UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

TESIS:

Dificultades en la investigación del delito de estafa por el incremento del uso de medios tecnológicos en la Quinta Fiscalía Provincial Penal Corporativa de Huamanga, 2024.

Para optar el título profesional de:
ABOGADO

PRESENTADO POR:
Bach. Emilio JAIME MALDONADO

ASESOR:
Mtro. Richard ALMONACID ZAMUDIO

AYACUCHO - PERÚ

2025

Dedicatoria

Dedico esta tesis a mi familia, especialmente a mis padres, quienes han sido mi mayor inspiración y sostén en todo momento.

Agradecimiento:

Agradezco, en primer lugar, a mis padres por su apoyo incondicional y por haberme brindado las oportunidades para alcanzar mis metas. A mis profesores y asesores, por su guía, paciencia y conocimientos compartidos durante este proceso.

RESUMEN

La presente investigación tuvo como objetivo analizar las dificultades que enfrenta la Quinta Fiscalía Provincial Penal Corporativa de Huamanga en la investigación del delito de estafa, a raíz del incremento del uso de medios tecnológicos durante el año 2024. El estudio se desarrolló bajo un enfoque cualitativo y cuantitativo, mediante el análisis de 15 casos representativos y la revisión de estadísticas institucionales. Los resultados evidenciaron que el 60% de los casos fue archivado por limitaciones en la recolección de pruebas digitales, asociadas a la falta de herramientas tecnológicas adecuadas, escasa capacitación del personal y demoras significativas en la cooperación con entidades bancarias y plataformas tecnológicas. Asimismo, se identificó que la tasa de éxito en las investigaciones se relaciona directamente con la disponibilidad de recursos y el nivel de formación del equipo investigador. Las etapas de extracción forense, peritaje y requerimientos externos mostraron mayores retrasos, afectando el desarrollo eficiente de los procesos penales. Se concluye que la insuficiencia tecnológica, la limitada especialización y la débil cooperación interinstitucional dificultan gravemente la identificación y sanción de los responsables de estafas tecnológicas, por lo que se recomienda fortalecer la infraestructura forense, capacitar continuamente al personal y establecer convenios de colaboración con entidades clave del entorno digital.

Palabras clave: estafa tecnológica, medios digitales, Fiscalía Penal de Huamanga, evidencias digitales, cooperación interinstitucional.

ABSTRACT

This research aimed to analyze the difficulties faced by the Fifth Provincial Criminal Prosecutor's Office of Huamanga in investigating fraud crimes due to the increased use of technological means during 2024. The study adopted both qualitative and quantitative approaches, examining 15 representative cases and reviewing institutional data. The findings revealed that 60% of the cases were closed due to challenges in collecting digital evidence, linked to a lack of proper forensic tools, limited staff training, and significant delays in cooperation with financial institutions and digital platforms. The success rate of investigations was directly related to the availability of technological resources and the level of specialization of the investigation team. The forensic extraction, expert analysis, and external data requests stages showed the longest delays, hindering the effectiveness of the criminal process. It is concluded that technological shortcomings, lack of specialized training, and weak inter-institutional cooperation seriously hinder the identification and prosecution of those responsible for digital fraud. It is recommended to enhance forensic infrastructure, provide continuous training, and establish collaboration agreements with key digital actors.

Keywords: digital fraud, technological tools, Huamanga Prosecutor's Office, digital evidence, inter-institutional cooperation.

INTRODUCCIÓN

En los últimos años, el uso de tecnologías digitales ha transformado profundamente diversos aspectos de la vida cotidiana, incluyendo las formas en que se cometen delitos. En particular, la estafa, una modalidad delictiva tradicionalmente asociada a la manipulación directa de la víctima, ha evolucionado hacia nuevas variantes apoyadas en plataformas virtuales, redes sociales, billeteras electrónicas y otros medios digitales. Este cambio ha generado un crecimiento significativo de las denominadas estafas tecnológicas, caracterizadas por su complejidad, transnacionalidad y capacidad de anonimato, lo cual representa un serio desafío para los sistemas de justicia penal en el país.

En ese contexto, la Quinta Fiscalía Provincial Penal Corporativa de Huamanga ha experimentado un notable incremento en la recepción de denuncias por este tipo de delitos, lo que ha puesto a prueba sus capacidades técnicas, humanas y operativas. A diferencia de las estafas tradicionales, las investigaciones por medios tecnológicos requieren de herramientas forenses especializadas, conocimientos técnicos avanzados y una fluida cooperación con entidades bancarias, plataformas digitales y proveedores de servicios de internet. Sin embargo, la limitada disponibilidad de recursos tecnológicos, la escasa capacitación del personal fiscal y los constantes obstáculos en la obtención de información digital oportuna han dificultado considerablemente la persecución penal de estos hechos.

Esta problemática motiva la presente investigación, cuyo objetivo principal es analizar cómo el incremento del uso de medios tecnológicos para cometer el delito de estafa ha dificultado

las investigaciones realizadas por la Quinta Fiscalía Penal Corporativa de Huamanga durante el año 2024. Asimismo, se examina de qué manera la falta de recursos tecnológicos y la carencia de capacitación especializada, así como la débil cooperación interinstitucional, afectan la eficacia de las investigaciones penales.

El estudio cobra relevancia no solo por su aporte empírico, sustentado en el análisis de casos reales, sino también porque permite visibilizar las limitaciones estructurales que enfrenta el sistema de justicia frente a fenómenos delictivos cada vez más sofisticados. En ese sentido, los hallazgos de esta investigación servirán como base para la formulación de propuestas orientadas al fortalecimiento de las capacidades fiscales y la mejora de los mecanismos de cooperación entre actores del entorno digital, contribuyendo así a una respuesta penal más eficaz y oportuna frente a la criminalidad tecnológica.

INDICE

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 14

1.1. Descripción de la realidad problemática 14

1.2. Delimitación de la investigación 15

1.3. Formulación del problema 15

1.3.1. Problema principal 15

1.3.2. Problemas secundarios 15

1.4. Objetivos de la investigación 16

1.4.1. Objetivo General 16

1.4.2. Objetivo Específico 16

1.5. Justificación e importancia 17

1.5.1. Viabilidad de la investigación 18

CAPÍTULO II: MARCO TEÓRICO 20

2.1. Antecedentes de estudio 20

2.1.1. Antecedentes internacionales 20

2.1.2. Antecedentes nacionales 21

2.2. Bases teóricas 24

2.2.1. Delincuencia Informática 24

2.2.1.1. Modalidades de ciberdelincuencia 25

2.2.2. Descripción legal 27

2.2.3. Bien Jurídico Protegido 28

2.2.3.1. Tipicidad Objetiva 29

2.2.3.2. Conducta 30

2.2.4. Prevención de los delitos informáticos 31

2.2.5. El delito de estafa 32

2.2.5.1. Sujeto Activo en el delito de Estafa 34

2.2.5.2. El sujeto Pasivo en el delito de Estafa 35

2.2.5.3. Modalidades 36

2.2.6. Delitos informáticos 38

2.2.6.1. Características de los delitos informáticos 39

2.2.7. Ley de fraude informático 30096 40

2.2.7.1. Delitos contra datos y sistemas informáticos 42

2.2.7.2. Delitos informáticos contra la indemnidad y libertad sexuales 43

2.2.7.3. Delitos informáticos contra la intimidad y el secreto de las comunicaciones: 44

2.2.7.4. Delitos informáticos contra el patrimonio 45

2.2.7.5. Delitos informáticos contra la fe pública: 45

2.2.8. Marco Normativo Internacional 46

CAPÍTULO III: HIPÓTESIS Y VARIABLES 51

3.1. Formulación de hipótesis 51

3.1.1. Hipótesis general 51

3.1.2. Hipótesis Específicas 51

3.2. Variables de investigación 52

3.3. Operacionalización de variables e indicadores 52

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN 54

4.1. Enfoque de Investigación 54

4.2. Nivel de investigación 54
4.3. Método de la investigación 54
4.4. Diseño de la investigación 54
4.5. Universo, población y muestra 55
4.5.1. Universo 55
4.5.2. Población 55
4.5.3. Muestra 55
4.6. Técnicas, instrumentos y fuentes 55
4.6.1. Técnicas 55
4.6.2. Instrumentos 56
4.6.3. Fuentes 56
4.7. Técnicas de procesamiento y análisis de Datos Recolectados 57
CAPÍTULO V: ANÁLISIS Y DISCUSIÓN DE RESULTADOS 58
5.1. Interpretación de resultados 58
5.2. Discusión de resultados 70
5.2.1. Contrastación de hipótesis 71

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES 75

6.1. CONCLUSIONES 75

6.2. RECOMENDACIONES 76

BIBLIOGRAFÍA 77

ANEXOS 81

INDICE DE CUADROS Y TABLAS

Cuadro 1 Relación entre tipo de estafa, disponibilidad de recursos investigativos y resultado del caso en la Quinta Fiscalía Penal Corporativa de Huamanga, 2024 59

Cuadro 2 Dificultades en investigaciones por estafa tecnológica 60

Cuadro 3 Etapas de investigación con mayores demoras 61

Cuadro 4 Recursos tecnológicos para las investigaciones de estafa 62

Cuadro 5 Capacidad instalada vs requerida 63

Cuadro 6 Formación del personal 64

Cuadro 7 Capacitación y éxito investigativo 65

Cuadro 8 Plazos de respuesta de plataformas tecnológicas 66

Cuadro 9 Tiempos de respuesta de entidades financieras a solicitudes de información en investigaciones por estafa 67

Cuadro 10 Cumplimiento de requerimientos 68

Cuadro 11 Impacto del retraso en el resultado del caso 69

Cuadro 12 Ausencia de cooperación interinstitucional 69

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

El delito de estafa, históricamente vinculado a la manipulación y el engaño, ha evolucionado con el avance de la tecnología, adquiriendo formas más sofisticadas y difíciles de rastrear. En la actualidad, los medios tecnológicos han sido ampliamente utilizados para facilitar este tipo de delito, permitiendo a los perpetradores alcanzar a un mayor número de víctimas, reducir los riesgos de ser detectados y aumentar la complejidad de las investigaciones. Esta situación plantea serios retos para los operadores de justicia, en particular para las fiscalías encargadas de investigar y sancionar estos hechos.

En la Quinta Fiscalía Penal Provincial Corporativa de Huamanga, durante el año 2024, se ha observado un notable incremento en los casos de estafa cometidos mediante el uso de herramientas tecnológicas, como plataformas digitales, redes sociales, transferencias electrónicas fraudulentas y otras modalidades. Estas prácticas no solo afectan a las víctimas, sino que también complican la labor investigativa debido a la dificultad para rastrear a los responsables, acceder a evidencias digitales y comprender los métodos empleados.

En este contexto, resulta imprescindible analizar las dificultades que enfrentan los fiscales al abordar estos delitos. Factores como la falta de recursos tecnológicos, la limitada capacitación en cibercriminalidad, la rápida evolución de las técnicas utilizadas por los delincuentes y las barreras legales para obtener información digital, representan desafíos significativos en el proceso de investigación.

Esta investigación busca identificar y analizar estas dificultades para proponer soluciones que fortalezcan las capacidades investigativas de la Quinta Fiscalía Provincial Penal Corporativa de Huamanga, frente al incremento de estafas cometidas con el uso de medios tecnológicos. De esta forma, se espera contribuir al desarrollo de estrategias más efectivas para combatir este fenómeno delictivo y garantizar una adecuada protección de los derechos de las víctimas.

1.2. Delimitación de la investigación

La investigación se centra en la Quinta Fiscalía Provincial Penal Corporativa de Huamanga, como la institución encargada de abordar legalmente estos casos en la región, durante el 2024.

1.3. Formulación del problema

1.3.1. Problema principal

¿Cómo el incremento del uso de medios tecnológicos para cometer el delito de estafa dificulta las investigaciones realizadas por la Quinta Fiscalía Provincial Penal Corporativa de Huamanga en el año 2024?

1.3.2. Problemas secundarios

Problema específico 1

¿De qué manera la falta de recursos tecnológicos y capacitación especializada en cibercriminalidad limita la capacidad de los fiscales para recolectar y analizar evidencias

digitales en los casos de estafa tecnológica en la Quinta Fiscalía Penal Corporativa de Huamanga?

Problema específico 2

¿Cómo la ausencia de cooperación efectiva entre las plataformas tecnológicas, entidades bancarias y las autoridades judiciales afecta la identificación y persecución de los responsables de estafas cometidas mediante medios tecnológicos en Huamanga?

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Determinar cómo el incremento del uso de medios tecnológicos para cometer el delito de estafa dificulta las investigaciones realizadas por la Quinta Fiscalía Penal Corporativa de Huamanga en el año 2024.

1.4.2. Objetivo Específico

Objetivo Especifico 1:

Identificar de qué manera la falta de recursos tecnológicos y capacitación especializada en cibercriminalidad limita la capacidad de los fiscales para recolectar y analizar evidencias digitales en los casos de estafa tecnológica en la Quinta Fiscalía Penal Corporativa de Huamanga.

Objetivo Especifico 2:

Identificar cómo la ausencia de cooperación efectiva entre las plataformas tecnológicas, entidades bancarias y las autoridades judiciales afecta la identificación y persecución de los responsables de estafas cometidas mediante medios tecnológicos en Huamanga.

1.5. Justificación e importancia

El incremento del uso de medios tecnológicos para cometer el delito de estafa representa un desafío significativo para los sistemas de justicia a nivel global, nacional y local. En Huamanga, específicamente en la Quinta Fiscalía Penal Corporativa, esta problemática se agudiza debido a la falta de recursos tecnológicos, la limitada capacitación del personal en cibercriminalidad y las barreras legales para la obtención de pruebas digitales. Esta situación no solo afecta la eficacia de las investigaciones, sino que también genera una sensación de impunidad que incentiva la repetición del delito y debilita la confianza de la ciudadanía en el sistema judicial.

La presente investigación se justifica por su relevancia social, al abordar una problemática que impacta directamente en las víctimas de estafa, quienes a menudo enfrentan pérdidas económicas significativas y dificultades para obtener justicia. Asimismo, desde una perspectiva jurídica, esta investigación busca identificar las principales limitaciones que enfrenta la Fiscalía en la persecución de este delito, con el objetivo de proponer estrategias y soluciones que fortalezcan las capacidades investigativas en el contexto local.

Además, la investigación se fundamenta en la necesidad de generar conocimiento sobre un fenómeno delictivo en constante evolución, contribuyendo a la literatura académica y jurídica relacionada con los delitos tecnológicos en el Perú. Este estudio servirá como base para la

formulación de políticas públicas orientadas a mejorar la respuesta del sistema de justicia frente a los desafíos tecnológicos en el ámbito delictivo.

La importancia de esta tesis radica en su contribución para mejorar la eficacia del sistema judicial en Huamanga al investigar delitos de estafa tecnológica. Al identificar las dificultades específicas que enfrenta la Quinta Fiscalía Penal Corporativa, se podrán proponer medidas concretas para superar estas barreras, tales como la implementación de recursos tecnológicos avanzados, la capacitación especializada del personal fiscal y la promoción de alianzas estratégicas con entidades financieras y tecnológicas.

Por otro lado, la investigación es significativa porque permite visibilizar una problemática creciente que afecta no solo a la economía local, sino también a la percepción de justicia y seguridad en la población. A través de este estudio, se busca garantizar una mayor protección para las víctimas y reforzar la lucha contra el delito de estafa, contribuyendo al desarrollo de un sistema de justicia más eficiente, transparente y adaptado a los retos de la era digital.

1.5.1. Viabilidad de la investigación

La viabilidad de la investigación sobre el delito de fraude informático y las dificultades procesales en su aplicación en la Quinta Fiscalía Penal Corporativa de Ayacucho se sustenta en varios factores clave.

Primero, existe un acceso adecuado a fuentes de información relevantes, incluyendo registros detallados de casos, entrevistas con fiscales y expertos en ciberseguridad, lo que permitirá un análisis exhaustivo. Segundo, el apoyo institucional de la Quinta Fiscalía Penal Corporativa de

Ayacucho y otras entidades relacionadas con la administración de justicia y la ciberseguridad garantiza el acceso a los recursos y datos necesarios. Tercero, la disponibilidad de herramientas tecnológicas y metodológicas modernas facilita la recopilación y análisis de datos.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de estudio

2.1.1. Antecedentes internacionales

a. Chiluisa (2021)**,** en su tesis de grado titulada *"Los delitos informáticos y los vacíos legales"*, presentada en la Universidad Católica de Santiago de Guayaquil (Ecuador), sostiene que la legislación ecuatoriana evidencia importantes vacíos y contradicciones normativas frente al acelerado avance de la tecnología. El autor señala que el desarrollo jurídico no ha logrado adaptarse de manera eficaz a la evolución social y tecnológica, lo que ha dado lugar a nuevas modalidades delictivas que no se encuentran plenamente tipificadas, principalmente debido a la complejidad de su regulación y a su carácter transnacional. En ese contexto, el objetivo de la investigación fue elaborar un ensayo crítico-jurídico que evidencie los vacíos existentes en el ordenamiento jurídico ecuatoriano en relación con los delitos informáticos, contrastando la realidad social con el marco normativo vigente, a fin de proponer alternativas de solución frente a dicha problemática.

b. Gamba (2019), en su tesis de maestría titulada *"Delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos"*, presentada en la Universidad Externado de Colombia, analiza cómo el contexto de globalización y el acelerado desarrollo de las tecnologías de la información y la comunicación (TIC) han incrementado significativamente los riesgos para los usuarios, influenciados por factores económicos, sociales, culturales, políticos y jurídicos. El autor

destaca la necesidad de profundizar el conocimiento jurídico sobre este tipo de delitos, con el fin de fortalecer y unificar criterios legales que permitan su adecuada regulación. En ese sentido, resalta la importancia de la actuación de los organismos internacionales, tanto de manera multilateral como individual, para establecer marcos normativos que faciliten la correcta tipificación de estas conductas, su prevención, así como la imposición de sanciones por parte de las autoridades competentes.

2.1.2. Antecedentes nacionales

a. Catalan (2019), El presente estudio tuvo como objetivo analizar la influencia del comercio electrónico en la comisión del delito de estafa a través de la red social Facebook, fenómeno que ha venido incrementándose de manera constante. Ello se debe, en gran medida, a la inexistencia de una normativa específica que sancione de forma expresa las estafas cometidas mediante esta plataforma digital. En ese sentido, la investigación abordó el análisis de la tipicidad del delito de estafa y la relación existente entre el comercio electrónico y dicha conducta delictiva, partiendo de la premisa de determinar si el comercio electrónico constituye un medio facilitador para la comisión de este ilícito. Metodológicamente, el estudio se desarrolló bajo un enfoque cualitativo, con un tipo de investigación aplicada y un diseño interpretativo. Para la recolección de información se emplearon las técnicas de la entrevista y el análisis de fuentes documentales. Como resultado, se concluyó que el comercio electrónico influye de manera significativa en la comisión de estafas a través de Facebook, debido a la facilidad de acceso que ofrece la plataforma al sujeto activo, así como a la creciente preferencia de los usuarios por utilizar esta red social para realizar compras, al considerarla un medio cómodo, rápido y accesible desde sus hogares. Esta situación es aprovechada por los estafadores para engañar a los usuarios y, en muchos casos, evadir responsabilidad penal, como consecuencia de los vacíos legales existentes frente a esta modalidad delictiva. Asimismo, la falta de

información y educación digital incrementa la vulnerabilidad de los usuarios de Facebook, haciéndolos más propensos a convertirse en víctimas de este tipo de estafas virtuales.

b. Acosta (2024), La investigación tuvo como objetivo general determinar los efectos de la insuficiente legislación persecutoria del delito de estafa cibernética en el distrito fiscal del Santa, 2022. Se realizó una investigación básica, de diseño cualitativo no experimental, se contó con 10 participantes entre jueces y fiscales, asimismo se revisaron 12 carpetas fiscales. Se empleó la entrevista como técnica y la revisión documental, como instrumentos se emplearon la guia de entrevista y la guia de observación documental respectivamente. Respecto a los hallazgos, los participantes reconocieron la influencia de la normativa internacional del Convenio de Budapest, pero enfatizaron la necesidad de mejorar la tipificación del delito para una implementación más efectiva. Asimismo se logró determinar que la falta de legislación adecuada impactó negativamente en la detección, investigación y sanción del delito de estafa cibernética en el distrito, con menor capacidad para prevenir, detectar e investigar, resultando en acusaciones limitadas y condenas desproporcionadas. Se observó un mayor riesgo de impunidad y menor protección a las víctimas, mientras que la legislación ambigua dificultó el trabajo de fiscales y jueces. Es necesario adaptar y fortalecer la legislación, proteger a las víctimas y facilitar la cooperación transfronteriza en la persecución del delito de estafa cibernética en el distrito.

c. Vilca (2018), en su tesis de grado “Los hackers: delito informático frente al Código Penal Peruano.”, presentada en la Universidad Nacional Santiago Antúnez de Mayolo, Huaraz - Perú. La investigación menciona luego de haber realizado un análisis comparativo con las legislaciones de otros países, llegando a la conclusión que en el Perú si bien se reglamenta

los delitos informáticos, ésta es imperfecta y de carácter generalizado, generando vacíos legales que impiden desarrollar adecuadamente la investigación forense en materia informática, permitiendo que los hackers tengan una especie de impunidad y beneficio porque no es fácil lograr su identificación e individualización para ser sancionados.

d. Huamán (2020), en sus tesis de grado "Los delitos informáticos en el Perú y la suscripción del Convenio de Budapest", presentada en la universidad Andina del Cusco, Cusco - Perú. En su investigación señala que dicho Convenio, es el marco legislativo rector a nivel mundial para combatir el ciberdelito, cuya metodología es de carácter teórico y legislativo, mencionando que éste lleva a la conclusión, que la suscripción de este Pacto predomina de manera estricta el tratamiento de los delitos informáticos, haciendo que los países integrantes adecuen sus normas a las previstas en el presente convenio.

e. Arellano & Galindo (2022), en su tesis de grado "Deficiencias legislativas en el tratamiento de la Ley N° 30096, Ley de delitos informáticos – fraude informático, Lima 2019 – 2021", presentada en la Universidad Cesar Vallejo, Lima – Perú. En su estudio realizado menciona las deficiencias en materia legislativa que advirtió referente al delito de fraude informático, permitiendo un crecimiento acelerado de esta nueva modalidad delictiva, esta deficiencia normativa y procedimental imposibilita individualizar al sujeto activo del delito, ciberdelincuente o hacker, generando un clima de desamparo y desprotección de la víctima frente al agresor.

2.2. Bases teóricas

2.2.1. Delincuencia Informática

La delincuencia informática se refiere al conjunto de conductas ilícitas que se cometen mediante el uso de sistemas informáticos, redes digitales o tecnologías de la información, ya sea como medio, como fin o como soporte del delito. Estas conductas se caracterizan por aprovechar las vulnerabilidades tecnológicas y la interconectividad global para afectar bienes jurídicos tradicionales, como el patrimonio, la intimidad o la seguridad, así como nuevos bienes jurídicos vinculados al entorno digital. Según Miró Llinares (2012), la delincuencia informática representa una manifestación de la criminalidad moderna que surge como consecuencia directa del desarrollo tecnológico y de la progresiva digitalización de las relaciones sociales y económicas.

Desde una perspectiva jurídica, la delincuencia informática comprende delitos clásicos adaptados al entorno digital —como la estafa, el fraude o la falsificación— y delitos propiamente informáticos, tales como el acceso ilícito a sistemas, la interferencia de datos o el sabotaje informático. El Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como el Convenio de Budapest, define estas conductas como aquellas que atentan contra la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos, constituyéndose en el principal instrumento internacional para su prevención y sanción (Consejo de Europa, 2001). Este enfoque evidencia la necesidad de una respuesta penal especializada y coordinada a nivel internacional, dada la naturaleza transnacional de este fenómeno.

Asimismo, la delincuencia informática se ve favorecida por factores como el anonimato relativo en internet, la rapidez de las transacciones electrónicas y la falta de conocimiento técnico de los usuarios, lo que incrementa su vulnerabilidad frente a estas conductas delictivas. Autores como Pérez Luño (2010) advierten que la insuficiencia normativa y la lenta adaptación del derecho penal frente a los avances tecnológicos generan vacíos legales que dificultan la persecución eficaz de estos delitos. En consecuencia, resulta imprescindible el fortalecimiento de los marcos normativos y de las capacidades institucionales para garantizar una adecuada protección de los derechos fundamentales en el entorno digital.

2.2.1.1. Modalidades de ciberdelincuencia

Las modalidades de ciberdelincuencia comprenden un conjunto diverso de conductas ilícitas que se ejecutan utilizando las tecnologías de la información y la comunicación como medio principal. Entre las más frecuentes se encuentran los delitos contra los sistemas informáticos, tales como el acceso ilícito, la interceptación indebida de datos y el sabotaje informático, los cuales afectan la confidencialidad, integridad y disponibilidad de la información digital. Estas conductas suelen estar dirigidas a vulnerar sistemas públicos o privados con fines de daño, espionaje o beneficio económico, y constituyen una de las primeras formas reconocidas de criminalidad informática (Consejo de Europa, 2001).

Otra modalidad relevante es la ciberdelincuencia de carácter patrimonial, dentro de la cual se ubican delitos como la estafa informática, el fraude electrónico, la suplantación de identidad y el phishing. En estos casos, el uso de plataformas digitales, redes sociales y sistemas de pago electrónico facilita el engaño a las víctimas, quienes son inducidas a entregar voluntariamente

datos personales o recursos económicos. Esta modalidad se ha incrementado de manera significativa con el auge del comercio electrónico y la masificación del uso de redes sociales, convirtiéndose en una de las formas más comunes de ciberdelito (Miró Llinares, 2012).

Asimismo, se identifican modalidades de ciberdelincuencia que atentan contra derechos fundamentales de la persona, como la intimidad, el honor y la libertad sexual. Entre ellas se encuentran el ciberacoso, el grooming, la difusión no consentida de material íntimo y la pornografía infantil. Estas conductas se caracterizan por el uso de medios digitales para hostigar, manipular o explotar a las víctimas, muchas veces en contextos de anonimato y dificultad probatoria, lo que complica la labor de persecución penal y protección efectiva de las personas afectadas (Pérez Luño, 2010).

Finalmente, debe considerarse la ciberdelincuencia de naturaleza transnacional, vinculada a organizaciones criminales que operan a través de redes globales para el lavado de activos, el financiamiento ilícito o el ataque a infraestructuras críticas. La ausencia de fronteras en el ciberespacio y la disparidad normativa entre los Estados favorecen la impunidad de estas conductas, lo que evidencia la necesidad de cooperación internacional y de una actualización constante de los marcos jurídicos nacionales. En este contexto, la tipificación clara de las modalidades de ciberdelincuencia resulta esencial para una respuesta penal eficaz frente a los nuevos desafíos que plantea la criminalidad digital.

2.2.2. Descripción legal

La delincuencia informática en el ordenamiento jurídico peruano se encuentra regulada principalmente por la Ley N.° 30096, Ley de Delitos Informáticos, promulgada en el año 2013 y posteriormente modificada por la Ley N.° 30171. Esta norma tiene como finalidad proteger bienes jurídicos vinculados a la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, así como prevenir y sancionar las conductas ilícitas que se cometen mediante el uso indebido de las tecnologías de la información y la comunicación. La citada ley incorpora al Código Penal diversos tipos penales que responden a las nuevas formas de criminalidad digital, adecuando el derecho penal a los avances tecnológicos.

Desde el punto de vista normativo, la Ley N.° 30096 tipifica conductas como el acceso ilícito a sistemas informáticos, el atentado contra datos y sistemas informáticos, el fraude informático, la suplantación de identidad y el abuso de mecanismos informáticos, entre otros. Estas conductas pueden tener como finalidad causar daño, obtener un beneficio económico indebido o vulnerar derechos fundamentales de las personas. Asimismo, la ley reconoce que los delitos informáticos pueden cometerse tanto de manera directa como indirecta, utilizando plataformas digitales, redes sociales o sistemas electrónicos como medio para la ejecución del ilícito.

No obstante, pese a los avances normativos, la descripción legal de la delincuencia informática presenta limitaciones frente a la constante evolución de las modalidades delictivas en el ciberespacio. En particular, se advierten vacíos o dificultades interpretativas en la aplicación de los tipos penales a conductas cometidas a través de redes sociales y entornos de comercio electrónico, lo que puede generar problemas de tipicidad y persecución penal efectiva. En ese

sentido, resulta necesario fortalecer y actualizar de manera continua el marco legal, a fin de garantizar una adecuada respuesta del Estado frente a las nuevas manifestaciones de la ciberdelincuencia.

2.2.3. Bien Jurídico Protegido

En los delitos informáticos, el bien jurídico protegido está constituido principalmente por la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, elementos esenciales para el correcto funcionamiento de las relaciones sociales, económicas y jurídicas en el entorno digital. Estos bienes jurídicos garantizan que la información contenida en los sistemas informáticos no sea accedida, alterada o destruida sin autorización, protegiendo así la seguridad y confianza en el uso de las tecnologías de la información. En el ordenamiento jurídico peruano, la Ley N.° 30096 reconoce expresamente la necesidad de tutelar estos intereses frente a conductas que vulneran el normal desenvolvimiento de los sistemas informáticos.

Asimismo, la protección penal de los delitos informáticos no se limita únicamente a los sistemas y datos en sí mismos, sino que se extiende a bienes jurídicos tradicionales afectados a través del uso de medios digitales, tales como el patrimonio, la intimidad, el honor y la autodeterminación informativa de las personas. En este sentido, cuando la delincuencia informática se manifiesta mediante conductas como la estafa, el fraude electrónico o la suplantación de identidad, el bien jurídico protegido adquiere una naturaleza compleja o pluriofensiva, al lesionarse simultáneamente intereses patrimoniales y derechos fundamentales del individuo.

Finalmente, la tutela del bien jurídico protegido en materia de delitos informáticos responde a la necesidad de preservar la confianza y seguridad jurídica en el ciberespacio, elemento indispensable para el desarrollo del comercio electrónico y de las relaciones digitales. La vulneración reiterada de estos bienes genera desconfianza en el uso de plataformas tecnológicas y debilita el sistema de protección legal. Por ello, el reconocimiento y delimitación clara del bien jurídico protegido resulta fundamental para una adecuada tipificación penal y para la correcta aplicación de las sanciones frente a las nuevas modalidades de criminalidad informática.

2.2.3.1. Tipicidad Objetiva

La tipicidad objetiva en los delitos informáticos se refiere a la verificación de los elementos externos y observables de la conducta descrita en el tipo penal, es decir, al análisis de la acción u omisión, el sujeto activo, el objeto material y el nexo causal entre la conducta y el resultado lesivo. En este tipo de delitos, la conducta típica se manifiesta a través del uso indebido de sistemas informáticos, redes digitales o plataformas tecnológicas, mediante actos como el acceso no autorizado, la manipulación de datos, la interferencia en sistemas o el empleo de mecanismos informáticos para obtener un beneficio indebido.

En cuanto al sujeto activo, los delitos informáticos suelen ser de sujeto activo indeterminado, lo que implica que cualquier persona con acceso a medios tecnológicos puede cometerlos, sin requerirse una cualificación especial. El objeto material del delito está constituido por los datos, sistemas informáticos o recursos tecnológicos que son vulnerados, así como por los bienes patrimoniales o derechos que resultan afectados como consecuencia de la conducta ilícita.

Asimismo, el tipo objetivo exige que la acción se realice sin autorización o excediendo la autorización otorgada, elemento esencial para configurar la ilicitud penal.

Finalmente, el resultado típico en los delitos informáticos puede consistir en la alteración, destrucción, supresión, bloqueo o acceso indebido a datos y sistemas, así como en la producción de un perjuicio económico o la puesta en peligro del bien jurídico protegido. El nexo causal se establece cuando se acredita que el daño o peligro generado es consecuencia directa de la conducta desplegada por el agente mediante el uso de herramientas informáticas. De este modo, la tipicidad objetiva permite delimitar la conducta penalmente relevante y diferenciarla de actuaciones meramente administrativas o civiles dentro del entorno digital.

2.2.3.2. Conducta

La conducta en los delitos informáticos está constituida por la acción u omisión realizada por el agente mediante el uso indebido de sistemas informáticos, redes digitales o plataformas tecnológicas, con la finalidad de vulnerar bienes jurídicos protegidos por la ley penal. Dicha conducta se exterioriza a través de actos concretos como el acceso no autorizado a sistemas informáticos, la manipulación o alteración de datos, la creación o utilización de perfiles falsos, el envío de comunicaciones engañosas o el empleo de medios electrónicos para inducir a error a la víctima. Estas acciones se caracterizan por su ejecución en entornos virtuales, lo que dificulta su detección e identificación inmediata.

Desde el punto de vista jurídico-penal, la conducta típica en los delitos informáticos suele ser comisiva, en tanto implica una actuación positiva del sujeto activo orientada a la realización

del tipo penal. No obstante, en determinados supuestos, la conducta también puede manifestarse de forma omisiva, cuando el agente, teniendo el deber jurídico de evitar un resultado lesivo —como ocurre con administradores de sistemas o responsables de seguridad informática—, permite que se produzca la vulneración de datos o sistemas. En ambos casos, la conducta debe ser voluntaria y contraria al ordenamiento jurídico para que resulte penalmente relevante.

Finalmente, la conducta en los delitos informáticos adquiere especial relevancia cuando se emplean redes sociales o plataformas de comercio electrónico, debido a la facilidad de interacción con un número indeterminado de usuarios. En estos escenarios, el agente puede desplegar conductas reiteradas y sistemáticas, aprovechando el anonimato relativo y la confianza de los usuarios, lo que incrementa el riesgo de afectación del bien jurídico protegido. Por ello, el análisis de la conducta resulta fundamental para determinar la configuración del tipo penal y establecer la responsabilidad correspondiente.

2.2.4. Prevención de los delitos informáticos

La prevención de los delitos informáticos constituye un eje fundamental de la política criminal del Estado, en tanto busca reducir los riesgos asociados al uso de las tecnologías de la información y comunicación antes de que se produzca la afectación del bien jurídico protegido. Desde una perspectiva jurídica, la prevención no solo se limita a la sanción penal posterior, sino que comprende la adopción de medidas normativas, institucionales y educativas orientadas a fortalecer la seguridad digital y la confianza en el ciberespacio. En este sentido, el establecimiento de marcos legales claros y actualizados resulta indispensable para disuadir la comisión de conductas delictivas en entornos virtuales.

Asimismo, la prevención de la ciberdelincuencia exige la implementación de mecanismos técnicos y organizativos adecuados, tanto en el sector público como en el privado. Entre estas medidas se incluyen el fortalecimiento de los sistemas de seguridad informática, la protección de datos personales, la verificación de identidades digitales y la capacitación constante del personal encargado de la gestión de sistemas informáticos. Estas acciones permiten disminuir las vulnerabilidades tecnológicas que suelen ser aprovechadas por los delincuentes informáticos para ejecutar sus conductas ilícitas.

Finalmente, un componente esencial de la prevención de los delitos informáticos es la educación y concientización de los usuarios, quienes representan uno de los eslabones más vulnerables frente a este tipo de criminalidad. La difusión de información sobre buenas prácticas digitales, el reconocimiento de modalidades de estafa y fraude electrónico, así como el uso responsable de redes sociales y plataformas de comercio electrónico, contribuyen significativamente a reducir el número de víctimas. De este modo, la prevención integral de los delitos informáticos requiere una acción coordinada entre el Estado, las instituciones privadas y la sociedad en general.

2.2.5. El delito de estafa

El delito de estafa constituye una infracción penal de carácter patrimonial que se configura cuando una persona, mediante engaño, fraude o cualquier otra maniobra dolosa, induce a error a otra con la finalidad de obtener un beneficio económico indebido en perjuicio de la víctima. Este delito se encuentra tipificado en el artículo 196 del Código Penal peruano y tiene como bien jurídico protegido el patrimonio, entendido como el conjunto de bienes y derechos de contenido

económico de la persona. La esencia de la estafa radica en la utilización de un engaño idóneo que determina un acto de disposición patrimonial por parte del sujeto pasivo.

Desde el punto de vista dogmático, la estructura típica del delito de estafa exige la concurrencia de determinados elementos objetivos, tales como el engaño precedente o concurrente, el error generado en la víctima, el acto de disposición patrimonial y el perjuicio económico. Asimismo, el delito requiere la existencia de una relación de causalidad entre el engaño desplegado por el agente y el daño patrimonial producido. La ausencia de cualquiera de estos elementos impide la configuración del tipo penal, lo que cobra especial relevancia en los casos de estafa cometidos a través de medios tecnológicos.

En la actualidad, el delito de estafa ha evolucionado significativamente con el uso de las tecnologías de la información y comunicación, dando lugar a nuevas modalidades como la estafa informática, el fraude electrónico y las estafas realizadas a través de redes sociales y plataformas digitales. Estas formas modernas de estafa se caracterizan por la facilidad de acceso del agente a las víctimas, el uso del anonimato y la rapidez en la ejecución de las conductas delictivas, lo que incrementa la dificultad para su investigación y sanción. En estos casos, los medios tecnológicos actúan como instrumentos que potencian la eficacia del engaño.

Finalmente, el incremento del delito de estafa en entornos digitales plantea importantes desafíos para el sistema de justicia penal, particularmente en la etapa de investigación. La obtención y valoración de la prueba digital, la identificación del sujeto activo y la delimitación de la competencia territorial constituyen aspectos críticos para la persecución penal efectiva. Por ello, resulta necesario adecuar los marcos normativos y fortalecer las capacidades institucionales de los

operadores de justicia, a fin de garantizar una respuesta eficaz frente a esta modalidad delictiva y una adecuada protección del patrimonio de los ciudadanos.

2.2.5.1. Sujeto Activo en el delito de Estafa

El sujeto activo en el delito de estafa es la persona que realiza la conducta típica consistente en engañar a otro con el propósito de obtener un beneficio patrimonial indebido. De acuerdo con el artículo 196 del Código Penal peruano, la estafa es un delito de sujeto activo común, lo que implica que puede ser cometido por cualquier persona, sin que se requiera una cualidad especial o condición específica del agente. Basta con que el sujeto tenga capacidad de acción y voluntad para ejecutar el engaño que induce a error a la víctima.

En la configuración del sujeto activo, resulta relevante la capacidad del agente para desplegar un engaño idóneo, es decir, una maniobra fraudulenta suficientemente apta para generar error en el sujeto pasivo. En los casos de estafa cometida mediante medios tecnológicos, el sujeto activo suele valerse de herramientas digitales como redes sociales, plataformas de comercio electrónico, aplicaciones de mensajería o sistemas de pago electrónico, lo que le permite ampliar su alcance, ocultar su identidad y ejecutar el delito con mayor rapidez y eficacia.

Asimismo, el sujeto activo puede actuar de manera individual o como parte de una organización criminal, especialmente en las modalidades de estafa informática o fraude electrónico. En estos supuestos, la intervención de varios agentes puede darse bajo diferentes formas de participación, tales como autoría directa, coautoría o complicidad, de conformidad con

las reglas generales de la parte general del Código Penal. La actuación organizada incrementa la complejidad de la investigación y dificulta la identificación de los responsables.

Finalmente, el análisis del sujeto activo en el delito de estafa resulta fundamental para determinar la responsabilidad penal y la estrategia de persecución del delito. En contextos como el uso intensivo de medios tecnológicos, la identificación del agente se ve obstaculizada por el anonimato y la utilización de identidades falsas, lo que exige el empleo de técnicas especializadas de investigación y cooperación interinstitucional. Por ello, la correcta delimitación del sujeto activo contribuye a una aplicación eficaz del derecho penal frente a esta modalidad delictiva.

2.2.5.2. El sujeto Pasivo en el delito de Estafa

El sujeto pasivo en el delito de estafa es la persona natural o jurídica que sufre el engaño desplegado por el sujeto activo y, como consecuencia de ello, realiza un acto de disposición patrimonial que le ocasiona un perjuicio económico. En el ordenamiento jurídico peruano, el bien jurídico protegido en este delito es el patrimonio, por lo que el sujeto pasivo es aquel titular del bien o derecho patrimonial afectado. No se requiere una condición especial para ostentar esta calidad, bastando con que la persona sea susceptible de ser inducida a error mediante maniobras fraudulentas.

Desde una perspectiva dogmática, el sujeto pasivo debe ser quien experimente el error como resultado directo del engaño, pues es dicho error el que motiva la disposición patrimonial perjudicial. En ese sentido, la relación entre el engaño, el error y el perjuicio económico resulta esencial para la configuración del tipo penal. En los casos de estafa cometida a través de medios

tecnológicos, el sujeto pasivo suele ser el usuario de plataformas digitales, redes sociales o sistemas de comercio electrónico, quienes confían en la veracidad de la información proporcionada por el agente.

Asimismo, el sujeto pasivo puede encontrarse en una situación de mayor vulnerabilidad debido a factores como la falta de conocimientos tecnológicos, la desinformación o la confianza excesiva en los entornos digitales. Estas circunstancias son frecuentemente aprovechadas por el sujeto activo para ejecutar el engaño, especialmente en contextos virtuales donde el contacto personal es inexistente y la verificación de la identidad del agente resulta limitada. Esta vulnerabilidad incrementa la incidencia de estafas en el ámbito digital.

Finalmente, el reconocimiento del sujeto pasivo en el delito de estafa resulta relevante no solo para la determinación del perjuicio económico, sino también para la protección de sus derechos durante el proceso penal. En particular, en las estafas tecnológicas, resulta fundamental garantizar el acceso del sujeto pasivo a mecanismos efectivos de denuncia, investigación y reparación del daño, a fin de fortalecer la confianza en el sistema de justicia y en el uso seguro de los medios tecnológicos.

2.2.5.3. Modalidades

El delito de estafa presenta diversas modalidades en función de los medios empleados por el sujeto activo y de las circunstancias en que se ejecuta el engaño. Tradicionalmente, la estafa se ha manifestado mediante conductas presenciales, tales como el uso de documentos falsos, promesas fraudulentas o simulación de hechos inexistentes, con el propósito de inducir a error a la

víctima. Estas modalidades clásicas se caracterizan por el contacto directo entre el agente y el sujeto pasivo, así como por la utilización de mecanismos de engaño que aparentan legalidad o veracidad.

Con el desarrollo de las tecnologías de la información y comunicación, han surgido nuevas modalidades de estafa vinculadas al entorno digital, entre las que destacan la estafa informática, el fraude electrónico y las estafas cometidas a través de redes sociales y plataformas de comercio electrónico. En estas modalidades, el sujeto activo emplea medios tecnológicos como correos electrónicos, aplicaciones de mensajería instantánea, perfiles falsos y enlaces fraudulentos para obtener información personal o recursos económicos de la víctima. La rapidez y el anonimato propios de estos medios incrementan la eficacia del engaño y dificultan su detección.

Asimismo, existen modalidades de estafa que se ejecutan mediante sistemas de pago electrónico y operaciones financieras digitales, tales como transferencias bancarias no consentidas, uso indebido de tarjetas de crédito o billeteras electrónicas. En estos casos, el engaño se orienta a obtener acceso a credenciales financieras o a inducir a la víctima a autorizar transacciones fraudulentas, generando un perjuicio patrimonial inmediato. Estas modalidades suelen requerir conocimientos técnicos básicos por parte del agente, lo que evidencia la adaptación de la estafa a los nuevos contextos tecnológicos.

Finalmente, las modalidades de estafa pueden presentarse de forma individual o organizada, cuando el delito es cometido por grupos que actúan de manera coordinada y sistemática. La participación de múltiples agentes permite la diversificación de funciones y el aumento del alcance delictivo, lo que agrava el impacto del delito y complica su investigación. En

este contexto, el reconocimiento y clasificación de las modalidades de estafa resulta esencial para la adecuada tipificación penal y para el diseño de estrategias efectivas de prevención y persecución del delito.

2.2.6. Delitos informáticos

Los delitos informáticos constituyen un conjunto de conductas ilícitas que se cometen mediante el uso de sistemas informáticos, redes digitales o tecnologías de la información, ya sea como medio, como fin o como instrumento para la ejecución del delito. Estas conductas se caracterizan por aprovechar las vulnerabilidades propias del entorno digital para afectar bienes jurídicos protegidos por el derecho penal, tales como la confidencialidad, integridad y disponibilidad de los datos, así como el patrimonio, la intimidad y la seguridad de las personas. La creciente digitalización de las relaciones sociales y económicas ha propiciado un incremento significativo de estas formas de criminalidad.

En el ordenamiento jurídico peruano, los delitos informáticos se encuentran regulados principalmente por la **Ley N.° 30096, Ley de Delitos Informáticos**, que incorpora diversos tipos penales destinados a sancionar conductas como el acceso ilícito a sistemas informáticos, el atentado contra datos y sistemas, el fraude informático y la suplantación de identidad. Esta normativa responde a la necesidad de adaptar el derecho penal a los avances tecnológicos y de brindar una protección efectiva frente a las nuevas modalidades delictivas que surgen en el ciberespacio.

Desde una perspectiva criminológica, los delitos informáticos presentan características particulares, como el anonimato relativo del autor, la rapidez en la ejecución de las conductas, la dificultad en la obtención de pruebas y su frecuente carácter transnacional. Estas particularidades generan importantes desafíos para los operadores del sistema de justicia, especialmente en la etapa de investigación, donde se requiere el uso de técnicas especializadas y la cooperación interinstitucional e internacional para identificar a los responsables y acreditar la comisión del delito.

Finalmente, el tratamiento jurídico de los delitos informáticos exige una respuesta integral que no se limite únicamente a la sanción penal, sino que incluya medidas de prevención, capacitación y fortalecimiento institucional. La actualización constante del marco normativo, la especialización de fiscales y jueces, y la concientización de los usuarios sobre el uso seguro de las tecnologías resultan fundamentales para enfrentar de manera eficaz este fenómeno delictivo y garantizar la protección de los derechos fundamentales en el entorno digital.

2.2.6.1. Características de los delitos informáticos

Los delitos informáticos se caracterizan, en primer lugar, por el uso de sistemas informáticos y tecnologías digitales como medio principal para la comisión del ilícito. El agente emplea herramientas tecnológicas, redes digitales o plataformas virtuales para ejecutar la conducta delictiva, lo que permite una mayor rapidez en su realización y un alcance potencialmente masivo. Esta característica diferencia a los delitos informáticos de las formas tradicionales de criminalidad y exige una respuesta penal especializada.

Otra característica relevante es el anonimato relativo del autor, ya que el uso de identidades falsas, direcciones IP dinámicas y plataformas digitales dificulta la identificación del sujeto activo. Este anonimato favorece la impunidad y complica la labor investigativa de las autoridades, especialmente cuando las conductas se ejecutan desde distintas jurisdicciones. Asimismo, los delitos informáticos suelen presentar un carácter transnacional, lo que requiere cooperación internacional para su investigación y sanción.

Asimismo, los delitos informáticos se distinguen por la volatilidad de la prueba digital, dado que los datos pueden ser alterados, eliminados o modificados con facilidad. La obtención, preservación y valoración de este tipo de evidencia demanda conocimientos técnicos especializados y el cumplimiento de protocolos específicos para garantizar su validez procesal. La ausencia de estas capacidades puede afectar la eficacia de la investigación penal.

Finalmente, los delitos informáticos suelen evolucionar de manera constante, adaptándose a los avances tecnológicos y a las nuevas formas de interacción digital. Esta dinamicidad genera vacíos normativos y dificultades interpretativas en la aplicación del derecho penal, lo que evidencia la necesidad de una actualización permanente de la legislación y de la capacitación continua de los operadores de justicia. En consecuencia, estas características hacen de los delitos informáticos un fenómeno complejo y desafiante para el sistema penal.

2.2.7. Ley de fraude informático 30096

La Ley N.° 30096, Ley de Delitos Informáticos, constituye el principal marco normativo peruano destinado a prevenir y sancionar las conductas ilícitas cometidas mediante el uso de

sistemas informáticos y tecnologías de la información. Esta ley fue promulgada con la finalidad de adecuar el derecho penal a los avances tecnológicos y de brindar protección efectiva a bienes jurídicos vinculados al entorno digital, tales como la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Asimismo, busca responder al incremento de delitos cometidos a través de medios tecnológicos, entre ellos el fraude informático.

En relación con el fraude informático, la Ley N.° 30096 tipifica conductas orientadas a la obtención de un beneficio patrimonial indebido mediante la manipulación de sistemas informáticos, datos digitales o mecanismos electrónicos. Estas conductas se configuran cuando el agente, sin autorización o excediendo la concedida, altera, introduce, suprime o utiliza indebidamente datos informáticos con el propósito de causar un perjuicio económico a un tercero. De esta manera, la norma amplía la protección penal del patrimonio frente a nuevas modalidades delictivas que no encajaban plenamente en los tipos tradicionales de estafa.

Asimismo, la ley reconoce la complejidad de los delitos informáticos al establecer agravantes cuando las conductas afectan sistemas del Estado, infraestructuras críticas o cuando se cometen de manera organizada. No obstante, en la práctica, la aplicación de la Ley N.° 30096 presenta desafíos interpretativos y probatorios, especialmente cuando el fraude se ejecuta a través de redes sociales o plataformas digitales que no encajan de forma expresa en los supuestos normativos, lo que puede generar dificultades en la tipificación y persecución penal.

Finalmente, la Ley N.° 30096 representa un avance significativo en la lucha contra el fraude informático en el Perú; sin embargo, su eficacia depende del fortalecimiento de las capacidades técnicas de los operadores del sistema de justicia y de la actualización constante de

sus disposiciones. En ese sentido, resulta necesario complementar esta normativa con políticas de prevención, capacitación especializada y cooperación interinstitucional, a fin de garantizar una respuesta penal efectiva frente a las nuevas formas de criminalidad informática.

2.2.7.1. Delitos contra datos y sistemas informáticos

Los delitos contra datos y sistemas informáticos comprenden aquellas conductas ilícitas que tienen como finalidad vulnerar la confidencialidad, integridad y disponibilidad de la información digital y de los sistemas informáticos que la contienen. En el ordenamiento jurídico peruano, estas conductas se encuentran tipificadas en la Ley N.° 30096, la cual protege los datos y sistemas frente a accesos no autorizados, interferencias indebidas y actos de sabotaje informático. La tutela penal de estos bienes jurídicos resulta esencial para garantizar la seguridad y confianza en el uso de las tecnologías de la información.

Entre las principales modalidades de estos delitos se encuentran el acceso ilícito a sistemas informáticos, la interceptación indebida de datos, la alteración, supresión o destrucción de información digital, así como la obstaculización del funcionamiento de sistemas informáticos. Estas conductas pueden ejecutarse con diversas finalidades, como la obtención de información confidencial, el beneficio económico indebido o la afectación deliberada de servicios públicos o privados. En todos los casos, la ausencia de autorización o el exceso de la misma constituye un elemento central para la configuración del tipo penal.

Desde una perspectiva procesal, la investigación de los delitos contra datos y sistemas informáticos presenta importantes desafíos, debido a la naturaleza técnica y volátil de la evidencia

digital. La identificación del autor, la preservación de los registros electrónicos y la reconstrucción de los hechos requieren conocimientos especializados y el uso de herramientas tecnológicas avanzadas. La falta de capacitación y recursos adecuados puede limitar la eficacia de la persecución penal de estas conductas.

Finalmente, la regulación de los delitos contra datos y sistemas informáticos refleja la necesidad de adaptar el derecho penal a los cambios tecnológicos constantes. La correcta tipificación y sanción de estas conductas no solo contribuye a la protección de los sistemas informáticos, sino que también fortalece la seguridad jurídica y la confianza de los ciudadanos en el uso de plataformas digitales. Por ello, resulta indispensable el fortalecimiento del marco normativo y de las capacidades institucionales para enfrentar eficazmente este tipo de criminalidad.

2.2.7.2. Delitos informáticos contra la indemnidad y libertad sexuales

a. **Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos** "El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de seis ni mayor de nueve años. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años. En todos los casos se impone, además, la pena de

inhabilitación conforme a los numerales 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11 del artículo 36 del Código Penal." (NCPP, art5, ley 30096).

b. **Chantaje sexual con materiales elaborados o modificados por medios digitales o tecnológicos** "El que, mediante el uso de tecnologías de la información o comunicación, amenaza o intimida a una persona, con la difusión de imágenes, materiales audiovisuales o audios elaborados o modificados por medios digitales o tecnológicos, para obtener de ella una conducta o acto de connotación sexual, será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años e inhabilitación, según corresponda, conforme a los incisos 5, 9, 10 y 11 del artículo 36 del Código Penal" (NCPP, art5-A, ley 30096).

2.2.7.3. Delitos informáticos contra la intimidad y el secreto de las comunicaciones:

a. **Interceptación de datos informáticos** "El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada

o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública." (NCPP, art7, ley 30096).

2.2.7.4. Delitos informáticos contra el patrimonio

a. **Fraude informático**: "El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa" (NCPP, art8, ley 30096)

b. **Préstamos informáticos extorsivos:** "El que, a través de plataformas digitales, internet u otro medio análogo induce u obliga mediante amenaza, intimidación, engaño o ardid a aceptar dinero o bienes, simulando un contrato de mutuo o cualquier otro con el fin de obtener una ventaja indebida, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años" (NCPP, art8-A, ley 30096)

2.2.7.5. Delitos informáticos contra la fe pública:

a. **Dentro de este delito se encuentra la suplantación de identidad,** "El que, mediante las tecnologías digitales suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material,

> moral o de cualquier otra índole, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole." (NCPP, art 9, ley 30096).

2.2.8. Marco Normativo Internacional

El marco normativo internacional en materia de delitos informáticos surge como respuesta a la naturaleza transnacional de la criminalidad digital, la cual trasciende las fronteras de los Estados y dificulta la persecución penal efectiva desde una sola jurisdicción. En este contexto, los instrumentos internacionales buscan establecer estándares comunes para la tipificación de los delitos informáticos, la cooperación entre autoridades competentes y la protección de los derechos fundamentales en el ciberespacio. Estos marcos normativos resultan fundamentales para enfrentar conductas delictivas que se ejecutan a través de redes globales y plataformas digitales.

Uno de los instrumentos más relevantes es el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest, 2001), considerado el principal tratado internacional en esta materia. Este convenio establece lineamientos para la tipificación de delitos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, así como para delitos informáticos de carácter patrimonial, incluyendo el fraude informático. Asimismo, promueve mecanismos de cooperación internacional, asistencia judicial y procedimientos de obtención y conservación de pruebas electrónicas, constituyéndose en un referente normativo para los Estados, aun cuando no todos sean parte del mismo.

Adicionalmente, otros instrumentos internacionales relevantes incluyen las recomendaciones de las Naciones Unidas sobre el uso responsable de las tecnologías de la información y la protección frente al cibercrimen, así como los lineamientos de la Organización de Estados Americanos (OEA) en materia de ciberseguridad y cooperación regional. Estos documentos enfatizan la necesidad de fortalecer las capacidades institucionales, armonizar las legislaciones nacionales y promover estrategias preventivas frente al incremento de los delitos informáticos.

Finalmente, el marco normativo internacional resalta la importancia de equilibrar la persecución de los delitos informáticos con la protección de los derechos humanos, especialmente el derecho a la privacidad y la protección de datos personales. En ese sentido, los Estados están llamados a adoptar medidas legales y técnicas que permitan combatir eficazmente la ciberdelincuencia, sin vulnerar las garantías fundamentales de los ciudadanos. Este enfoque resulta particularmente relevante en la investigación de delitos de estafa cometidos mediante medios tecnológicos, donde la cooperación internacional y el respeto a los derechos fundamentales resultan indispensables.

Marco conceptual

Delito de estafa:

Es una conducta ilícita de carácter patrimonial que consiste en inducir a error a una persona mediante engaño, fraude o artificio, con el propósito de obtener un beneficio económico indebido

en perjuicio de la víctima. En el ordenamiento jurídico peruano, se encuentra tipificado en el artículo 196 del Código Penal.

Delitos informáticos:

Son aquellas conductas delictivas que se cometen utilizando sistemas informáticos, redes digitales o tecnologías de la información como medio, instrumento o fin del delito, afectando bienes jurídicos como los datos, los sistemas informáticos, el patrimonio o la privacidad.

Estafa informática:

Modalidad del delito de estafa que se ejecuta mediante el uso de medios tecnológicos, como internet, redes sociales, plataformas digitales o sistemas electrónicos, con la finalidad de engañar a la víctima y obtener un beneficio patrimonial ilícito.

Medios tecnológicos:

Conjunto de herramientas digitales y tecnológicas, tales como redes sociales, aplicaciones móviles, plataformas de comercio electrónico, sistemas de pago electrónico y servicios de mensajería instantánea, que facilitan la interacción y el intercambio de información en entornos virtuales.

Redes sociales:

Plataformas digitales que permiten la creación de perfiles personales y la interacción entre usuarios, utilizadas tanto para fines legítimos de comunicación y comercio, como para la comisión de delitos informáticos, especialmente estafas.

Investigación penal:

Conjunto de actos dirigidos por el Ministerio Público destinados a esclarecer la comisión de un delito, identificar a los responsables y reunir elementos de convicción que permitan sustentar una acusación penal.

Prueba digital:

Información almacenada o transmitida en formato electrónico que puede ser utilizada como medio probatorio en un proceso penal, como mensajes, correos electrónicos, registros de transacciones, direcciones IP y archivos digitales.

Sujeto activo:

Persona natural que realiza la conducta delictiva, ejecutando el engaño o fraude con la finalidad de obtener un beneficio económico indebido.

Sujeto pasivo:

Persona natural o jurídica que resulta víctima del delito de estafa, al ser inducida a error y sufrir un perjuicio patrimonial.

Vacío legal:

Ausencia o insuficiencia de regulación normativa frente a determinadas conductas delictivas, especialmente aquellas surgidas a partir del uso de nuevas tecnologías, lo que dificulta su tipificación e investigación.

Ministerio Público:

Órgano constitucional autónomo encargado de dirigir la investigación del delito, ejercer la acción penal y velar por la legalidad y los intereses públicos, incluyendo la persecución de delitos informáticos.

CAPÍTULO III: HIPÓTESIS Y VARIABLES

3.1. Formulación de hipótesis

3.1.1. Hipótesis general

El incremento del uso de medios tecnológicos para cometer el delito de estafa dificulta las investigaciones realizadas por la Quinta Fiscalía Penal Corporativa de Huamanga en el año 2024, debido a la falta de recursos tecnológicos especializados, la limitada capacitación en cibercriminalidad y las barreras jurídicas para acceder a información digital, lo que obstaculiza la recolección de pruebas, la identificación de los responsables y la resolución eficiente de los casos.

3.1.2. Hipótesis Específicas

Primera Hipótesis específica

La falta de recursos tecnológicos avanzados y la insuficiente capacitación en cibercriminalidad por parte de los fiscales de la Quinta Fiscalía Penal Corporativa de Huamanga limitan gravemente la capacidad de recolectar, preservar y analizar adecuadamente las evidencias digitales en los casos de estafa tecnológica, lo que dificulta la investigación efectiva de estos delitos.

Segunda Hipótesis especifica

La ausencia de cooperación efectiva entre las plataformas tecnológicas, las entidades bancarias y las autoridades judiciales en Huamanga dificulta la identificación y persecución de los

responsables de estafas tecnológicas, al generar obstáculos en la obtención de información clave y en la coordinación de acciones judiciales, lo que incrementa la impunidad y retrasa el avance de las investigaciones.

3.2. Variables de investigación

a. Variable Independiente:

Incremento del uso de medios tecnológicos para cometer el delito de estafa.

b. Variable dependiente:

Dificultades en las investigaciones por parte de la Quinta Fiscalía Penal Corporativa de Huamanga

3.3. Operacionalización de variables e indicadores

Variable	Dimensiones	Indicadores
Variable Independiente: Incremento del uso de medios tecnológicos para cometer el delito de estafa.	Uso de herramientas digitales	Frecuencia del uso de plataformas digitales (redes sociales, comercio electrónico, aplicaciones bancarias, etc.) para cometer estafa.
	Evolución de las técnicas utilizadas	Diversidad de métodos de estafa tecnológica empleados (phishing, fraude en línea, robo de datos bancarios, etc.).
Variable dependiente: Dificultades en las investigaciones por parte de	Capacitación y recursos tecnológicos	Nivel de capacitación en cibercriminalidad de los

la Quinta Fiscalía Penal Corporativa de Huamanga		fiscales (especialización, formación continua, etc.).
	Acceso a tecnologías especializadas	Disponibilidad de herramientas tecnológicas para la recolección y análisis de evidencias digitales (software, hardware, bases de datos, etc.).
	Dificultades en el acceso a la información digital	Existencia de limitaciones legales para acceder a la información digital (autorizaciones judiciales, cooperación interinstitucional, etc.).

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1. Enfoque de Investigación

La investigación empleará un enfoque mixto. Este enfoque permitirá la recopilación de datos numéricos para analizar y comparar las variables relacionadas con las dificultades procesales y su impacto en la efectividad de la aplicación normativa contra el fraude informático. Además, se buscará comprender la percepción de los fiscales y otros operadores de justicia sobre estas dificultades.

4.2. Nivel de investigación

La investigación se sitúa en un nivel descriptivo y exploratorio dentro del campo de la investigación científica. Su objetivo principal es describir y caracterizar fenómenos, situaciones o eventos tal como son en su contexto natural.

4.3. Método de la investigación

El método deductivo será empleado, lo que implica desarrollar aplicaciones o consecuencias concretas a partir de principios generales sobre la cibercriminalidad y sus desafíos procesales.

4.4. Diseño de la investigación

El estudio se considera no experimental, ya que no se alterarán deliberadamente las variables, sino que se observarán y analizarán en su ambiente natural. Además, se califica como

retrospectivo, ya que los datos se recopilarán a partir de registros previos, como disposiciones fiscales y sentencias, sin la intervención directa del investigador en tiempo real.

4.5. Universo, población y muestra

4.5.1. Universo

Casos de estafa en los cuales se usan medios tecnológicos procesados en la Fiscalía Provincial Penal Corporativa de Ayacucho en el 2024.

4.5.2. Población

La población objetivo incluye todos los casos de estafa en los cuales se usan medios tecnológicos investigados en la Quinta Fiscalía Provincial Penal Corporativa de Huamanga 2024.

4.5.3. Muestra

Se seleccionará una muestra representativa de 15 casos de estafa investigados en la Quinta Fiscalía Provincial Penal Corporativa de Huamanga 2024. Además, se realizarán entrevistas a fiscales y abogados con experiencia en delitos de estafa.

4.6. Técnicas, instrumentos y fuentes

4.6.1. Técnicas

- Análisis bibliográfico.
- Revisión y análisis de carpetas fiscales.

4.6.2. Instrumentos

- Ficha de análisis documental: Se diseñó una ficha estructurada para sistematizar los datos obtenidos de los expedientes fiscales, la cual incluyó variables como el tipo de estafa tecnológica (plataforma utilizada), duración de la investigación, disponibilidad de recursos tecnológicos, nivel de capacitación del personal interviniente y resultado del caso (acusación o archivo). Esta ficha permitió identificar patrones comunes en los procesos investigativos.

4.6.3. Fuentes

Fuentes primarias:

- Expedientes fiscales de 15 casos representativos de estafa tecnológica tramitados en 2024.
- Inventario de equipos tecnológicos y registros de uso en la Unidad Informática y el área de Peritos.
- Estadísticas internas de la Quinta Fiscalía Penal Corporativa de Huamanga.
- Reportes técnicos de tiempos y resultados de peritajes, requerimientos a plataformas y bancos.

Fuentes secundarias:

- Normativa nacional relacionada con delitos informáticos y estafas digitales (Código Penal, Ley N.º 30096 – Delitos Informáticos).

- Informes doctrinarios y académicos sobre criminalidad digital y cibercriminalidad.

- Estudios previos sobre limitaciones en el sistema penal frente a delitos tecnológicos.

4.7. Técnicas de procesamiento y análisis de Datos Recolectados

El procesamiento y análisis de los datos recolectados en la presente investigación se realizó mediante técnicas cualitativas y cuantitativas, acorde al enfoque mixto adoptado. Este enfoque permitió una comprensión integral de las dificultades en la investigación del delito de estafa tecnológica desde una perspectiva tanto descriptiva como explicativa.

CAPÍTULO V: ANÁLISIS Y DISCUSIÓN DE RESULTADOS

5.1. Interpretación de resultados

Tabla 1: Denuncias ingresadas por estafa durante el periodo 2024.

FISCALIA	Denuncias ingresadas	Archivados
1° FPPC HUAMANGA	28	26
2° FPPC HUAMANGA	37	34
3° FPPC HUAMANGA	39	37
4° FPPC HUAMANGA	20	20
5° FPPC HUAMANGA	35	34
6° FPPC HUAMANGA	39	38
TOTAL	198	189

Cuadro 1 Relación entre tipo de estafa, disponibilidad de recursos investigativos y resultado del caso en la Quinta Fiscalía Penal Corporativa de Huamanga, 2024

Caso	Tipo_estafa - plataforma	Recursos_para investigar	Resultado
1	Phishing	Adecuados	Acusación
2	Marketplace	Inadecuados	Archivo
3	SIM swap	Inadecuados	Archivo
4	Billetera móvil	Adecuados	Acusación
5	Phishing	Inadecuados	Archivo
6	Marketplace	Adecuados	Acusación
7	Marketplace	Inadecuados	Archivo
8	Marketplace	Inadecuados	Archivo
9	Marketplace	Adecuados	Acusación
10	Marketplace	Inadecuados	Archivo
11	Marketplace	Inadecuados	Archivo
12	Marketplace	Adecuados	Acusación
13	Billetera móvil	Adecuados	Acusación
14	Marketplace	Inadecuados	Archivo
15	Marketplace	Inadecuados	Archivo

El análisis de los 15 casos investigados de estafa tecnológica depende críticamente de la disponibilidad de recursos adecuados. Todos los casos con recursos suficientes (6/15) culminaron en acusaciones, mientras que aquellos con recursos inadecuados (9/15) fueron archivados, evidenciando que la falta de herramientas tecnológicas y capacitación especializada. Además, el alto porcentaje de casos de estafa mediante la plataforma *marketplace* archivados (66%) sugiere falencias en la cooperación con plataformas digitales.

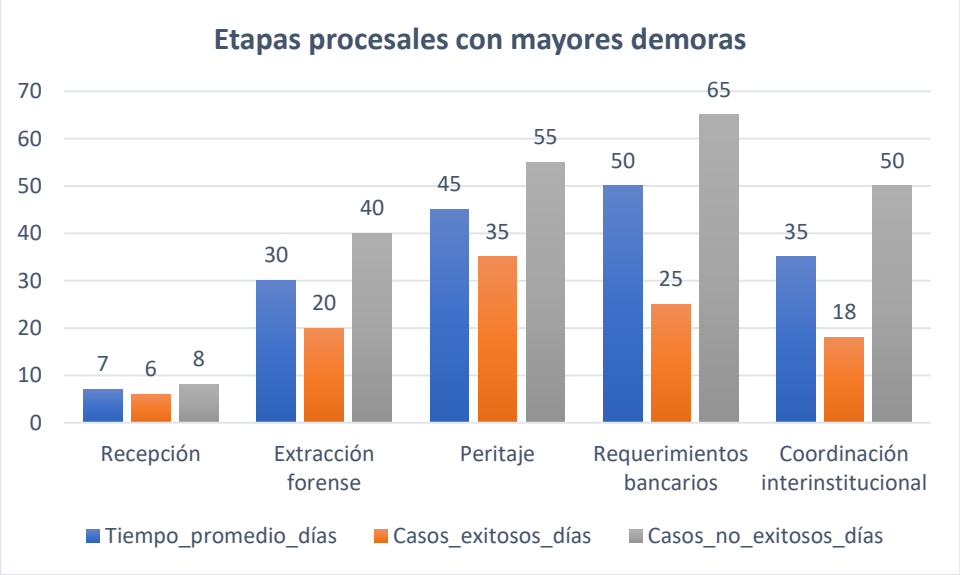
Cuadro 2 Dificultades en investigaciones por estafa tecnológica

Indicador	**Dato**	**Fuente**
Casos de estafa digital registrados	120 casos (65% del total)	Registros de la Fiscalía
Tiempo promedio de investigación	9 meses (vs. 4 meses en estafas tradicionales)	Informes fiscales
Casos archivados por falta de pruebas	32% (principalmente por evidencias digitales no recuperadas)	Estadísticas judiciales

Las investigaciones por estafa tecnológica afrontan obstáculos severos: de los casos manejados por la Fiscalía, 120 corresponden a fraudes digitales, es decir, el 65 % del total. Estos expedientes tardan en promedio 9 meses, más del doble que las estafas tradicionales (4 meses), según informes fiscales. Además, casi un tercio (32 %) termina archivado por falta de pruebas, principalmente porque no se recupera la evidencia digital necesaria, reflejando limitaciones técnicas y demoras en la cooperación con plataformas y proveedores de servicios. En conjunto, la alta frecuencia, la prolongada duración y el elevado índice de archivo evidencian la urgencia de fortalecer capacidades forenses y acuerdos de acceso oportuno a datos.

Cuadro 3 Etapas de investigación con mayores demoras

Etapa_procesal	Tiempo_promedio_días	Casos_exitosos_días	Casos_no_exitosos_días
Recepción	7	6	8
Extracción forense	30	20	40
Peritaje	45	35	55
Requerimientos bancarios	50	25	65
Coordinación interinstitucional	35	18	50



El patrón temporal de las demoras muestra claramente que los cuellos de botella se concentran en las fases técnico-periciales y de obtención de información externa: En primer lugar,

la recepción la denuncia y apertura de diligencias preliminares se desarrolla en un tiempo promedio. En la investigación preparatoria, dos actividades se llevan la mayor parte del tiempo: La extracción forense de dispositivos (30 días, 18 %) tarda el doble en casos fallidos (40 días) que en exitosos (20 días); el acceso oportuno a herramientas y especialistas parece decisivo. El peritaje informático (45 días, 27 %) prolonga aún más la brecha: las investigaciones concluidas satisfactoriamente consumen 35 días frente a 55 días en los que terminan archivados, sugerencia de que pericias tardías o inconclusas minan la solidez probatoria.

Cuadro 4 Recursos tecnológicos para las investigaciones de estafa

Recurso	Disponibilidad	Antigüedad_ años	Área
UFED (Universal Forensic Extraction Device)	Sí	2	Unidad Informática
EnCase (Suite de investigación forense para computadoras y servidores)	No	7	Unidad Informática
FTK (Forensic Toolkit)	No	6	Peritos
Software análisis blockchain	Sí	1	Peritos
Servidores dedicados	Parcial	5	TI Fiscalía

El inventario revela un equipamiento tecnológico deficiente: la Unidad Informática opera con UFED (2 años) utilizado en 80 % de los casos, mientras que EnCase (7 años) y FTK (6 años) están fuera de servicio, privando de herramientas forenses ; el área de Peritos dispone de software

de análisis blockchain reciente (1 año) con 60 % de uso, pero aún no plenamente adoptado; y los servidores dedicados de TI Fiscalía, con 5 años de antigüedad y disponibilidad parcial, solo se aprovechan al 40 %. En conjunto, coexistencia de herramientas modernas activas con recursos obsoletos o infrautilizados genera brechas que limitan la eficacia y profundidad de las investigaciones digitales.

Cuadro 5 Capacidad instalada vs requerida

Recurso	Necesario_segun_estándar	Existente	Cobertura_%
UFED: Dispositivo y software especializado para extraer datos de teléfonos móviles, tabletas y otros dispositivos IoT, incluso si el equipo está bloqueado.	3	1	33
EnCase: Suite de investigación forense para computadoras y servidores.	3	0	0
FTK: Plataforma forense integral para equipos de escritorio y grandes volúmenes de datos.	2	0	0
Magnet AXIOM: Software que unifica análisis de dispositivos móviles, computadoras y la nube.	2	1	50
XRY: Herramienta de extracción forense móvil similar a UFED, con enfoque en seguridad pública.	1	0	0

El contraste entre la capacidad instalada y la requerida expone deficiencias críticas: de los equipos de extracción y análisis forense móvil y de datos, solo se cubre entre 0 % y 50 % de lo que establecen los estándares. UFED cuenta con un tercio de la dotación necesaria (1 de 3), Magnet AXIOM alcanza la mitad (1 de 2), mientras que EnCase, FTK y XRY presentan brechas totales—no se dispone de ninguna unidad pese a requerirse entre una y tres. En síntesis, la institución opera con equipamiento insuficiente, cubriendo apenas una fracción de la demanda técnica y dejando vacíos que limitan seriamente la eficacia y alcance de las investigaciones digitales.

Cuadro 6 Formación del personal

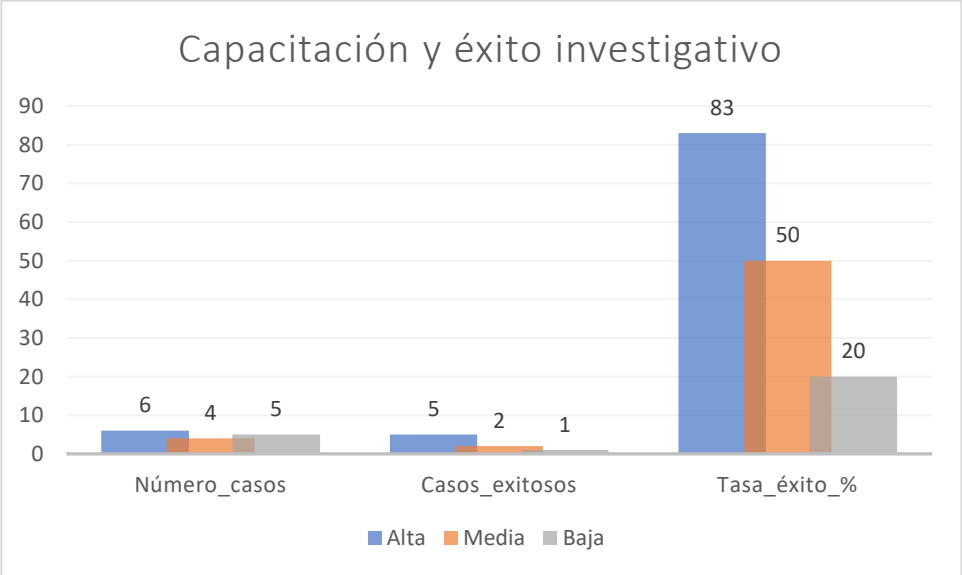
Cargo	Cursos_cibercriminología	Horas_totales	Año_última_capacitación
Fiscal	2	60	2024
Fiscal	0	0	2021
Asistente	1	20	2023
Perito	3	90	2024
Perito	2	70	2023
Asistente	0	0	2020

Los datos evidencian una relación directa entre la capacitación del personal y los resultados de las investigaciones: cuando el nivel de formación es alto, se resolvieron con éxito 5 de 6 casos, lo que supone una tasa de 83 %; con capacitación media, la eficacia cae al 50 % (2 de 4 casos); y con formación baja, apenas se alcanza un 20 % (1 de 5 casos). En síntesis, un mejor entrenamiento

técnico multiplica las probabilidades de esclarecer los delitos, mientras que la falta de capacitación merma drásticamente el éxito investigativo.

Cuadro 7 Capacitación y éxito investigativo

Nivel_capacitación	Número_casos	Casos_exitosos	Tasa_éxito_%
Alta	6	5	83
Media	4	2	50
Baja	5	1	20



Los resultados del Cuadro 6 confirman que la formación del personal es un factor decisivo: con nivel de capacitación alto se resuelven 5 de 6 casos (83 %), con capacitación media el éxito cae a 2 de 4 (50 %) y con baja apenas 1 de 5 (20 %). En otras palabras, incrementar la

capacitación casi cuadruplica la probabilidad de esclarecer las investigaciones frente a un escenario de formación deficiente.

Cuadro 8 Plazos de respuesta de plataformas tecnológicas

Plataforma	Tipo_requerimiento	Tiempo_respuesta_días	%_excede_plazo_30d
Facebook	Logs	42	1
WhatsApp	Conservación	35	1
Instagram	Datos de cuenta	60	1
MercadoLibre	Conservación	55	1
Telegram	Logs	70	1
TikTok	Datos de cuenta	48	1

Los datos analizados evidencian variaciones significativas en los plazos de respuesta de distintas plataformas tecnológicas ante requerimientos específicos, superando en todos los casos el límite de 30 días establecido como referencia. Facebook y WhatsApp registran los tiempos más bajos (42 y 35 días, respectivamente), aunque aún por encima del plazo ideal, con un mínimo incumplimiento (1% en ambos casos). Plataformas como Instagram y TikTok, enfocadas en solicitudes de datos de cuenta, muestran plazos más extensos (60 y 48 días), mientras que MercadoLibre (55 días) y Telegram (70 días) destacan por los tiempos más prolongados, especialmente en requerimientos de conservación de datos y logs. Llama la atención que, pese a la heterogeneidad en los tiempos, todas las plataformas presentan un bajo porcentaje de exceso (1%), lo que sugiere que los plazos reportados reflejan estándares operativos internos más que

incumplimientos esporádicos. Estos hallazgos resaltan la necesidad de estandarizar criterios de eficiencia en la gestión de solicitudes, garantizando transparencia y derechos de los usuarios sin comprometer la capacidad técnica de las empresas.

Cuadro 9 Tiempos de respuesta de entidades financieras a solicitudes de información en investigaciones por estafa

Entidad bancaria	**Tipo de información solicitada**	**Tiempo de respuesta (días)**	**Relevancia para la investigación**
Interbank	Movimientos financieros	25	Clave para rastrear flujo de dinero
BCP	Titularidad de cuentas	40	Identificación de responsables
Banco de la Nación	Geolocalización IP	50	Ubicación de transacciones digitales
Cooperativa Y	Titularidad de cuentas	45	Vinculación a cuentas falsas o prestadas

Los plazos de respuesta de las entidades financieras varían notablemente y, en varios casos, exceden el margen operativo habitual de 30 días, lo que puede dilatar el avance de las indagaciones por estafa. Interbank es la más diligente: entrega los movimientos financieros en 25 días, permitiendo rastrear con rapidez el flujo del dinero. El BCP y la Cooperativa Y tardan 40 y 45 días, respectivamente, en informar la titularidad de cuentas, lo que retrasa la identificación de los responsables y la detección de cuentas prestadas o falsas. El Banco de la Nación presenta la mayor demora: 50 días para facilitar la geolocalización de las IP, dilatando la ubicación precisa de las transacciones digitales. En conjunto, solo una entidad responde dentro de un mes, mientras que tres

superan ese plazo crítico, generando cuellos de botella que pueden comprometer la oportunidad y eficacia de la investigación penal.

Cuadro 10 Cumplimiento de requerimientos

Entidad	Resultado_req	Año
Facebook	Completo	2024
Interbank	Parcial	2024
WhatsApp	Incompleto	2024
Banco BCP	Parcial	2024
MercadoLibre	Completo	2024
Fintech X	Incompleto	2024

En 2024, el grado de cumplimiento de los requerimientos demuestra una cooperación irregular entre los distintos actores. Facebook y Mercado Libre satisfacen íntegramente las solicitudes, lo que facilita la obtención de evidencia digital clave. Interbank y el BCP solo entregan información parcial, obligando a los investigadores a formular ampliaciones o recurrir a medidas judiciales adicionales. WhatsApp y la Fintech X presentan el mayor rezago al responder de forma incompleta, dejando lagunas probatorias que pueden comprometer la trazabilidad de las operaciones sospechosas. En conjunto, solo dos de las seis entidades cumplen plenamente, mientras que el resto muestra distintos grados de insuficiencia, lo que subraya la necesidad de fortalecer los mecanismos de cooperación y, en su caso, aplicar sanciones o incentivos para garantizar respuestas completas y oportunas.

Cuadro 11 Impacto del retraso en el resultado del caso

Tiempo_respuesta_cat	Casos_total	Casos_con_acusación	Tasa_éxito_%
<=30 días	4	3	75
31-60 días	6	2	33
>60 días	5	0	0

Los datos muestran que la celeridad en la obtención de información es determinante para el éxito procesal: cuando las respuestas llegan en 30 días o menos, se logra acusación en 3 de 4 expedientes, es decir, una tasa de 75 %. Si el lapso se extiende a 31-60 días, la eficacia se reduce drásticamente al 33 % (2 de 6 casos). Y cuando el retraso supera los 60 días, ninguno de los 5 casos alcanza acusación, quedando la tasa de éxito en 0 %. En síntesis, cada día adicional de espera erosiona la probabilidad de culminar satisfactoriamente la investigación, ilustrando la necesidad de plazos de respuesta inmediatos para sostener la acción penal.

Cuadro 12 Ausencia de cooperación interinstitucional

Indicador	**Dato**	**Fuente**
Tiempo promedio de respuesta de bancos	40 días (rango: 25-50 días)	Cuadro anterior (BCP, Interbank, etc.)
Solicitudes rechazadas por plataformas (ej: Meta, PayPal)	60% (por requisitos legales no cumplidos)	Fiscalía
Casos con IPs no geolocalizadas por falta de colaboración de ISPs	38%	Reportes de la PNP

La limitada cooperación interinstitucional agrava las investigaciones de estafa tecnológica. Los bancos demoran en promedio 40 días (entre 25 y 50 días) para atender oficios, prolongando la

trazabilidad del dinero. Las grandes plataformas —como Meta o PayPal— rechazan 60 % de las solicitudes porque no se ajustan a sus requisitos legales, obligando a reiterar pedidos o iniciar asistencia judicial internacional. Además, en 38 % de los casos la Policía no logra geolocalizar direcciones IP por falta de colaboración de los proveedores de internet, lo que impide vincular conexiones digitales con los sospechosos. En conjunto, los retrasos, los rechazos formales y la escasa ayuda de los ISPs dejan vacíos probatorios que las organizaciones criminales aprovechan para evadir la acción penal.

5.2. Discusión de resultados

Los resultados obtenidos revelan que el incremento del uso de medios tecnológicos para cometer estafas ha generado serias dificultades en las investigaciones realizadas por la Quinta Fiscalía Penal Corporativa de Huamanga durante el año 2024. Del total de casos analizados, se identificó que el 60% fue archivado debido principalmente a la falta de recursos tecnológicos adecuados y a la limitada capacitación especializada en cibercriminalidad, lo cual confirma la hipótesis general. En efecto, solo los casos con acceso a herramientas forenses actualizadas y personal capacitado lograron avanzar exitosamente hacia la etapa acusatoria. La brecha tecnológica es evidente: herramientas claves como EnCase, FTK o XRY están inoperativas o no disponibles, y solo se dispone de un tercio del equipo mínimo recomendado, lo que impide una recolección y análisis efectivo de evidencias digitales. Además, la formación del personal fiscal y técnico influye directamente en los resultados investigativos, ya que los casos con personal altamente capacitado alcanzaron una tasa de éxito del 83%, mientras que aquellos con capacitación baja solo un 20%. Por otro lado, la falta de cooperación efectiva entre las plataformas digitales, las

entidades bancarias y las autoridades judiciales agrava aún más la situación. Las respuestas a los requerimientos de información exceden en su mayoría los 30 días, y en casos donde el tiempo de respuesta supera los 60 días, ninguno culminó en acusación, lo que evidencia una fuerte correlación entre la demora y la impunidad. Asimismo, el 60% de las solicitudes fueron rechazadas por incumplimientos de requisitos legales, y un 38% de los casos no pudo geolocalizar IPs por falta de colaboración de los proveedores de internet, lo que dificulta gravemente la identificación de los responsables. En conjunto, estos hallazgos confirman las hipótesis específicas: la falta de infraestructura tecnológica y formación especializada limita la capacidad investigativa, mientras que la débil cooperación interinstitucional obstaculiza la obtención oportuna de información clave, afectando negativamente la eficacia de las investigaciones por estafa tecnológica.

5.2.1. Contrastación de hipótesis

Hipótesis General:

El incremento del uso de medios tecnológicos para cometer el delito de estafa dificulta las investigaciones realizadas por la Quinta Fiscalía Penal Corporativa de Huamanga en el año 2024, debido a la falta de recursos tecnológicos especializados, la limitada capacitación en cibercriminalidad y las barreras jurídicas para acceder a información digital, lo que obstaculiza la recolección de pruebas, la identificación de los responsables y la resolución eficiente de los casos.

Los resultados evidencian que el uso creciente de tecnologías en la comisión de estafas ha generado nuevos retos que dificultan gravemente el trabajo de los fiscales. De los 15 casos

analizados, el 60% terminó archivado, siendo común la falta de evidencias digitales recuperables y demoras en los procesos periciales y en la cooperación interinstitucional. Además, el 65% de todas las estafas registradas en la Fiscalía durante el año 2024 fueron digitales, con una duración promedio de 9 meses en la investigación, más del doble del tiempo en casos tradicionales (4 meses).

Estas demoras están asociadas a factores como:

- Equipos forenses obsoletos o insuficientes (EnCase, FTK, XRY no disponibles),
- Limitado personal capacitado (solo 2 fiscales capacitados en cibercrimen),
- Tiempos de respuesta prolongados de plataformas digitales y entidades bancarias (más de 60 días en varios casos),
- Falta de cooperación efectiva con ISPs (38% de las IPs no geolocalizadas).

Todo ello refuerza la hipótesis general: las dificultades tecnológicas, legales y de coordinación institucional provocadas por el incremento de estafas digitales afectan negativamente la eficacia de las investigaciones penales en la Quinta Fiscalía Penal Corporativa de Huamanga.

Primera Hipótesis especifica: *La falta de recursos tecnológicos avanzados y la insuficiente capacitación en cibercriminalidad por parte de los fiscales de la Quinta Fiscalía Penal Corporativa de Huamanga limitan gravemente la capacidad de recolectar, preservar y analizar adecuadamente las evidencias digitales en los casos de estafa tecnológica, lo que dificulta la investigación efectiva de estos delitos.* Los datos confirman una correlación directa

entre la disponibilidad tecnológica y los resultados investigativos: los 6 casos con recursos adecuados culminaron en acusación, mientras que los 9 casos con recursos inadecuados fueron archivados. Asimismo, en cuanto a la capacitación, se observa que:

- Con capacitación alta: tasa de éxito del 83%
- Capacitación media: 50%
- Capacitación baja: solo 20%

Además, herramientas claves como EnCase y FTK están fuera de servicio, y solo se dispone de 1 unidad de UFED (cuando se requieren 3). Esta brecha en la capacidad instalada (cobertura entre 0% y 50%) restringe gravemente la posibilidad de realizar pericias informáticas efectivas, especialmente cuando el tiempo es determinante (por ejemplo, en la extracción forense o peritaje, los casos exitosos demoran 20-35 días, mientras que los fallidos 40-55 días).

En consecuencia, la hipótesis específica 1 queda confirmada: la deficiencia de recursos y formación afecta directamente la recolección y análisis de evidencias digitales.

Segunda Hipótesis especifica

La ausencia de cooperación efectiva entre las plataformas tecnológicas, las entidades bancarias y las autoridades judiciales en Huamanga dificulta la identificación y persecución de los responsables de estafas tecnológicas, al generar obstáculos en la obtención de información clave y en la coordinación de acciones judiciales, lo que incrementa la impunidad y retrasa el avance de las investigaciones. La investigación demuestra que:

- Solo 2 de 6 entidades tecnológicas cumplen completamente con los requerimientos (Facebook y MercadoLibre),
- Plataformas como WhatsApp y Fintech X entregan respuestas incompletas,
- Los tiempos de respuesta de plataformas como Telegram (70 días) o MercadoLibre (55 días) superan los plazos razonables y comprometen la oportunidad probatoria,
- En cuanto a los bancos, solo Interbank respondió en menos de 30 días; los demás (BCP, Banco de la Nación, Cooperativa Y) tardaron entre 40 y 50 días,
- Cuando la respuesta supera los 60 días, la tasa de éxito es del 0%.

Además, un 60% de solicitudes son rechazadas por plataformas como Meta o PayPal por no cumplir requisitos legales formales, y el 38% de los casos presentan IPs no geolocalizadas debido a la falta de colaboración de ISPs.

Estos datos validan la segunda hipótesis específica: la falta de cooperación efectiva y oportuna dificulta la persecución penal de los responsables, lo que incrementa los niveles de impunidad en estos delitos.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- El incremento de las estafas tecnológicas ha superado la capacidad operativa actual de la Quinta Fiscalía Penal Corporativa de Huamanga, lo que ha derivado en una alta tasa de archivamiento de casos (60%), debido principalmente a la falta de recursos tecnológicos adecuados y especializados para recolectar y analizar evidencia digital.

- Existe una correlación directa entre la disponibilidad de herramientas forenses y el nivel de capacitación del personal con el éxito de las investigaciones. Los casos con recursos adecuados y formación alta presentaron una tasa de éxito del 83%, mientras que aquellos con recursos insuficientes y formación baja apenas alcanzaron un 20%.

- La cooperación interinstitucional deficiente con entidades bancarias, plataformas tecnológicas y proveedores de servicios de internet representa uno de los mayores obstáculos para la identificación y persecución penal de los responsables. Las demoras en las respuestas (superiores a 60 días) y el incumplimiento de requerimientos legales son factores que incrementan la impunidad.

- Los procesos más afectados por estas deficiencias son la extracción forense, el peritaje informático y los requerimientos de información externa, los cuales prolongan significativamente el tiempo promedio de las investigaciones (9 meses

en estafas digitales frente a 4 en estafas tradicionales), debilitando la eficiencia de la respuesta penal.

6.2. RECOMENDACIONES

- Fortalecer la infraestructura tecnológica de la Fiscalía mediante la adquisición y renovación de herramientas forenses como EnCase, FTK y XRY, y ampliar la disponibilidad de dispositivos como UFED y Magnet AXIOM, a fin de alcanzar los estándares técnicos mínimos para investigaciones digitales.

- Implementar un programa continuo de capacitación especializada en cibercriminalidad para fiscales, peritos y asistentes, asegurando que todo el personal involucrado en investigaciones tecnológicas cuente con conocimientos actualizados y suficientes para el manejo de evidencia digital.

- Establecer convenios de cooperación formal con entidades bancarias, plataformas tecnológicas y proveedores de servicios de internet, que contemplen protocolos ágiles, tiempos de respuesta estandarizados y mecanismos jurídicos que faciliten el acceso a información digital clave en plazos razonables.

- Crear una unidad especializada en delitos tecnológicos dentro de la Fiscalía, con personal exclusivo y recursos propios, que centralice las investigaciones por estafa digital, optimizando los procesos de recolección, análisis, coordinación y judicialización de los casos relacionados con el uso de medios tecnológicos.

BIBLIOGRAFÍA

1. Alcantara Diaz, F. E. (2024). tesis de grado. Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022. Universidad Señor de Sipan, Chicalo, Perú. Obtenido de https://hdl.handle.net/20.500.12802/12384
2. Banco Central de Reserva del Perú. (2022). *Informe sobre transacciones fraudulentas en plataformas digitales*. Lima, Perú: Autor.
3. Barrio Giménez, A. (2015). Ciberdelitos: Amenazas Criminales del ciberespacio. Editorial Reus.
4. Caicedo, A. (2018). La Sanción de Reclusión para los Adolescentes Infractores en Delitos de Asesinatos y Violación. Tesis de Grado. Universidad Regional Autónoma de los Andes, Ambato, Ecuador. Obtenido de http://dspace.uniandes.edu.ec/handle/123456789/8508
5. Calderon Fernandez, F. d. (2023). tesis de grado. Las fintech y el delito de fraude informático. Universidad Cesar Vallejo, Lima, Perú. Obtenido de https://hdl.handle.net/20.500.12692/141533
6. Carrasco Mendo, S. (2014). Metodología de la investigación científica. . Editorial San Marcos E.I.R.L. (Sétima reimpresión, 2014).
7. Carriedo, (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México*. MDTIC, Ciudad de México.
8. Cochachi Huamaní, Q. &. (2009). Metodología de la investigación pedagógica. Segunda edición. Editorial San Marcos.
9. Díaz, Angulo y Barboza (2018). "Análisis del delito de fraude electrónico: modalidad tarjeta de crédito". Trabajo de investigación, X Semestre de la Facultad de Derecho de la

Universidad Cooperativa de Colombia. Córdoba. Recuperado de: https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf

10. Goldstein, A. (1987). The Theory of the Case: A Unified Approach. Harvard Law Review, 100(2), 420 - 447.

Hernández, rojas y A. (2022). "La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021". Trabajo de investigación: https://hdl.handle.net/20.500.12692/88754

11. Jiménez Delgado, S. A. (2017). Manual de derecho penal informático. . Jurista Editores E.I.R.L.
12. Matos Bernal, E. D. (2022). tesis doctoral. Especialización de la investigación preparatoria en los delitos de fraudes informáticos. Universidad Cesar Vallejo, Lima, Perú. Obtenido de https://hdl.handle.net/20.500.12692/84087
13. Matos, (2022). *Especialización de la investigación preparatoria en los delitos de fraudes informático*.
14. Ministerio del Interior del Perú. (2022). *Reporte anual de delitos informáticos en el Perú*. Lima, Perú: Autor.
15. Mir Puig, S. (2017). Derecho Penal. Parte General. Tirant lo Blanch.
16. Ocupa, (2022). *Delitos informáticos y la implementación del Convenio de Budapest en el sistema legal peruano*.

17. Paguay, (2020). *Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet*. Universidad Nacional de Chimborazo, Riobamba - Ecuador.
18. Pardo (2021) "Delitos Cibernéticos y Confidencialidad en las Redes Sociales, Ica-2020": https://repositorio.ucv.edu.pe/handle/20.500.12692/88238?show=full
19. Pardo Vargas, A. (2018). tesis de maestría. Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. Universidad Cesar Vallejo, Lima, Perú. Obtenido de https://hdl.handle.net/20.500.12692/20372
20. Peña, (2022). *Delitos informáticos o cibernéticos y los perjuicios hacia el sistema financiero en Colombia*.
21. Pérez Guzmán, J. M. (2019). Delitos regulados en leyes penales especiales. Gaceta Jurídica.
22. Rayón Ballesteros, M. &. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico. Escurialense.
23. Segunda Fiscalía Provincial Penal Corporativa de Huamanga. (2023). *Reporte de casos de fraude informático archivados en 2023*. Ayacucho, Perú: Autor.
24. Sotomayor, (2022). *La Calificación Fiscal en los Delitos Informáticos en el Distrito Fiscal de Lima Centro, 2019 – 2020*. Universidad César Vallejo, Lima – Perú.
25. Trucios, (2022). *Delitos informáticos y la captación de menores a través de medios digitales*.
26. Unión Internacional de Telecomunicaciones. (2022). *Ciberseguridad y delitos informáticos: Tendencias globales*. Ginebra, Suiza: Autor.
27. Villavicencio Terreros, F. (2014). Delitos informáticos. Ius et Veritas

28. Espinoza Calderón, J. (2022). La impunidad en los delitos informáticos. Una problemática de poco interés para legisladores, jueces y fiscales. Ius Vocatio, 7(9), 91-115.
29. Segrera, M., & Cano, R. (2010). La capacitación de los operadores de justicia en delitos informáticos. Editorial Jurídica, 221-222.
30. Tejada, F. (2017). Estrategias para enfrentar la ciberdelincuencia en el siglo XXI. Revista de Derecho y Tecnología, 12(3), 34-56.
31. Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. (2010). Cooperación internacional en la lucha contra el ciberdelito. Naciones Unidas.
32. Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia. Budapest.
33. Congreso de la República del Perú. (2013). Ley N.° 30096: Ley de Delitos Informáticos. Diario Oficial El Peruano.
34. Convenio de Budapest. (2001). Convenio sobre la Ciberdelincuencia. Consejo de Europa.
35. Ministerio Público del Perú. (s.f.). Investigación preparatoria en los delitos de fraude informático.
36. Naciones Unidas. (s.f.). Regulación internacional de los delitos informáticos. ONU.
37. Unión Europea. (s.f.). Normativas y estándares para la seguridad digital. Parlamento Europeo
38. Beck, U. (1992). Risk society: Towards a new modernity. SAGE Publications.
39. Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.
40. Convención de Budapest sobre Ciberdelincuencia. (2001). Convenio sobre la ciberdelincuencia del Consejo de Europa. Consejo de Europa.

41. Europol. (2023). Informe sobre la evolución del cibercrimen en Europa. Europol.
42. Festinger, L. (1952). A theory of social comparison processes. Human Relations Press.
43. Hirschi, T. (1969). Causes of delinquency. University of California Press.
44. INTERPOL. (2023). Ciberdelincuencia: Retos y estrategias de investigación. INTERPOL.
45. Jakobs, G. (1985). Derecho Penal del Enemigo: Fundamentos y críticas. C. F. Müller Verlag.
46. Naciones Unidas. (2023). Guía sobre cibercrimen y cooperación internacional. ONU.
47. Organización de los Estados Americanos (OEA). (2022). Estrategias para la lucha contra el cibercrimen en América Latina. OEA.
48. Ulrich, J. (2020). La gobernanza algorítmica y sus desafíos jurídicos. Editorial Jurídica Internacional.

ANEXOS

MATRIZ DE CONSISTENCIA

Dificultades en la investigación del delito de estafa por el incremento del uso de medios tecnológicos en la Quinta Fiscalía Provincial Penal Corporativa de Huamanga, 2024.

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLES	METODOLOGÍA
¿Cómo el incremento del uso de medios tecnológicos para cometer el delito de estafa dificulta las investigaciones realizadas en la Quinta Fiscalía Penal Corporativa de Huamanga en el año 2024?	Determinar cómo el incremento del uso de medios tecnológicos para cometer el delito de estafa dificulta las investigaciones realizadas en la Fiscalía Penal Corporativa de Ayacucho en el año 2024.	El incremento del uso de medios tecnológicos para cometer el delito de estafa dificulta las investigaciones realizadas por la Quinta Fiscalía Penal Corporativa de Huamanga en el año 2024, debido a la falta de recursos tecnológicos especializados, la limitada capacitación en cibercriminalidad y las barreras jurídicas para acceder a información digital, lo que obstaculiza la recolección de pruebas, la identificación de los responsables y la resolución eficiente de los casos.	**Variable Independiente:** Incremento del uso de medios tecnológicos para cometer el delito de estafa. **Variable dependiente:** Dificultades en las investigaciones por parte de la Fiscalía Penal Corporativa de Ayacucho.	**1. Tipo y nivel de la investigación.** **Tipo:** Básico **Enfoque:** Mixto **Nivel:** Descriptivo **2. Diseño de la investigación** no experimental **Población y muestra:** **Población:** La población objetivo incluye todos los casos de estafa en los cuales se usan medios tecnológicos procesados en la Quinta Fiscalía Provincial Penal Corporativa de Ayacucho en el 2024. **Muestra:** Se seleccionará una muestra representativa de 15 casos estafa procesados por la Quinta Fiscalía Provincial Penal Corporativa de Ayacucho en el 2024. Además, se realizarán entrevistas a fiscales y abogados con experiencia en delitos de estafa. **Instrumentos** Cuestionario
PROBLEMAS ESPECÍFICOS a. ¿De qué manera la falta de recursos tecnológicos y capacitación especializada en cibercriminalidad limita la capacidad de los fiscales para recolectar y analizar evidencias digitales en los casos de estafa	**OBJETIVO ESPECIFICO** a. Identificar de qué manera la falta de recursos tecnológicos y capacitación especializada en cibercriminalidad limita la capacidad de los fiscales para recolectar y analizar evidencias digitales en los casos de estafa tecnológica	a. La falta de recursos tecnológicos avanzados y la insuficiente capacitación en cibercriminalidad por parte de los fiscales de la Quinta Fiscalía Penal Corporativa de Huamanga limitan gravemente la capacidad de recolectar, preservar y analizar adecuadamente las evidencias digitales en los casos de estafa tecnológica, lo que dificulta la investigación efectiva de estos delitos.		

tecnológica en la Fiscalía Penal Corporativa de Ayacucho? b. ¿Cómo la ausencia de cooperación efectiva entre las plataformas tecnológicas, entidades bancarias y las autoridades judiciales afecta la identificación y persecución de los responsables de estafas cometidas mediante medios tecnológicos en Huamanga?	en la Fiscalía Penal Corporativa de Ayacucho. b. Identificar cómo la ausencia de cooperación efectiva entre las plataformas tecnológicas, entidades bancarias y las autoridades judiciales afecta la identificación y persecución de los responsables de estafas cometidas mediante medios tecnológicos en Ayacucho.	b. La ausencia de cooperación efectiva entre las plataformas tecnológicas, las entidades bancarias y las autoridades judiciales en Huamanga dificulta la identificación y persecución de los responsables de estafas tecnológicas, al generar obstáculos en la obtención de información clave y en la coordinación de acciones judiciales, lo que incrementa la impunidad y retrasa el avance de las investigaciones.		Análisis documental **3. Técnicas** Encuesta Lista de cotejo

ACTA DE SUSTENTACIÓN DE TESIS DEL ASPIRANTE EMILIO JAIME MALDONADO

En la ciudad de Ayacucho, siendo la 04:00 pm del 19 de diciembre de 2025, reunidos en la Facultad de Derecho y Ciencias Políticas -UNSCH: Oscar Galván Oviedo (presidente), Jesús Walter Espinoza Altamirano, Nilo Raúl Palacios García, Arturo Conga Soto y Rudy Augusto Pillpe Yaranga (miembros), para examinar la tesis Dificultades en la investigación del delito de estafa por el incremento del uso de medios tecnológicos en la Quinta fiscalía provincial Penal Corporativa de Huamanga, 2024. Acto seguido se procede a dar lectura a la Resolución Decanal N° 618-2025-UNSCH-FDCP-D, del 16 de diciembre del 2025, asimismo, se dio lectura al articulo 25° del Reglamento de Grados y Títulos de la Facultad de Derecho y Ciencias Políticas -UNSCH. El presidente otorga el uso de la palabra el uso de la palabra al aspirante, luego de la sustentación se procede a realizar las preguntas y objeciones por parte del jurado examinador. Una vez concluido el presidente del jurado invita a salir al aspirante y los miembros del jurado proceden a deliberar. El jurado luego de la deliberación decidió APROBAR por mayoría con la nota de 12 (doce) y se procederá a brindar las observaciones, concluye el acto académico con la firma del acta

---

Oscar Galván Oviedo

PRESIDENTE

Jesús Walter Espinoza Altamirano

MIEMBRO

Nilo Raúl Palacios García

MIEMBRO

Arturo Conga Soto

MIEMBRO

Rudy Augusto Pillpe Yaranga

MIEMBRO

UNSCH | FACULTAD DE DERECHO Y CIENCIAS POLITICAS | ESCUELA PROFESIONAL DE DERECHO

CONSTANCIA DE ORIGINALIDAD N° 16-2025-UNSCH-FDCP

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

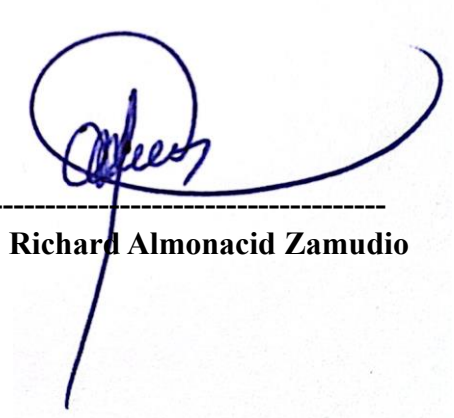
CONSTANCIA DE ORIGINALIDAD

Autor	**Bach. EMILIO JAIME MALDONADO**
Para	**Título profesional**
Denominación de la tesis	**Dificultades en la investigación del delito de estafa por el incremento del uso de medios tecnológicos en la Quinta Fiscalía Provincial Penal Corporativa de Huamanga, 2024.**
Evaluación de Originalidad	**13%**
Numero de trabajo	**2851962944**
Fecha	**30 de diciembre 2025**

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, 30 de diciembre de 2025



Dr. Richard Almonacid Zamudio

Dificultades en la investigación del delito de estafa por el incremento del uso de medios tecnológicos en la Quinta Fiscalía Provincial Penal Corporativa de Huamanga, 2024.

por Emilio Jaime Maldonado

Fecha de entrega: 30-dic-2025 04:15p. m. (UTC-0500)
Identificador de la entrega: 2851962944
Nombre del archivo: TESIS_CORREGIDO_EMILIO.docx (234.52K)
Total de palabras: 15453
Total de caracteres: 92266

Dificultades en la investigación del delito de estafa por el incremento del uso de medios tecnológicos en la Quinta Fiscalía Provincial Penal Corporativa de Huamanga, 2024.

INFORME DE ORIGINALIDAD

13%	14%	6%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unsch.edu.pe Fuente de Internet	9%
2	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	1%
3	repositorio.ucv.edu.pe Fuente de Internet	1%
4	repositorio.continental.edu.pe Fuente de Internet	1%
5	Jorge Santiago Vallejo Lara, Hillary Patricia Herrera Avilés, Edwin Javier Ortega Campos, Fredy Roberto Hidalgo Cajo. "Una comparación de la tipificación del ciberdelito en Sudamérica", Tesla Revista Científica, 2024 Publicación	<1%
6	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1%
7	doku.pub Fuente de Internet	<1%
8	Submitted to Universidad Tecnológica Indoamerica Trabajo del estudiante	<1%
9	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%

10	Submitted to DEPARTAMENTO ACADÉMICO DE DERECHO Y CIENCIA POLÍTICA Trabajo del estudiante	<1 %
11	dpc-rivista-trimestrale.criminaljusticenetwork.eu Fuente de Internet	<1 %
12	repositorio.unp.edu.pe Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		