencias, mientras otros concentraron la explicación en la ruta bancaria. La principal dificultad argumentativa se ubicó en el paso desde la titularidad o recepción hacia las inferencias sobre conocimiento, voluntad y forma de intervención. La descripción de las fuentes tuvo mayor desarrollo que la explicación de algunas inferencias, y los contraindicios e hipótesis alternativas recibieron un tratamiento menos explícito que los elementos de cargo. Así, la titularidad no operó como un fundamento autosuficiente de autoría o participación; la individualización dependió del contexto y de la conexión razonada entre los hechos sustentados y la conducta atribuida, conservando la diferencia entre formular una acusación y declarar responsabilidad penal.

RECOMENDACIONES

Primera. A la Presidencia de la Junta de Fiscales Superiores del Distrito Fiscal de Ayacucho y a los responsables de los despachos penales, se recomienda promover una pauta de trabajo para integrar la información digital y financiera antes de formular acusaciones por fraude informático. La pauta debería organizar una matriz por persona investigada con la fuente, el dato relevante, la fecha y hora, el hecho sustentado, la limitación del identificador, la correspondencia con otras fuentes, la conducta atribuida y la inferencia sobre intervención. Se propone evaluar su utilidad mediante una aplicación piloto y revisión interna, sin asumir que su eficacia haya sido demostrada por esta investigación ni convertirla en una lista rígida de documentos exigibles a todas las modalidades.

Segunda. A los fiscales responsables de las investigaciones y a los equipos de apoyo técnico, se recomienda priorizar la preservación y obtención oportuna de registros digitales, conforme a las competencias y autorizaciones aplicables. Las solicitudes deberían precisar el recurso investigado, el intervalo temporal, la zona horaria y el tipo de registro requerido. Asimismo, se recomienda documentar la procedencia, conservación y metodología de análisis y explicar las limitaciones de las direcciones IP, líneas y dispositivos cuando se utilicen para vincular personas. La capacitación práctica de fiscales y asistentes debería concentrarse en distinguir autenticidad e integridad del dato de su capacidad para identificar al usuario efectivo, así como en detectar necesidades de corroboración y de apoyo pericial.

Tercera. A los fiscales encargados del seguimiento financiero, se recomienda ampliar razonablemente la reconstrucción desde la primera cuenta receptora hacia los retiros, transferencias sucesivas y destinos pertinentes para la hipótesis investigada. La decisión de continuar el rastreo debería atender a la relevancia, disponibilidad y viabilidad jurídica de la diligencia. Se recomienda registrar separadamente al titular, a quien controló o dispuso de la cuenta y al beneficiario identificado, y solicitar información complementaria sobre canales, horarios, medios de acceso y operaciones posteriores

cuando resulte necesaria. La coordinación con entidades financieras debería orientarse a obtener respuestas completas y comparables, evitando atribuir la ejecución informática o la participación consciente únicamente por la identificación registral de una cuenta.

Cuarta. A los fiscales encargados de elaborar los requerimientos acusatorios, se recomienda incorporar una explicación expresa de la relación entre las rutas y de las inferencias que sustentan la intervención de cada acusado. Para ello, conviene presentar una cronología integrada, precisar qué elemento respalda cada hecho y justificar la conexión hacia conocimiento, voluntad y forma de participación.

BIBLIOGRAFÍA

Alzate Obando, V., & Aponte Bedoya, S. M. (2025). *Garantías del debido proceso en delitos informáticos, municipio de Pereira durante los años 2020–2021*. Universidad Libre. https://repository.unilibre.edu.co/handle/10901/32757

Carriel Cagua, J. D., Sigcha Chiguano, W. G., Morán Delgado, M. J., Mendoza Segovia, J. A., & Segura Osorio, M. B. (2026). Responsabilidad penal en delitos informáticos desafíos de la persecución penal en entornos digitales. *Sage Sphere Multidisciplinary Studies, 3*(1), 1–22. https://doi.org/10.63688/xbm39w11

Congreso Constituyente Democrático. (1993). *Constitución Política del Perú*. https://www.congreso.gob.pe/constitucionyreglamento/

Congreso de la República del Perú. (2011). *Ley n.º 29733, Ley de Protección de Datos Personales*. https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Congreso de la República del Perú. (2013). *Ley n.º 30096, Ley de Delitos Informáticos*. https://www.leyes.congreso.gob.pe/documentos/leyes/30096.pdf

Congreso de la República del Perú. (2014). *Ley n.º 30171, Ley que modifica la Ley 30096, Ley de Delitos Informáticos*. https://www.leyes.congreso.gob.pe/Documentos/Leyes/Textos/30171.pdf

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia* (ETS n.º 185). https://rm.coe.int/1680081561

Estrada Salvador Ramírez, C. T. (2024). La impunidad en los delitos informáticos. Una problemática de poco interés para legisladores, jueces y fiscales. *Ius Vocatio, 7*(9), 91–115. https://doi.org/10.35292/iusVocatio.v7i9.928

Gonzáles Obando, G. L. (2021). Garantías procesales penales en la evidencia digital. *Revista de Investigación de la Academia de la Magistratura, 3*(5), 165–174. https://doi.org/10.58581/rev.amag.2021.v3n5.09

Herrera Figueroa, G. I. (2026). *La incidencia del delito de fraude informático y la protección efectiva del ciudadano, distrito judicial de Huánuco, 2022–2023* [Tesis de licenciatura, Universidad de Huánuco]. Repositorio Institucional UDH. https://hdl.handle.net/20.500.14257/7004

Ibarra Chango, M. del C., Tanqueño Colcha, O. P., Naranjo Villares, A. E., & Yumbay Yaguachi, C. E. (2026). Sostenibilidad financiera y blockchain: Una perspectiva teórica sobre trazabilidad, ética y responsabilidad contable. *Journal of Science and Research, 11*(XII CTIE y III CIVS). https://doi.org/10.5281/zenodo.20597139

Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología, 9*(1), 151–184. https://doi.org/10.5354/0719-2584.2020.57149

Ministerio del Interior. (2019). *Manual para el recojo de la evidencia digital* (Resolución Ministerial N.º 848-2019-IN). https://www.gob.pe/institucion/mininter/informes-publicaciones/1199631-manual-para-el-recojo-de-la-evidencia-digital

Monroy Sotomayor, T. P. (2026). Evolución de la cibercriminalidad y desafíos del Derecho penal frente a los delitos informáticos. *Polo del Conocimiento, 11*(7), 135–146. https://doi.org/10.23857/pc.v11i7.12012

Perú. (2004). *Decreto Legislativo n.º 957, Código Procesal Penal*. https://spij.minjus.gob.pe/Normas/textos/290704T.pdf

Ramos Mera, J. M. (2026). La funcionalidad informática como objeto de tutela penal: Bases dogmáticas para la comprensión del bien jurídico en los delitos informáticos. *Revista Jurídica Crítica y Derecho, 7*(13), 28–42. https://doi.org/10.29166/cyd.v7i13.10451

Reyes Quezada, D. J., & Palacios Rodas, C. A. (2026). Marco jurídico ecuatoriano versus convenio de Budapest: Análisis comparativo de la recolección de evidencia digital en phishing transfronterizo durante el período 2020–2024. *Ciencia y Educación, 7*(2.2), 117–134. https://doi.org/10.5281/zenodo.18795379

Toscano-Quispe, S. Y., Villalva-Salguero, T. F., Abad-Basantes, C. A., & Sarango-Romero, V. J. (2026). Fallos en la trazabilidad digital de la cadena de suministro y su impacto en el control de calidad. *Journal of Economic and Social Science Research, 6*(2), 45–56. https://doi.org/10.55813/gaea/jessr/v6/n2/239

Tribunal Constitucional del Perú. (2008, 13 de octubre). *Sentencia del Expediente n.º 00728-2008-PHC/TC (Giuliana Flor de María Llamoja Hilares)*. https://www.tc.gob.pe/jurisprudencia/2008/00728-2008-HC.pdf

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 licenciatura, Universidad Privada del Norte]. Repositorio Institucional UPN. https://hdl.handle.net/11537/28942

Villacorta Saldaña, F. (2026). *La disposición de archivo preliminar en el delito informático y la inobservancia de los fines del proceso penal en la segunda fiscalía corporativa de Huánuco, 2022–2023* [Tesis de licenciatura, Universidad de Huánuco]. Repositorio Institucional UDH. https://hdl.handle.net/20.500.14257/7493

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

ANEXOS

ANEXOS

Anexo 1. Matriz de consistencia

Anexo 2. Matriz de categorización y ruta de instrumentos

Anexo 3. Ficha de análisis documental

Anexo 4. Guía de entrevista semiestructurada

Anexo 1

Matriz de consistencia

Problemas	Objetivos	Categoría y subcategorías	Metodología
Problema general ¿Cómo se desarrolla el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025?	**Objetivo general** Analizar el tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025.	**Categoría principal** Tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación.	**Enfoque:** cualitativo. **Tipo:** básica, con orientación jurídico-empírica. **Alcance:** descriptivo-interpretativo. **Diseño:** estudio de caso cualitativo documental; no experimental y retrospectivo. **Métodos:** inductivo, analítico-sintético, hermenéutico-jurídico y estudio de caso. **Escenario:** Distrito Fiscal de Ayacucho, 2019–2025. **Muestra documental:** 12 requerimientos acusatorios por fraude informático (RA-01 a RA-12); no probabilística, intencional y por criterios. **Participantes:** 8 (3 fiscales provinciales, 3 fiscales adjuntos provinciales y 2 asistentes en función fiscal). **Técnicas:** análisis documental y entrevista semiestructurada. **Instrumentos:** ficha de análisis documental y guía de entrevista semiestructurada. **Análisis:** temático y comparativo; codificación y triangulación de fuentes.
Problema específico 1 ¿Cómo se desarrolla la trazabilidad digital para identificar y vincular al acusado con la manipulación del sistema informático en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025?	**Objetivo específico 1** Examinar el tratamiento de la trazabilidad digital para identificar y vincular al acusado con la manipulación del sistema informático en los requerimientos acusatorios por fraude informático.	**Subcategoría 1** Tratamiento fiscal de la trazabilidad digital.	
Problema específico 2 ¿Cómo se desarrolla la trazabilidad financiera para reconstruir el desplazamiento y destino del dinero en los requerimientos acusatorios por fraude informático del Distrito Fiscal de Ayacucho durante el periodo 2019-2025?	**Objetivo específico 2** Analizar el tratamiento de la trazabilidad financiera para reconstruir el desplazamiento y destino del dinero en los requerimientos acusatorios por fraude informático.	**Subcategoría 2** Tratamiento fiscal de la trazabilidad financiera.	
Problema específico 3 ¿Cómo se articulan la trazabilidad digital y financiera para sustentar la imputación y diferenciar la titularidad de una cuenta receptora de la autoría o participación en el fraude informático?	**Objetivo específico 3** Determinar cómo se articulan la trazabilidad digital y financiera para sustentar la imputación y diferenciar la titularidad de una cuenta receptora de la autoría o participación en el fraude informático.	**Subcategoría 3** Articulación probatoria para sustentar la imputación.	

Nota. Elaboración propia. Por tratarse de una investigación cualitativa, no se formularon hipótesis ni variables; el análisis se organizó mediante categorías y subcategorías.

Anexo 2

Matriz de categorización y ruta de instrumentos

Categoría principal: Tratamiento fiscal de la trazabilidad digital y financiera para sustentar la imputación.

Objetivo específico	Subcategoría	Referentes de análisis	Técnica e instrumento (ítems)	Fuente de información
Examinar el tratamiento de la trazabilidad digital para identificar y vincular al acusado con la manipulación del sistema informático.	**Tratamiento fiscal de la trazabilidad digital**	• Fuentes e identificadores (IP, líneas, SIM, IMEI, dispositivos) • Registros de acceso y autenticación • Comunicaciones, páginas falsas y capturas • Informes técnicos y pericias • Autenticidad, integridad y conservación • Usuario efectivo y límites atributivos	**Ficha de análisis documental:** secciones B y E **Guía de entrevista:** preguntas 1 a 4	RA-01 a RA-12; FP, FAP y AFF
Analizar el tratamiento de la trazabilidad financiera para reconstruir el desplazamiento y destino del dinero.	**Tratamiento fiscal de la trazabilidad financiera**	• Origen y recepción de fondos • Titularidad de las cuentas • Fecha, hora, monto y canal • Retiros y transferencias posteriores • Control efectivo de la cuenta • Destino y beneficiario identificable	**Ficha de análisis documental:** secciones C y E **Guía de entrevista:** preguntas 5 a 7	RA-01 a RA-12; FP, FAP y AFF
Determinar cómo se articulan ambas trazabilidades para sustentar la imputación y diferenciar titularidad de autoría o participación.	**Articulación probatoria para sustentar la imputación**	• Correspondencia temporal y funcional • Conducta individual (tiempo, modo y lugar) • Control y disposición • Conocimiento y voluntad • Forma de intervención • Regla inferencial • Contraindicios e hipótesis alternativas • Motivación	**Ficha de análisis documental:** secciones D y E **Guía de entrevista:** preguntas 8 a 10	RA-01 a RA-12; FP, FAP y AFF

Nota. Elaboración propia

Anexo 3

Ficha de análisis documental

Título: La trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático, Ayacucho 2019-2025

Objetivo de la ficha: registrar el razonamiento fiscal exteriorizado en cada requerimiento acusatorio respecto de la trazabilidad digital, la trazabilidad financiera y su articulación para sustentar la imputación.

Indicaciones: registrar únicamente lo que consta en el documento. Para cada referente, marcar el nivel de desarrollo: (D) desarrollado, (M) mencionado sin explicación suficiente, (N) no identificado o (NA) no aplicable a la modalidad.

A. Datos generales

Código del requerimiento	
Año de emisión	
Fiscalía (anonimizada)	
Modalidad del hecho	
Número de acusados	
Forma de intervención atribuida	

B. Trazabilidad digital (subcategoría 1)

Referente	Fuente y dato consignado	Nivel	Folio
Dirección IP / registros de acceso			
Línea telefónica, SIM, IMEI			
Dispositivo identificado o incautado			
Comunicaciones, páginas falsas, capturas			
Informe técnico o pericia			
Autenticidad, integridad y cadena de custodia			
Vinculación con el usuario efectivo			
Limitaciones técnicas declaradas			

C. Trazabilidad financiera (subcategoría 2)

Referente	Fuente y dato consignado	Nivel	Folio
Cuenta de origen y cuenta receptora			
Titularidad de las cuentas			
Fecha, hora, monto y canal			

Referente	Fuente y dato consignado	Nivel	Folio
Retiros y transferencias posteriores			
Billeteras digitales o criptomonedas			
Control efectivo de la cuenta			
Destino final y beneficiario			

D. Articulación probatoria (subcategoría 3)

Referente	Contenido identificado	Nivel	Folio
Cronología integrada de operaciones			
Correspondencia temporal y funcional			
Conducta individualizada (tiempo, modo, lugar)			
Inferencia sobre conocimiento y voluntad			
Regla de inferencia exteriorizada			
Diferencia titular / ejecutor / facilitador / beneficiario			
Contraindicios incorporados			
Hipótesis alternativas examinadas			

E. Síntesis interpretativa del investigador

Fecha de registro: _____ Responsable: _____

Nota. Instrumento elaborado a partir de los apartados 4.9 y 5.3 de la tesis (ejes de codificación de la Tabla 9).

Anexo 4

Guía de entrevista semiestructurada

Título: La trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático, Ayacucho 2019-2025

Objetivo: recoger los criterios, experiencias y dificultades de los operadores fiscales sobre el tratamiento de la trazabilidad digital y financiera para sustentar la imputación en casos de fraude informático.

Código del participante	FP-0__ / FAP-0__ / AFF-0__
Función	
Años de experiencia en delitos informáticos	
Fecha y lugar	
Modalidad de la entrevista	Presencial ( ) Virtual ( )
Duración	

Presentación: Agradezco su participación. La entrevista tiene fines exclusivamente académicos; sus respuestas serán anonimizadas mediante un código y no se consignarán nombres, números de carpetas, cuentas ni datos que permitan identificar a las personas involucradas. Puede omitir cualquier pregunta o retirarse en cualquier momento.

Objetivo específico 1: trazabilidad digital

1. Según su experiencia, ¿qué fuentes digitales (direcciones IP, registros de acceso, líneas telefónicas, tarjetas SIM, IMEI, dispositivos, comunicaciones o páginas falsas) resultan necesarias para reconstruir la ruta digital en un caso de fraude informático?

2. ¿Cómo se verifica la autenticidad, integridad y conservación de la información digital antes de incorporarla al requerimiento acusatorio (actas, cadena de custodia, respuesta formal de la entidad, metodología del informe técnico)?

3. ¿Qué dificultades ha enfrentado para obtener o preservar oportunamente esa información (demoras de operadoras y bancos, eliminación de registros, IP compartidas, proveedores extranjeros)?

4. ¿Qué elementos adicionales considera necesarios para vincular un identificador técnico (una IP, una línea o un dispositivo) con la persona que efectivamente realizó la operación?

Objetivo específico 2: trazabilidad financiera

5. ¿Qué información bancaria considera indispensable para reconstruir el desplazamiento del dinero (cuentas de origen y destino, titularidad, fecha, hora, monto, canal)?

6. ¿Cómo diferencia la titularidad registral de una cuenta receptora del control efectivo sobre ella? ¿Qué datos utiliza para establecer quién accedió, retiró o dispuso de los fondos?

7. ¿Hasta qué punto se sigue el recorrido del dinero después de la primera cuenta receptora (retiros, transferencias sucesivas, agentes, billeteras digitales o criptomonedas) y qué factores lo limitan?

Objetivo específico 3: articulación probatoria e imputación

8. ¿Cómo relaciona la secuencia digital con la secuencia financiera para individualizar la conducta de cada investigado? ¿Qué papel cumple la correspondencia temporal y funcional?

9. ¿Qué hechos le permiten inferir conocimiento, voluntad y una forma concreta de intervención, y cómo distingue al ejecutor de la manipulación, al facilitador de la cuenta y al beneficiario final?

10. ¿Cómo se examinan los contraindicios y las explicaciones alternativas (préstamo de cuenta, pérdida de tarjeta, suplantación, uso por terceros) y de qué manera se exterioriza la regla de inferencia en el requerimiento acusatorio?

Cierre: ¿Desea agregar alguna consideración sobre el tratamiento de la trazabilidad digital y financiera en las acusaciones por fraude informático? Muchas gracias por su colaboración.

Nota. Guía de diez preguntas abiertas vinculadas con los tres objetivos específicos (apartado 4.9 de la tesis). La profundización se adaptó al rol de cada participante.

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

Creado el 14 de junio de junio de 1979

ACTA DE SUSTENTACIÓN DE TESIS DEL ASPIRANTE JOSEPH MICHAEL QUISPE ATAUQUI

En la ciudad de Ayacucho siendo las 17:00 horas del día viernes 23 de octubre de 2026, reunidos en el auditorio de la Facultad de Derecho y Ciencias Políticas – UNSCH, los miembros del jurado examinador: Marlene León Palacios (presidente), Katherine Irma Quispe Vargas, Yenny Juana Barraza Torres, Oliverio García Quilca y Julio César Tello Jurado (miembros). Para examinar la tesis del aspirante Joseph Michael Quispe Atauqui titulado: La trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático, Ayacucho, 2019-2025.

Acto seguido se da lectura de la Resolución Decanal N° 420-2026-UNSCH-FDCP-D de fecha 16 de octubre del 2026 y el artículo 25 del Reglamento de Grados y Títulos.

Acto seguido el presidente del jurado otorga el uso de la palabra al aspirante, luego de la sustentación se procede a realizar las preguntas y/o objeciones que el jurado considere pertinente, una vez concluida se invita al aspirante y al público en general a salir del auditorio, acto seguido el jurado procede a deliberar.

El jurado decidió APROBAR POR UNANIMIDAD con la nota de 15 (QUINCE), con lo que concluye el acto académico con la firma del acta siendo las 18:37 pm horas.

Marlene León Palacios
(Presidente)

Katherine Irma Quispe Vargas
(Miembro)

Jenny Juana Barraza Torres
(Miembro)

Oliverio García Quilca
(Miembro)

Julio César Tello Jurado
(Miembro)

CONSTANCIA DE ORIGINALIDAD N° 02-2026-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.° 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. Joseph Michael QUISPE ATAUQUI**
Para	**Título profesional**
Denominación de la tesis	**La trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático, Ayacucho, 2019-2025**
Evaluación de Originalidad	**3%**
Numero de trabajo	**3074811220**
Fecha	**29 de octubre 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, 29 de octubre de 2026

Jenny Juana Barraza Torres

La trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático, Ayacucho, 2019-2025

por Joseph Michael QUISPE ATAUQUI

Fecha de entrega: 29-oct-2026 09:28p. m. (UTC-0500)
Identificador de la entrega: 3074811220
Nombre del archivo: TESIS_CORREGIDA_JOSEPH_QUISPE_ATAUQUI_2_.docx (601.31K)
Total de palabras: 23462
Total de caracteres: 148287

La trazabilidad digital y financiera para sustentar la imputación en los requerimientos acusatorios por fraude informático, Ayacucho, 2019-2025

INFORME DE ORIGINALIDAD

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

FUENTES PRIMARIAS

1	repositorio.upsc.edu.pe:8080 Fuente de Internet	<1%
2	repositorio.uap.edu.pe Fuente de Internet	<1%
3	repositorio.ucv.edu.pe Fuente de Internet	<1%
4	Submitted to Universidad Tecnologica del Peru Trabajo del estudiante	<1%
5	docplayer.net Fuente de Internet	<1%
6	hdl.handle.net Fuente de Internet	<1%
7	repositorio.ucsm.edu.pe Fuente de Internet	<1%
8	Submitted to D.A. de Derecho Trabajo del estudiante	<1%
9	repositorio.continental.edu.pe Fuente de Internet	<1%
10	Submitted to Universidad Catolica De Cuenca Trabajo del estudiante	<1%
11	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	<1%
12	repositorio.uncp.edu.pe Fuente de Internet	<1%
13	Submitted to Universidad Mariano Gálvez de Guatemala Trabajo del estudiante	<1%

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		