UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

TESIS:

La problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga 2023.

Para optar el título profesional de:

ABOGADO

PRESENTADO POR:

Bach. Luis Eduardo BERROCAL ALFARO

ASESOR:

Dr. Jesús Walter ESPINOZA ALTAMIRANO

AYACUCHO - PERÚ

2024

Dedicatoria:

A mis padres por su apoyo incondicional en cada momento de mi vida.

Agradecimiento:

Agradezco a mis docentes de pregrado, por haber contribuido en mi formación académica.

Resumen

El presente trabajo de tesis estudia la problemática de la investigación del delito de fraude informático. Este estudio reveló varias dificultades significativas que afectan la eficacia de estas investigaciones.

Primero, se identificó una insuficiencia de recursos tecnológicos. Las herramientas disponibles para la investigación de fraudes informáticos son consideradas insuficientes y no adecuadas por la mayoría de los fiscales y abogados. Esta falta de recursos limita la capacidad de los investigadores para abordar estos delitos de manera efectiva.

En segundo lugar, se destacó la falta de capacitación y especialización del personal. Los fiscales y abogados señalaron que no reciben capacitación regular y adecuada sobre fraudes informáticos, y que el equipo no cuenta con la especialización necesaria. Esta carencia de formación y especialización contribuye a la ineficacia en la investigación de estos delitos.

Además, se identificó una deficiencia en la coordinación interinstitucional. Existe una percepción generalizada de que no hay colaboraciones frecuentes con otras instituciones y que el intercambio de información con otras entidades no es eficiente ni oportuno. Esta falta de coordinación y colaboración interinstitucional dificulta la investigación y el procesamiento de fraudes informáticos.

Finalmente, se señaló la inadecuación del marco normativo. Las leyes actuales son consideradas inadecuadas para investigar y procesar casos de fraude informático, y no existen suficientes regulaciones específicas. Esta falta de un marco normativo actualizado limita la capacidad de los fiscales para actuar de manera efectiva y procesar a los responsables de estos delitos.

Los hallazgos del estudio sugieren la necesidad urgente de mejorar las herramientas tecnológicas, la capacitación y especialización del personal, la coordinación interinstitucional y el marco normativo para abordar eficazmente los fraudes informáticos en el Distrito Fiscal de Huamanga. Estos cambios son esenciales para mejorar la eficacia de las investigaciones y reducir la impunidad de los delitos de fraude informático.

Palabras clave: Delitos informáticos, investigación fiscal, fraude informático.

Abstract

The present thesis studies the problems of investigating the crime of computer fraud. This study revealed several significant difficulties that affect the effectiveness of these investigations.

First, a lack of technological resources was identified. The tools available for the investigation of computer fraud are considered insufficient and not adequate by the majority of prosecutors and lawyers. This lack of resources limits investigators' ability to address these crimes effectively.

Secondly, the lack of training and specialization of personnel was highlighted. Prosecutors and lawyers indicated that they do not receive regular and adequate training on computer fraud, and that the team does not have the necessary specialization. This lack of training and specialization contributes to the inefficiency in the investigation of these crimes.

In addition, a deficiency in inter-institutional coordination was identified. There is a general perception that there are not frequent collaborations with other institutions and that the exchange of information with other entities is not efficient or timely. This lack of inter-institutional coordination and collaboration makes the investigation and prosecution of computer fraud difficult.

Finally, the inadequacy of the regulatory framework was pointed out. Current laws are considered inadequate to investigate and prosecute cases of computer fraud, and there are not enough specific regulations. This lack of an updated regulatory framework limits the ability of prosecutors to act effectively and prosecute those responsible for these crimes.

The findings of the study suggest the urgent need to improve technological tools, staff training and specialization, inter-institutional coordination and the regulatory framework to effectively address computer fraud in the Huamanga Fiscal District. These changes are

essential to improve the effectiveness of investigations and reduce impunity for computer fraud crimes.

Keywords: Computer crimes, tax investigation, computer fraud.

INTRODUCCIÓN

En el contexto actual, la ciberdelincuencia ha experimentado un incremento significativo, afectando tanto a individuos como a organizaciones en todo el mundo. En el Distrito Fiscal de Huamanga, durante el año 2023, se ha observado un aumento alarmante en los casos de fraude informático, lo que ha generado una preocupación creciente entre las autoridades y la sociedad en general. Este tipo de delitos no solo implica pérdidas económicas considerables, sino que también pone en riesgo la integridad y la privacidad de la información personal y corporativa.

La investigación del fraude informático presenta múltiples desafíos, entre los cuales se destacan la insuficiencia de recursos tecnológicos, la falta de capacitación especializada del personal investigador y la inadecuación del marco normativo vigente. Estos factores limitan la capacidad de los fiscales para actuar de manera efectiva y procesar a los responsables de estos delitos, lo que a menudo resulta en la impunidad de los mismos.

Según un artículo de Infobae, las denuncias por ciberdelincuencia en Perú se incrementaron en un 150% en 2023, siendo el fraude informático uno de los delitos más comunes. Este aumento en los casos de fraude subraya la necesidad de mejorar las herramientas tecnológicas y la capacitación del personal para enfrentar estos desafíos. Cabeza, Y. (2023, septiembre 9)

El presente estudio tiene como objetivo principal evaluar la problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga durante el año 2023. A través de un análisis detallado de las percepciones de fiscales y abogados, se busca identificar las principales dificultades técnicas y operativas que enfrentan en la investigación de estos delitos. Además, se pretende proponer recomendaciones que

contribuyan a mejorar la eficacia de las investigaciones y reducir la impunidad de los fraudes informáticos.

En este contexto, se analizarán aspectos clave como la disponibilidad y adecuación de las herramientas tecnológicas, la capacitación y especialización del personal, la coordinación interinstitucional y la adecuación del marco normativo. Los resultados de este estudio proporcionarán una visión integral de la situación actual y servirán como base para el desarrollo de estrategias y políticas que fortalezcan la capacidad de respuesta del sistema de justicia ante los desafíos que plantea la ciberdelincuencia en el Distrito Fiscal de Huamanga.

ÍNDICE GENERAL

ÍNDICE DE TABLAS Y FIGURAS

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

a. Realidad Internacional

El fraude informático es un problema global que afecta tanto a individuos como a organizaciones. A nivel internacional, los ciberdelincuentes utilizan técnicas avanzadas como el phishing, malware y ransomware para robar información personal y financiera. La falta de una legislación uniforme y la rápida evolución de la tecnología dificultan la lucha contra estos delitos. Organizaciones como INTERPOL y Europol trabajan en conjunto con gobiernos para combatir el cibercrimen, pero la cooperación internacional sigue siendo un desafío. *INTERPOL. (2021, noviembre 11)*

El fraude informático tiene un impacto económico significativo. Según datos del International Observatory of Computer Crime, los ciberdelitos, incluyendo el fraude informático, generan pérdidas de miles de millones de dólares anualmente. Las empresas invierten grandes sumas en ciberseguridad para protegerse, pero los ciberdelincuentes continúan encontrando nuevas vulnerabilidades. La naturaleza transnacional del fraude informático requiere una cooperación internacional robusta. Organizaciones como INTERPOL juegan un papel crucial en la coordinación de operaciones policiales y en la creación de alianzas multisectoriales para combatir el cibercrimen. La colaboración entre países es esencial para rastrear y detener a los ciberdelincuentes que operan a través de fronteras. A nivel global, la legislación sobre fraude informático varía significativamente. Algunos países tienen leyes estrictas y recursos dedicados a la ciberseguridad, mientras que otros están rezagados en la implementación de medidas efectivas. El Convenio sobre Ciberdelincuencia del Consejo de Europa es uno de los marcos legales más importantes, proporcionando directrices para la cooperación internacional y la armonización de leyes.

b. Realidad Nacional

En Perú, el fraude informático ha aumentado significativamente en los últimos años. Según informes, las denuncias por ciberdelincuencia se incrementaron en un 150% en 2023. Los delitos más comunes incluyen estafas mediante redes sociales, correos electrónicos y suplantación de identidad. La Fiscalía de Prevención del Delito ha implementado acciones preventivas en entidades bancarias para combatir estos delitos. Sin embargo, la falta de recursos y capacitación en las fuerzas del orden sigue siendo un obstáculo importante. Cabeza, Y. (2023)

Durante el año 2023, la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional del Perú (PNP) registró un total de 2,485 casos de delitos informáticos en el país. Entre estos casos, se destacaron el fraude electrónico y la suplantación de identidad como las modalidades más frecuentes, según información de la agencia de noticias Andina.

Las modalidades más comunes enfrentadas por la PNP el año pasado incluyeron phishing, carding, suplantación de identidad, Thief Transfer, SIM Swapping, fake apps, y vishing. El robo de cuentas de WhatsApp también figuró entre los delitos informáticos más reportados, donde los delincuentes utilizaban chips extranjeros para solicitar códigos de verificación a las víctimas y así tomar control de sus cuentas.

En 2023, se reportaron 294 casos de phishing. Esta práctica consiste en engañar a las personas para que revelen información confidencial a través de correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos diseñados para manipular a las víctimas y descargar malware u obtener datos personales, como números de tarjetas de crédito. Cabeza, Y. (2023)

El carding, otro fraude virtual significativo, se presentó en 262 casos el año pasado. Este delito implica el uso de información de tarjetas robadas para realizar compras en línea, generalmente mediante la suplantación de identidad.

Asimismo, se registraron 87 casos de Thief Transfer, en los que los delincuentes accedían a aplicaciones financieras de las víctimas para transferir dinero o suplantar su identidad para solicitar préstamos a través de contactos guardados en el celular. Además, se reportaron 108 casos de grooming, en los cuales adultos se hacían pasar por menores con fines de chantaje sexual, resultando en seis detenciones. Hubo también 50 casos de pornografía infantil, con 39 personas detenidas y 19 menores rescatados.

Otros delitos informáticos denunciados incluyeron el acceso ilícito a sistemas informáticos. En 2023, se realizaron avances normativos para mejorar la investigación y el combate contra estos delitos. Un avance significativo fue la promulgación del Decreto Legislativo N° 1614 en diciembre del año pasado, que modifica la Ley N° 30096, Ley de Delitos Informáticos, y endurece las penas para el acceso ilícito a sistemas informáticos y la suplantación de páginas web como parte del fraude informático.

En comparación con 2022, cuando se detuvo a 229 personas implicadas en ciberdelitos y se registraron 3,946 casos ante la Divindat, un aumento del 70% en las detenciones respecto a 2021, el promedio mensual de denuncias en 2022 fue de 407. Los delitos más recurrentes continuaron siendo el fraude informático, la estafa agravada y la suplantación de identidad, según reportó Infobae. Este es el delito informático más investigado en el Perú, y los casos se han incrementado en 58% en el 2023. Afines del año pasado se logró la prisión preventiva de tres miembros de una banda criminal dedicada a realizar transferencias ilegales de celulares robados. Las nueve víctimas de fraude informático sufrieron el robo de más de 150,000 soles.

El uso de celulares robados es uno de los casos más frecuentes en el Perú para este delito informático, que se ha convertido en el más investigado durante el 2023 con 21,842 denuncias en las fiscalías provinciales penales y mixtas del país. Esta cifra representa un incremento del 58% respecto al año previo. Además, entre enero y febrero se han registrado 3,903 denuncias de fraude informático en el ámbito nacional. Cabeza, Y. (2023) La jefa de la Unidad Fiscal Especializada en Ciberdelincuencia y titular de la Fiscalía Superior Corporativa Especializada en Ciberdelincuencia de Lima Centro del Ministerio Público, Aurora Castillo Fuerman, señaló a El Peruano que el fraude informático continúa siendo el delito informático más denunciado, y también el que ha tenido más sentencias en el 2023. Castillo Fuerman, A. (2023, septiembre 9).

c. Realidad Local

En el Distrito Fiscal de Huamanga, la investigación del delito de fraude informático enfrenta una serie de desafíos significativos que reflejan tanto las limitaciones del contexto local como las características emergentes del delito en sí. A pesar de la creciente prevalencia del fraude informático a nivel global, la respuesta investigativa en esta región específica revela profundas deficiencias que afectan la eficacia y eficiencia del sistema judicial.

Los casos de fraude informático en Huamanga a menudo sufren retrasos significativos durante las investigaciones. Estos retrasos pueden ser causados por la falta de personal especializado, la complejidad técnica de los casos y la insuficiencia de procedimientos estandarizados para la investigación y procesamiento de delitos informáticos. Como resultado, los casos pueden estancarse, y los delincuentes pueden evitar sanciones efectivas debido a la prolongación de los procesos legales.

La investigación del fraude informático también se ve afectada por una falta de coordinación entre las distintas entidades involucradas, como la policía, el Ministerio

Público y las instituciones financieras. Esta falta de cooperación puede resultar en una duplicación de esfuerzos, pérdidas de tiempo y dificultades en el intercambio de información crítica. La ausencia de una estrategia coordinada y unificada dificulta la respuesta efectiva a los casos de fraude informático.

Aunque existen leyes y normativas que abordan el fraude informático, su aplicación en Huamanga muestra vacíos y deficiencias. La Ley N° 30096 de Delitos Informáticos puede no estar completamente adaptada a las nuevas modalidades de fraude, lo que impide una respuesta legal adecuada y efectiva. La falta de actualizaciones normativas también contribuye a la inseguridad jurídica y a la dificultad para imponer sanciones adecuadas.

1.2. Definición del problema de investigación

1.2.1. Problema principal

¿Cuáles son las principales dificultades que enfrenta el Distrito Fiscal de Huamanga en la investigación de delitos de fraude informático durante el año 2023?

1.2.2. Problemas secundarios

a. ¿Cuáles son las dificultades técnicas que afectan la investigación del fraude informático en el Distrito Fiscal de Huamanga en el año 2023?

b. ¿Qué factores limitan la eficacia de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga en 2023?

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Identificar cuáles son las principales dificultades que enfrenta el Distrito Fiscal de Huamanga en la investigación de delitos de fraude informático durante el año 2023.

1.3.2. Objetivo Específico

a. Identificar cuáles son las dificultades técnicas que afectan la investigación del fraude informático en el Distrito Fiscal de Huamanga en el año 2023.

b. Describir cuales son factores que limitan la eficacia de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga en 2023.

1.4. Hipótesis de la investigación

1.4.1. Hipótesis general

El Distrito Fiscal de Huamanga, enfrenta dificultades significativas en la investigación de delitos de fraude informático durante el año 2023, principalmente debido a la falta de recursos tecnológicos adecuados y la escasa capacitación especializada del personal investigador en técnicas de ciberseguridad ello termina con el archivo de las investigaciones de fraude informático y por ende impunidad del delito.

1.4.2. Hipótesis Específicas

a). La ausencia de un marco normativo actualizado que contemple las nuevas modalidades de fraude digital limita la capacidad de los fiscales para actuar de manera efectiva.

b). La insuficiente coordinación interinstitucional entre las entidades encargadas de la persecución de estos delitos y una infraestructura tecnológica deficiente que dificulta la recolección y análisis de evidencia digital.

1.5. Delimitación de la investigación

Delimitación espacial: El marco espacial de la investigación se centrará en la Fiscalía Corporativa Penal de Huamanga.

Delimitación temporal: Se realizó el estudio descriptivo de las carpetas fiscales del delito de fraude informático, investigaciones realizadas en la Fiscalía Provincial Penal Corporativa de Huamanga durante el periodo de enero a diciembre del año 2023.

1.6. Justificación e importancia

1.6.1. Justificación

La problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga durante el año 2023 se puede justificar a través de los hallazgos de diversos estudios y expertos en el campo. Según Valdivia Zapata (2023), la eficacia de la persecución penal del delito de fraude informático en Perú se ve gravemente afectada por la falta de herramientas tecnológicas adecuadas y la insuficiente capacitación del personal encargado de estas investigaciones. Este autor destaca que, aunque las tecnologías de la información y comunicación han avanzado significativamente, las entidades encargadas de combatir el fraude informático no cuentan con los recursos necesarios para enfrentar estos desafíos de manera efectiva.

Además, el informe de la Defensoría del Pueblo (2023) subraya que la ciberseguridad en Perú enfrenta retos importantes debido a la rápida evolución de las técnicas utilizadas por los ciberdelincuentes y la falta de una legislación adecuada que

contemple estas nuevas modalidades de fraude. La falta de coordinación interinstitucional y la ineficiencia en el intercambio de información entre las entidades encargadas de la persecución de estos delitos también son factores que limitan la eficacia de las investigaciones.

En resumen, la problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga en 2023 se justifica por la combinación de una infraestructura tecnológica deficiente, la falta de capacitación especializada del personal y la inadecuación del marco normativo vigente, lo que resulta en una alta tasa de impunidad para estos delitos.

1.6.2. Importancia de la investigación

La importancia de este estudio radica en su potencial para aportar al fortalecimiento del sistema de justicia penal en Huamanga al abordar las problemáticas específicas de la investigación de delitos de fraude informático, un tipo de crimen que está en constante evolución y que representa una amenaza creciente en el entorno digital moderno. Al identificar las debilidades y vacíos existentes en los procedimientos de investigación actuales, esta investigación ofrece valiosas recomendaciones que pueden ser implementadas por el Distrito Fiscal de Huamanga y otras jurisdicciones similares para mejorar la eficacia en la persecución de estos delitos.

1.6.3. Viabilidad de la investigación

La viabilidad de la investigación sobre la problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga en 2023 se basa en varios factores clave. Primero, la accesibilidad a la información proporcionada por la fiscalía es fundamental, ya que garantiza que se pueda obtener una base de datos adecuada para el análisis. La investigación también se asegurará de que se apliquen principios éticos para

proteger la privacidad de los participantes, manteniendo la confidencialidad en todo momento. Además, la disponibilidad de recursos financieros y logísticos, así como el respaldo institucional, son elementos esenciales que facilitan la ejecución del proyecto.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de estudio

2.1.1. Antecedentes internacionales

Quevedo (2017), En su investigación titulada “Investigación y Prueba del Ciberdelito”, elaborada para optar por el grado de Doctor por el Departamento de Derecho y Ciencias Políticas de la Universidad de Barcelona, sostiene que, aunque existen múltiples estrategias para investigar los ciberdelitos, es crucial que estas respeten las restricciones establecidas por los derechos constitucionales. Además, se argumenta que el progreso tecnológico ha generado nuevas manifestaciones de ciberdelincuencia, lo cual ha puesto de manifiesto la insuficiencia de la legislación actual en Centroamérica. Esto subraya la necesidad de que los países de la región cooperen entre sí para abordar de manera efectiva este desafío.

Chiluisa (2021) “Los delitos informáticos y los vacíos legales” que afectan a los ciudadanos del Ecuador, señala que La legislación ecuatoriana enfrenta una serie de lagunas y contradicciones normativas debido a los continuos avances en el ámbito jurídico, que exigen esfuerzos reforzados para mantenerse al ritmo de la evolución social y tecnológica. Esta última ha dado lugar a una nueva ola de delitos que no están completamente tipificados debido a las dificultades para regular conductas que cruzan fronteras.

Gamba (2018), “Delito Informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos”; menciona que los delitos informáticos están avanzando rápidamente, lo que genera riesgos diarios para sus usuarios debido a factores económicos, sociales, culturales, políticos y jurídicos. Esto hace necesaria una mayor comprensión y conocimiento de estos delitos, que ayude a establecer

criterios legales claros para su regulación y ordenamiento. La cooperación de organismos internacionales, tanto de manera multilateral como individual, es esencial para desarrollar estrategias que permitan tomar medidas, proporcionar herramientas para la adecuación normativa, prevenir la comisión de estos delitos y aplicar sanciones a los infractores por parte de las autoridades competentes.

2.1.2. Antecedentes nacionales

Alcantara (2024) En el proyecto de investigación “Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022” El delito de fraude cibernético representa una problemática significativa en nuestra legislación, lo que motivó plantear como objetivo general analizar la Ley N° 30096, Ley de Delitos Informáticos, y su eficacia en la regulación de los fraudes informáticos en el Perú. Este análisis busca identificar posibles vacíos o lagunas legales que puedan ser aprovechados por los ciberdelincuentes.

En el primer capítulo se examinará el contexto problemático del tema, abarcando un enfoque internacional, nacional y local. Este análisis incluirá una revisión de antecedentes relevantes, el marco teórico asociado, y la formulación del problema de investigación en términos generales y específicos. Asimismo, se justificará la relevancia del estudio desde perspectivas teóricas, sociales, prácticas y metodológicas, y se presentarán los objetivos generales y específicos que guiarán la investigación.

En el segundo capítulo se describirá el material y los métodos empleados en el estudio. Esto incluirá una explicación detallada del tipo y diseño de investigación, el contexto en el que se desarrollará el análisis, la caracterización de los participantes, y las técnicas utilizadas para la recolección de datos. Además, se discutirá la validez y confiabilidad de los instrumentos, junto con los criterios éticos y de rigor científico adoptados para garantizar la calidad del estudio.

En el tercer capítulo se presentarán los resultados en forma de tablas y figuras, se discutirá su significado y se analizará el aporte práctico del estudio. Finalmente, el cuarto capítulo ofrecerá las conclusiones y recomendaciones, junto con las referencias bibliográficas y anexos pertinentes.

Matos (2022), “Especialización de la investigación preparatoria en los delitos de fraudes informático”, El presente trabajo de investigación tuvo como objetivo analizar la aplicación de la investigación preparatoria en los delitos de fraude informático dentro del ámbito del Ministerio Público de Lima Norte. Con un enfoque cualitativo, de tipo aplicado y utilizando un diseño basado en la teoría fundamentada, se recopilaron datos clave, confiables y actualizados a través de entrevistas y análisis documental.

Los hallazgos reflejaron de manera precisa la situación actual, permitiendo concluir que es imprescindible introducir reformas normativas en la Ley de Delitos Informáticos, así como implementar una infraestructura especializada para abordar este tipo de delitos. Asimismo, se evidenció la necesidad de mejoras logísticas, capacitación de los operadores de justicia encargados de las investigaciones, y el fortalecimiento institucional tanto del Ministerio Público como de la Policía Nacional del Perú (Divindat). Como resultado, se propuso que las autoridades competentes adopten e implementen las sugerencias planteadas para mejorar la respuesta a este tipo de delitos.

Pardo (2018) La presente investigación titulada “Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018” tuvo como objetivo general examinar cómo se maneja el tratamiento jurídico penal de los delitos informáticos contra el patrimonio en el Distrito Judicial de Lima en 2018. Utilizando métodos cualitativos de investigación, de nivel descriptivo y explicativo, se aplicó la técnica de entrevistas, con una guía específica para recoger información de expertos, tanto nacionales como internacionales, sobre el tema. Las conclusiones indican que el tratamiento jurídico actual

es inadecuado, ya que agrupa erróneamente todos los delitos informáticos contra el patrimonio bajo la categoría de fraude informático, creando ambigüedad en la interpretación de las normas y dificultando su efectiva sanción. Se recomienda que el Congreso de la República promueva una ley que permita la adhesión de Perú al Convenio de Budapest y que desarrolle una legislación clara para tipificar de manera específica los distintos delitos informáticos contra el patrimonio, incluyendo fraudes, estafas, sabotajes y hurtos informáticos. Además, se sugiere establecer fiscalías especializadas en estos delitos, que la Corte Penal Internacional asuma competencia sobre delitos informáticos transnacionales, y que las universidades integren un curso obligatorio de derecho informático en sus currículos. También es aconsejable que, a nivel escolar, tanto en primaria como secundaria, se incluya un curso de informática que enfatice la prevención de delitos informáticos..

Fernandez (2023) El avance tecnológico y crecimiento económico han traído consigo, nuevos modelos de negocio e inversión para el Perú. Las "Fintech" o tecnologías financieras, que combinan "Technology" y "Financial," están transformando el sector financiero con innovaciones como ahorros, créditos y crowdfunding. Sin embargo, la Superintendencia de Banca, Seguro y AFP (SBS) no regula actualmente la operatividad de estas empresas, permitiendo que muchas operen sin autorización y sin un marco legal adecuado para sancionar posibles infracciones o delitos. Según el artículo 159, numeral 4, de la Constitución del Perú, el Ministerio Público debe liderar las investigaciones desde la etapa policial, y el fiscal especializado en delitos informáticos debe seguir el Decreto Legislativo N°052 y el Nuevo Código Procesal Penal para garantizar la legalidad. Esto plantea un riesgo de que las fintech sean usadas para cometer fraudes informáticos, como el phishing. La investigación, de enfoque cualitativo y diseño de teoría fundamentada, busca identificar estos riesgos y evaluar la Ley N° 30096, políticas públicas y derecho comparado en relación con las fintech. La muestra del estudio incluye cinco especialistas

en derecho, policía, fiscalía y contabilidad, con experiencia en ciberperitaje y fraude financiero. Se concluye que los vacíos legales en la Ley N° 30096 deben ser abordados para permitir una mejor investigación de fraudes informáticos cometidos por fintech.

2.2. Bases teóricas

El fraude informático es un fenómeno complejo que ha sido estudiado desde diversas perspectivas teóricas, siendo algunas de las más importantes:

a. Teoría del Triángulo del Fraude

Propuesta por Donald Cressey, esta teoría sugiere que el fraude ocurre cuando se combinan tres factores: presión, oportunidad y racionalización. La presión puede ser financiera, como deudas o problemas económicos, o emocional, como la necesidad de mantener un estilo de vida o satisfacer expectativas familiares. La oportunidad surge de debilidades en los controles internos de una organización, como la falta de supervisión, controles inadecuados o acceso no restringido a recursos valiosos. La racionalización es el proceso mediante el cual el delincuente justifica su comportamiento, convenciéndose de que su acción es aceptable o necesaria. Por ejemplo, pueden pensar que solo están "tomando prestado" el dinero y que lo devolverán más adelante, o que merecen una compensación adicional por su trabajo.

Esta teoría es ampliamente utilizada en la prevención del fraude, ya que permite a las organizaciones identificar y mitigar los factores que pueden llevar a un empleado a cometer fraude. Al fortalecer los controles internos, proporcionar apoyo financiero y emocional a los empleados, y fomentar una cultura de ética y transparencia, las organizaciones pueden reducir significativamente el riesgo de fraude.

b. Teoría de la Gestión de Riesgos de Fraude (GRF)

Esta teoría propone un enfoque sistemático para gestionar los riesgos de fraude, que incluye varias etapas clave:

- **Identificación de Riesgos**: Consiste en reconocer y catalogar los posibles riesgos de fraude que podrían afectar a la organización. Esto puede incluir la revisión de procesos internos, entrevistas con empleados y análisis de datos históricos de fraude.

- **Mitigación de Riesgos**: Esta etapa implica la implementación de controles internos y políticas de prevención diseñadas para reducir la probabilidad de que ocurra un fraude. Esto puede incluir la segregación de funciones, auditorías internas, controles de acceso y la implementación de tecnologías de detección de fraude.

- **Monitoreo y Revisión**: Los controles y políticas implementados deben ser monitoreados y revisados regularmente para asegurar su efectividad. Esto incluye la realización de auditorías periódicas y la actualización de los controles en respuesta a nuevos riesgos o cambios en el entorno de la organización.

La Teoría de la Gestión de Riesgos de Fraude (GRF) proporciona un marco estructurado para abordar el fraude de manera proactiva, permitiendo a las organizaciones minimizar sus riesgos y proteger sus activos de manera más efectiva.

c. Teoría del Comportamiento de las Personas (TCP)

La Teoría del Comportamiento de las Personas (TCP) analiza cómo los comportamientos y actitudes de las personas pueden influir en la comisión de fraudes. Esta teoría se enfoca en factores psicológicos y sociales que pueden llevar a un individuo a cometer un fraude informático. Entre los factores psicológicos se incluyen la personalidad del individuo, su moralidad y sus valores éticos. Por ejemplo, una persona con una baja moralidad o con valores éticos flexibles puede ser más propensa a justificar el fraude.

Los factores sociales también juegan un papel crucial. La presión de grupo, la cultura organizacional y las normas sociales pueden influir en la decisión de cometer fraude. En un entorno donde el fraude es común o tolerado, los individuos pueden sentirse más inclinados a participar en actividades fraudulentas. Además, la percepción de impunidad o la creencia de que no serán atrapados puede motivar a las personas a cometer fraude.

La TCP también considera el impacto de las experiencias personales y profesionales. Las personas que han sido víctimas de fraude o que han observado a otros cometer fraude sin consecuencias pueden desarrollar una actitud más permisiva hacia estas actividades. Asimismo, la falta de reconocimiento o recompensas en el trabajo puede llevar a los empleados a buscar compensaciones ilícitas.

En resumen, la Teoría del Comportamiento de las Personas (TCP) proporciona una comprensión profunda de los factores psicológicos y sociales que pueden influir en la comisión de fraudes informáticos, ayudando a las organizaciones a identificar y mitigar estos riesgos de manera más efectiva.

d. Teoría de Disuasores y Motivadores de Fraude (DMF)

La Teoría de Disuasores y Motivadores de Fraude (DMF) examina los factores que pueden disuadir o motivar a una persona a cometer fraude. Esta teoría se basa en la idea de que el comportamiento fraudulento es influenciado tanto por factores que lo desalientan como por aquellos que lo fomentan.

Disuasores:

- **Sanciones Legales**: La existencia de leyes estrictas y sanciones severas puede disuadir a las personas de cometer fraude. El miedo a ser atrapado y enfrentar

consecuencias legales graves, como multas o prisión, actúa como un fuerte disuasor.

- **Controles Internos Efectivos**: La implementación de controles internos robustos dentro de una organización, como auditorías regulares, segregación de funciones y sistemas de monitoreo, puede reducir las oportunidades para cometer fraude. Estos controles dificultan que los empleados puedan llevar a cabo actividades fraudulentas sin ser detectados.

- **Cultura Organizacional Ética**: Fomentar una cultura organizacional que valore la ética y la integridad puede disuadir el fraude. Cuando los empleados sienten que la honestidad es valorada y recompensada, es menos probable que se involucren en comportamientos fraudulentos.

Motivadores:

- **Necesidades Financieras**: Las dificultades económicas personales pueden motivar a las personas a cometer fraude. La presión financiera, como deudas o la necesidad de mantener un cierto estilo de vida, puede llevar a los individuos a buscar soluciones ilícitas.

- **Percepción de Baja Probabilidad de Ser Descubierto**: Si una persona cree que es poco probable que sea atrapada, puede sentirse más inclinada a cometer fraude. La percepción de que los controles son débiles o inexistentes puede aumentar esta motivación.

- **Racionalización**: La capacidad de justificar el comportamiento fraudulento es un motivador clave. Las personas pueden convencerse de que su acción es aceptable o necesaria, por ejemplo, creyendo que solo están "tomando prestado" el dinero y

que lo devolverán más adelante, o que merecen una compensación adicional por su trabajo.

e. Teoría de la Inteligencia y Contrainteligencia (TIC)

La Teoría de la Inteligencia y Contrainteligencia (TIC) se enfoca en el uso de técnicas avanzadas de inteligencia y contrainteligencia para prevenir y detectar fraudes informáticos. Esta teoría abarca varias estrategias clave:

- **Recopilación de Información**: Implica la obtención de datos relevantes de diversas fuentes, como registros de transacciones, comunicaciones electrónicas y actividades en línea. Esta información se utiliza para construir un perfil detallado de posibles amenazas y comportamientos sospechosos.

- **Análisis de Información**: Una vez recopilada, la información se analiza utilizando técnicas de análisis de datos y algoritmos de aprendizaje automático. Este análisis permite identificar patrones y anomalías que podrían indicar actividades fraudulentas. Por ejemplo, transacciones inusuales o accesos no autorizados a sistemas informáticos pueden ser señales de fraude.

- **Implementación de Medidas de Seguridad**: Basándose en los resultados del análisis, se implementan medidas de seguridad para proteger los sistemas informáticos. Estas medidas pueden incluir la actualización de software de seguridad, la implementación de firewalls, la encriptación de datos y la configuración de sistemas de detección de intrusiones.

- **Monitoreo Continuo**: La TIC también enfatiza la importancia del monitoreo continuo de los sistemas informáticos para detectar y responder rápidamente a cualquier actividad sospechosa. Esto incluye la vigilancia en tiempo real de las

redes y sistemas, así como la realización de auditorías periódicas para asegurar que las medidas de seguridad sean efectivas.

- **Colaboración Interinstitucional**: La cooperación entre diferentes entidades, como agencias gubernamentales, empresas privadas y organizaciones internacionales, es crucial para compartir información y coordinar esfuerzos en la lucha contra el fraude informático. Esta colaboración permite una respuesta más rápida y efectiva ante las amenazas.

La Teoría de la Inteligencia y Contrainteligencia (TIC) proporciona un enfoque integral para la prevención y detección de fraudes informáticos, combinando la recopilación y análisis de información con la implementación de medidas de seguridad y el monitoreo continuo para proteger los sistemas informáticos de manera efectiva.

2.3. Concepto de los delitos informáticos

El concepto de **delitos informáticos** se relaciona principalmente con la idea de cometer crímenes a través del uso de computadoras, internet y otras tecnologías digitales. Sin embargo, esta concepción no abarca por completo la complejidad de esta forma de criminalidad, ya que las tecnologías mencionadas son meramente instrumentos que facilitan, pero no determinan, la comisión de tales delitos. A pesar de que el término "delitos informáticos" no se encuentra frecuentemente en las legislaciones penales tradicionales, describe una nueva forma de criminalidad que ha surgido a partir del uso creciente de la tecnología informática.

Según Mühlen, un delito informático abarca cualquier conducta delictiva en la que la computadora funcione como herramienta o como blanco del acto ilícito. De manera similar, Dannecker define el delito informático como una manifestación de criminalidad

vinculada, de forma directa o indirecta, al procesamiento electrónico de datos, en la cual interviene un dispositivo de procesamiento electrónico de información.

Desde nuestra perspectiva, consideramos la criminalidad informática como aquellas acciones orientadas a vulnerar sistemas de seguridad, tales como el acceso no autorizado a computadoras, correos electrónicos o bases de datos mediante el uso indebido de credenciales. Estas conductas son específicas y solo pueden llevarse a cabo utilizando tecnología.

En un sentido más amplio, la criminalidad informática incluye cualquier acción en la que las tecnologías de la información y la comunicación (TIC) actúen como objetivo, herramienta o escenario de ejecución, afectando distintos bienes jurídicos. Esto genera desafíos tanto criminológicos como penales, derivados de las particularidades inherentes al entorno digital en el que se desarrollan dichos delitos.

2.4. Antecedentes de los delitos informáticos

En un principio, los delitos informáticos estaban previstos en el artículo 186, inciso 3, segundo párrafo del Código Penal de 1991. Sin embargo, no se reconocían como un delito autónomo, sino como una circunstancia agravante del delito de hurto. En la actualidad, los delitos informáticos se encuentran regulados en el Capítulo X del Código Penal, que incluye los artículos 207-A (interferencia, acceso o copia ilícita de información en bases de datos), 207-B (alteración, daño o destrucción de bases de datos), 207-C (circunstancias agravantes) y 207-D (tráfico ilegal de datos). Además, están contemplados en diversas leyes penales especiales.

Entre estas normativas destaca la Ley N.º 30096, conocida como Ley de Delitos Informáticos, la cual está estructurada en siete capítulos:

- **Capítulo I:** Define la finalidad y el objeto de la ley.
- **Capítulo II:** Regula los delitos contra datos y sistemas informáticos.
- **Capítulo III:** Aborda los delitos informáticos contra la indemnidad y la libertad sexual.
- **Capítulo IV:** Trata los delitos informáticos contra la intimidad y el secreto de las comunicaciones.
- **Capítulo V:** Se centra en los delitos informáticos contra el patrimonio.
- **Capítulo VI:** Regula los delitos informáticos contra la fe pública.
- **Capítulo VII:** Contiene disposiciones comunes.

Posteriormente, con la promulgación de la Ley N.º 30171, se modificó la Ley N.º 30096 para alinearla con los estándares del Convenio de Budapest sobre cibercriminalidad. Esta ley introdujo ajustes en los artículos 2, 3, 4, 7, 8 y 10, permitiendo que los delitos se configuren de manera deliberada e ilegítima. Las principales modificaciones incluyeron:

- **Artículo 1:** Actualización de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley N.º 30096.
- **Artículo 2:** Revisión de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley N.º 30096.
- **Artículo 3:** Incorporación del artículo 12 a la Ley N.º 30096.
- **Artículo 4:** Modificación de los artículos 158, 162 y 323 del Código Penal.
- **Artículo 5:** Inclusión de los artículos 154-A y 183-B en el Código Penal.

- **Disposición Complementaria Derogatoria Única:** Eliminación del artículo 6 de la Ley N.º 30096.

2.5. Características y Alcance de los Delitos Informáticos

Es importante aclarar que no todo delito que involucra el uso de computadoras u otros dispositivos tecnológicos puede clasificarse automáticamente como un delito informático. La mera utilización de tecnología en la comisión de un delito no es suficiente para categorizarlo bajo esta denominación; es necesario que la tecnología desempeñe un papel central en la ejecución o en la naturaleza del delito.

a. **Mediación Tecnológica**: Los delitos informáticos requieren, en general, la mediación de tecnología avanzada, ya sea como herramienta o como objetivo del delito. Esto puede incluir el uso de software especializado, redes informáticas, y plataformas digitales.

b. **Invasión de Sistemas de Seguridad**: Estos delitos a menudo implican la intrusión en sistemas protegidos mediante contraseñas o medidas de seguridad cibernética, con el fin de acceder, manipular o extraer datos sin autorización.

c. **Afectación a Bienes Jurídicos**: Aunque los delitos informáticos pueden impactar una variedad de bienes jurídicos, incluyendo la privacidad, la propiedad intelectual, y la seguridad económica, su elemento unificador es el uso indebido de sistemas tecnológicos para perpetrar la ofensa.

d. **Naturaleza Global**: La infraestructura tecnológica global permite que estos delitos se cometan desde cualquier lugar del mundo, lo que presenta desafíos significativos para la jurisdicción y la aplicación de la ley.

e. **Evolución Rápida**: La rápida evolución de la tecnología significa que los delitos informáticos también están en constante cambio, adaptándose a nuevas herramientas y vulnerabilidades tecnológicas.

2.6. La Ley 30096

La Ley 30096 de Perú establece varios delitos informáticos específicos, cada uno con sus definiciones y sanciones correspondientes. A continuación, se presenta un resumen de los principales delitos informáticos previstos en dicha ley, con conceptos adicionales según lo establecido en la normativa.

2.6.1. Delitos Contra Datos y Sistemas Informáticos

a. **Acceso Ilícito (Artículo 2)**: Este delito se refiere a la entrada no autorizada a sistemas informáticos, vulnerando medidas de seguridad. La pena para este delito es de uno a cuatro años de prisión y una multa de treinta a noventa días. Además, se castiga con la misma pena a quien exceda los niveles de acceso autorizados.

b. **Atentado a la Integridad de Datos Informáticos (Artículo 3)**: Consiste en dañar, introducir, borrar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos de manera deliberada. La pena es de tres a seis años de prisión y una multa de ochenta a ciento veinte días.

c. **Atentado a la Integridad de Sistemas Informáticos (Artículo 4)**: Se refiere a la utilización ilegítima de un sistema informático, impidiendo el acceso, entorpeciendo o imposibilitando su funcionamiento. La pena es de tres a seis años de prisión y una multa de ochenta a ciento veinte días.

2.6.2. Delitos Informáticos Contra la Indemnidad y Libertad Sexual

Proposiciones a Menores con Fines Sexuales por Medios Tecnológicos (Artículo 5): Este delito involucra contactar a menores de catorce años a través de internet para obtener material pornográfico o proponer actos sexuales. La pena es de cuatro a ocho años de prisión e inhabilitación. Si la víctima tiene entre catorce y dieciocho años y se utiliza engaño, la pena es de tres a seis años de prisión e inhabilitación.

2.6.3. Delitos Informáticos Contra la Intimidad y el Secreto de las Comunicaciones

Interceptación de Datos Informáticos (Artículo 7): Este delito implica interceptar deliberada e ilegítimamente datos informáticos en transmisiones no públicas. La pena es de tres a seis años de prisión.

2.6.4. Delitos Informáticos Contra el Patrimonio

Fraude Informático (Artículo 8): Involucra obtener un beneficio ilícito a través de la manipulación de datos o sistemas informáticos en perjuicio de terceros. La pena es de tres a ocho años de prisión y una multa de sesenta a ciento veinte días. Si el fraude afecta al patrimonio del Estado destinado a fines asistenciales o programas de apoyo social, la pena es de cinco a diez años de prisión y una multa de ochenta a ciento cuarenta días.

2.6.5. Delitos Informáticos Contra la Fe Pública

Suplantación de Identidad (Artículo 9): Se refiere a suplantar la identidad de una persona natural o jurídica mediante tecnologías de la información, causando un perjuicio material o moral. La pena es de tres a cinco años de prisión

2.7. Delito de fraude informático

El fraude informático se caracteriza como un delito de resultado, lo que implica que no basta con realizar las conductas descritas en el tipo penal; es necesario que dichas acciones provoquen un perjuicio económico. El sujeto activo de este delito puede ser cualquier individuo que actúe en contra de una persona natural o jurídica, que se configura como el sujeto pasivo.

Este ilícito también requiere un resultado y solo puede cometerse de forma dolosa, ya que el autor debe actuar con plena conciencia y voluntad de suplantar la identidad de una persona natural o jurídica, generando un daño económico como consecuencia de su acción.

2.7.1. Fraude informático y sus modalidades

Zevallos (2020) identifica las siguientes modalidades comunes de fraude informático:

a. **Clonación de tarjetas de crédito:** Este delito se realiza utilizando dispositivos electrónicos conocidos como *skimmers*, que leen la banda magnética de las tarjetas. Los datos se obtienen, generalmente, en establecimientos como restaurantes o gasolineras por empleados que los copian a computadoras personales y luego los transfieren a tarjetas clonadas con la misma información que la original.

b. **Phishing:** Este método delictivo tiene como objetivo robar la identidad de la víctima. A través de correos electrónicos engañosos, los ciberdelincuentes obtienen información confidencial como números de tarjetas de crédito, contraseñas, datos de cuentas bancarias y datos personales. Las víctimas ingresan sus datos en sitios fraudulentos creyendo que son legítimos, permitiendo así el acceso a su información.

c. **Spear Phishing o phishing segmentado:** Similar al phishing, esta variante está dirigida a grupos específicos, como adultos mayores, que suelen ser más vulnerables a estos engaños.

d. **Transferencias electrónicas fraudulentas:** Aquí, el delincuente obtiene información confidencial necesaria para acceder a las cuentas bancarias de la víctima y realizar operaciones no autorizadas. Esto suele lograrse mediante correos electrónicos falsos que aparentan ser de instituciones financieras, solicitando datos personales bajo pretextos engañosos.

e. **Compras por internet con información robada de tarjetas:** Los delincuentes aprovechan que la víctima realiza compras utilizando conexiones Wi-Fi públicas. Sustraen información de la tarjeta, como el número, la fecha de vencimiento y el código de verificación, para realizar compras en páginas web confiables el mismo día y evitar sospechas.

f. **Vishing:** En esta modalidad, los delincuentes envían mensajes SMS haciéndose pasar por entidades bancarias, solicitando a la víctima que llame a un número falso o responda con información personal, como números de tarjeta o claves de acceso, para realizar operaciones fraudulentas.

g. **Ransomware:** Mediante un software malicioso, los ciberdelincuentes bloquean el acceso al ordenador de la víctima desde una ubicación remota. Esto ocurre frecuentemente cuando se abren correos electrónicos maliciosos o se descargan archivos infectados, permitiendo a los delincuentes extraer información valiosa.

h. **Smishing:** Utiliza mensajes de texto que aparentan provenir de instituciones legítimas. Los mensajes contienen enlaces que llevan a páginas fraudulentas o instalan códigos maliciosos en los dispositivos de las víctimas. Un ejemplo común es el envío de mensajes

que informan falsamente sobre premios, incitando a las víctimas a ingresar a un enlace comprometido.

2.8. Fraude informático y estafa

El fraude informático y la estafa comparten una relación estrecha, tanto que los sistemas jurídicos de países como Alemania y España los regulan de manera sucesiva o conjunta, respectivamente. Ambos delitos afectan el patrimonio de terceros, aunque emplean métodos diferentes. En la doctrina comparada, se los describe como tipos penales "paralelos". En el caso de Alemania, se distingue entre la "estafa" y la "estafa computacional" para diferenciar la estafa tradicional del fraude informático.

No obstante, esta distinción puede ser considerada inapropiada debido a las diferencias estructurales entre ambos delitos. La estafa requiere ciertos elementos: un engaño, un error, una disposición patrimonial y un perjuicio patrimonial, todos conectados causalmente. En este contexto, el error es un fenómeno psicológico que implica una percepción equivocada de la realidad, lo cual solo puede experimentar una persona natural. Las máquinas, al no tener capacidad de percepción o juicio, no pueden ser "engañadas" en el sentido penal de la estafa.

Por lo tanto, no es posible considerar como estafa las acciones fraudulentas dirigidas contra sistemas automatizados de información, ya que el sujeto afectado es una máquina y no una persona. Estas conductas encajan mejor dentro del fraude informático, que se basa en la manipulación o alteración de datos o programas informáticos con el propósito de causar un perjuicio patrimonial.

Es importante distinguir entre los fraudes realizados contra sistemas informáticos y aquellos realizados a través de ellos. Los primeros son catalogados como fraude informático, mientras que los segundos, como la estafa telefónica, pueden considerarse

una forma de estafa al utilizar computadoras como medio para engañar a las personas, como en los casos de mensajes fraudulentos en plataformas de ventas o subastas en línea.

Existe una postura doctrinal minoritaria que sostiene que el fraude informático podría subsumirse en el delito de estafa. Según esta visión, el error no sería un elemento esencial y el engaño no requeriría necesariamente que su destinatario sea una persona física. Argumentan que la disposición patrimonial no la realiza la máquina, sino la persona que la programó.

Sin embargo, esta posición entra en conflicto con la tipificación de la estafa en el ordenamiento jurídico vigente. La estafa requiere un sujeto que defrauda y otro que es víctima del fraude, tal como lo establece el Código Penal al penalizar "al que defraudare a otro". Este delito implica una interacción comunicativa entre personas, en la cual se produce un intercambio de información que atribuye significado a los actos delictivos. Esta característica hace de la estafa un "delito de comunicación", donde la relación entre el autor del engaño y la víctima es fundamental.

Por otro lado, resulta contradictorio pensar que el fraude informático, siendo uno de los delitos más significativos en el ámbito digital, no esté regulado en una legislación específica, sino que se incluya en disposiciones del Código Penal con una redacción que data de 1874. La evolución de la informática y el surgimiento de nuevos tipos de conductas delictivas han llevado a los estados a adaptar sus leyes a esta realidad. Los redactores del Código Penal original no contemplaron estas situaciones, limitándose a describir hipótesis de estafa específicas y no un concepto general de fraude aplicable al contexto digital.

2.9. Perfil del ciberdelincuente

El perfil del ciberdelincuente (sujeto activo) en los delitos informáticos se caracteriza por requerir habilidades y conocimientos avanzados en el manejo de sistemas informáticos.

Estas competencias han llevado a clasificar a los autores de estos delitos como "delincuentes de cuello blanco", cuyas características principales incluyen:

a. **Conocimientos técnicos especializados**: Dominan herramientas y tecnologías informáticas.

b. **Acceso a información sensible**: Suelen ocupar puestos estratégicos en sus lugares de trabajo, lo que les permite manejar datos confidenciales. Este tipo de conductas se conoce como *delitos ocupacionales*, dado que están vinculadas a las funciones laborales que desempeñan.

Según Marcelo Manson, los perpetradores de delitos informáticos no son delincuentes comunes, sino personas altamente especializadas en informática. Afirma que quienes cometen estos actos poseen habilidades técnicas específicas y suelen desempeñar funciones estratégicas en organizaciones donde manejan información sensible. En esa misma línea, Camacho Losa señala que los ciberdelincuentes generalmente son empleados de confianza de las empresas afectadas, lo que los distingue de los delincuentes marginales.

Por otro lado, Vives Antón y Gonzales Cussac amplían el concepto del sujeto activo, indicando que pueden ser tanto personas autorizadas para operar los sistemas (como operadores o programadores) como individuos externos que acceden sin autorización a terminales públicas o privadas. Sin embargo, Gutiérrez Francés y Ruiz Vadillo sostienen que cualquier persona puede ser autor de un delito informático, sin necesidad de contar con habilidades técnicas específicas o acceso privilegiado.

Desde nuestra perspectiva, el sujeto activo no se limita exclusivamente a empleados con acceso a información sensible. Si bien coincidimos parcialmente en que dichos individuos tienen mayores posibilidades de cometer estos delitos, también es

posible que personas externas con habilidades informáticas sean responsables de estas conductas. Por lo tanto, estos delitos se consideran de *dominio*, es decir, requieren un control técnico o práctico de las herramientas informáticas necesarias para cometerlos.

En este contexto, los sujetos activos se agrupan en categorías según sus métodos y motivaciones:

a. **Hackers**: Son individuos que acceden a sistemas informáticos sin autorización, motivados por la curiosidad o el desafío intelectual, más que por intenciones dañinas. Este tipo de actividad no busca alterar ni manipular sistemas, sino comprender su funcionamiento. Según Sieber, los hackers son personas que acceden sin permiso a sistemas de procesamiento de datos, no con fines fraudulentos, sino como una forma de exploración no autorizada. Morón Lerma también los define como aquellos que interfieren en sistemas informáticos o redes electrónicas de forma subrepticia, sin causar daños y más allá de los límites de lo autorizado.

b. **Crackers**: A diferencia de los hackers, los crackers tienen intenciones destructivas. Se dedican a introducirse en sistemas remotos para eliminar datos, interrumpir servicios legítimos y generar problemas en sistemas, procesadores o redes informáticas. Una característica distintiva de los crackers es que suelen utilizar programas preexistentes, disponibles generalmente en internet, a diferencia de los hackers, que desarrollan sus propias herramientas y dominan lenguajes de programación avanzados.

2.10. Delito de fraude informáticos tipo penal

El artículo 1 de la Ley de Delitos Informáticos establece como objetivo principal prevenir y sancionar las conductas ilícitas que afectan sistemas y datos informáticos, el secreto de las comunicaciones y otros bienes jurídicos de relevancia penal, como el

patrimonio, la fe pública y la libertad sexual. Estas acciones delictivas se realizan mediante el uso de tecnologías de la información y comunicación (TIC). La norma busca garantizar condiciones mínimas que permitan a las personas ejercer su derecho a la libertad y al desarrollo, fortaleciendo así la lucha contra la ciberdelincuencia.

Además de cumplir con la función punitiva del Estado para proteger la información, esta ley tiene como propósito fundamental alinear la legislación penal peruana con estándares internacionales, en particular con el *Convenio sobre Cibercriminalidad del Consejo de Europa* (CETS 185), conocido como el Convenio de Budapest.

El delito informático, como lo describe esta norma, se comete para obtener un beneficio ilícito en perjuicio de terceros, adoptando diversas modalidades:

1. **Diseño**: Consiste en la creación de datos informáticos con fines ilícitos, como la recuperación no autorizada de contraseñas bancarias mediante la manipulación de chips telefónicos.

2. **Introducción**: Implica incorporar datos previamente diseñados en un sistema para acceder de manera indebida a cuentas bancarias de las víctimas.

3. **Alteración**: Se refiere a la modificación de contraseñas u otros elementos del sistema con el objetivo de facilitar el delito.

4. **Borrado**: Consiste en eliminar o suprimir datos o sistemas de seguridad, lo que permite la ejecución del delito sin restricciones.

5. **Supresión**: Tiene como finalidad ocultar datos informáticos para facilitar el acto delictivo.

6. **Clonación de datos informáticos**: Implica copiar datos en dispositivos electrónicos, como sucede en la clonación de tarjetas de débito o crédito.

7. **Interferencia o manipulación**: Se trata de interrumpir la recepción de señales o manipular el funcionamiento normal de un sistema informático para obtener un beneficio ilícito, perjudicando a terceros.

2.10.1. Bien Jurídico protegido

El bien jurídico protegido en los delitos informáticos se concibe de manera integrada y multidimensional. En un primer nivel, está la información en sentido amplio: aquella que se almacena, procesa y transmite mediante sistemas automatizados de tratamiento de datos. En un segundo nivel, se incluyen otros bienes afectados indirectamente por estos delitos, tales como la indemnidad sexual, la intimidad, entre otros. La información, entendida como el contenido de bases o bancos de datos y el producto de procesos informáticos automatizados, adquiere el estatus de bien autónomo con valor económico, lo cual ha motivado su protección legal como bien jurídico.

Sin embargo, es importante considerar que la información no solo tiene un valor económico, sino también un valor intrínseco para las personas, ya que es vital para la fluidez y la seguridad jurídica, y para los sistemas que la procesan. Estos sistemas pueden equipararse a bienes tradicionalmente protegidos, como el patrimonio (en casos de fraude informático), la reserva y confidencialidad de datos (en delitos que afectan la intimidad), o la seguridad del tráfico probatorio (en la falsificación de datos o documentos). Por lo tanto, en los delitos informáticos, no puede limitarse la información como el único bien jurídico afectado, sino que debe entenderse como parte de un conjunto de bienes que se ven comprometidos. Esto se debe a la naturaleza de la conducta típica en esta modalidad delictiva, que afecta diversos intereses colectivos. En este sentido, coincidimos en que es fundamental reconocer la complejidad de los bienes jurídicos involucrados en los delitos informáticos

2.11. Fraude informático, relación con otros ilícitos de la parte especial

El fraude informático, en una definición inicial, se relaciona con la generación de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas en sistemas informáticos. Esta perspectiva se considera una aproximación estricta, que enmarca el fraude informático en un contexto específico. Sin embargo, también existen concepciones más amplias del término.

Desde una visión más amplia, el fraude informático abarca otras conductas. Por un lado, se incluyen acciones que no necesariamente generan directamente un perjuicio patrimonial, sino que buscan obtener datos esenciales para causarlo en un momento posterior. Por otro lado, cuando se deja en segundo plano el medio utilizado (la manipulación o alteración de datos) y se focaliza en el resultado de daño a intereses patrimoniales mediante sistemas informáticos, el fraude informático puede confundirse con otros delitos de la Parte Especial del Código Penal que afectan al mismo bien jurídico y que también pueden realizarse mediante sistemas tecnológicos.

Dada esta ambigüedad, es recomendable adoptar una definición precisa y estricta del fraude informático, basada en tres elementos fundamentales: la conducta, el resultado y el ánimo del agente. Sin embargo, antes de definir claramente el fraude informático, es necesario diferenciarlo de otros delitos similares que, a nivel doctrinal y normativo, tradicionalmente se han vinculado a este.

2.11.1. Fraude informático, phishing y pharming

El fraude informático suele relacionarse con el phishing y en menor medida con el pharming. En la práctica, la ejecución de operaciones bancarias en línea proporciona un contexto ideal para fraudes informáticos, como el phishing, que se basa en obtener de manera fraudulenta información personal y bancaria de usuarios para realizar

transacciones ilícitas a favor del autor o de terceros (Miró Llinares, 2012; Kochheim, 2015). En términos simples, el phishing “pesca” datos personales aprovechando que las víctimas, de manera consciente o inconsciente, revelan información confidencial (Miró Llinares, 2013). Dado que implica el uso de datos ajenos, suele vincularse con el robo de identidad (Brody, Mulig y Kimball, 2007), lo cual se facilita en el entorno anónimo del ciberespacio (Brunst, 2009; Agustina, 2009).

El phishing ha evolucionado en sus métodos de ejecución. En sus inicios, se recurría a técnicas de "ingeniería social" (Flores Mendoza, 2014), que buscaban manipular al usuario para que proporcionara información confidencial a través de correos electrónicos falsos de entidades confiables (Krombholz et al., 2014; Rosenblut, 2008; Herzog, 2009). Estos correos solían incluir advertencias de cancelación de cuentas, lo que forzaba a los usuarios a facilitar datos personales (Fernández Teruelo, 2011). Ante esta modalidad, las instituciones bancarias implementaron medidas de alerta para que sus clientes ignoraran estos correos.

Sin embargo, al verse descubierto este método, el phishing avanzó hacia el uso de software malicioso (malware) para obtener datos sin interacción humana, eliminando la necesidad de convencer a la víctima (Kochheim, 2015; San Juan, Vozmediano y Vergara, 2009). Este cambio en la técnica hizo que el phishing se asemejara más al ámbito de la criminalidad informática que al fraude basado en engaño directo.

En algunos casos, el phishing implica únicamente la obtención de datos que posteriormente son vendidos para que otros realicen el fraude (Oxman, 2013). Otra modalidad involucra a intermediarios o "mulas", quienes prestan sus cuentas bancarias para transferir el dinero obtenido ilícitamente (Fernández Teruelo, 2011; Miró Llinares, 2013).

Dado que el fraude informático implica la manipulación de sistemas para perjudicar el patrimonio, el phishing en su forma inicial no cumple con esta definición, ya que no altera directamente los datos de los sistemas informáticos. No obstante, la obtención de datos a través de malware en la segunda fase de desarrollo del phishing podría ser calificada como espionaje informático, en lugar de fraude, pues no siempre ocasiona un perjuicio patrimonial directo a la víctima.

Por otro lado, el **pharming** implica la creación de un sitio web falso que simula el de una entidad bancaria (Miró Llinares, 2012; Kochheim, 2015), redirigiendo a los usuarios a estas páginas para que ingresen datos confidenciales. Esta técnica es considerada más sofisticada que el phishing, ya que modifica el DNS del usuario para engañarlo, permitiendo al atacante acceder a información sensible sin necesidad de correo engañoso (Flores Mendoza, 2014). Aunque el pharming implica la manipulación de datos, no necesariamente constituye un fraude informático hasta que se produzcan transferencias o cargos en la cuenta de la víctima.

Desde el punto de vista legal, el pharming en su forma básica podría ser considerado un acto preparatorio del fraude informático o una forma de sabotaje informático (alteración de datos) o falsificación informática. Sin embargo, las dificultades legales surgen si se entiende que la intención del atacante no es dañar directamente los datos, sino emplearlos con fines ilícitos para obtener beneficios económicos.

Ambas modalidades, phishing y pharming, destacan en el panorama de los fraudes informáticos y presentan desafíos en su tipificación jurídica, al combinar elementos de manipulación de datos, robo de identidad y fraude patrimonial en un contexto digital complejo.

2.11.2. Fraude informático, espionaje informático (o hacking) y sabotaje informático

Es posible establecer conexiones entre el fraude informático y otros ciberdelitos, como el espionaje informático (o hacking) y el sabotaje informático.

En primer lugar, estos delitos están relacionados porque todos afectan a los "datos informáticos". Según el artículo 1, letra b) del Convenio sobre Ciberdelincuencia del Consejo de Europa (CCCE), los datos informáticos se definen como "toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función".

Además, cuando estos delitos se cometen en el ciberespacio, comparten un bien jurídico común denominado funcionalidad informática, aunque también pueden afectar otros intereses públicos o privados.

Debido a que estos delitos forman parte de la delincuencia informática, comparten elementos criminológicos específicos de este ámbito, como las condiciones favorables que ofrece el ciberespacio para llevar a cabo actividades transnacionales (Miró Llinares, 2012) y los efectos perjudiciales que pueden tener para un gran número de víctimas potenciales (Sieber, 2014).

Desde el punto de vista de la conducta delictiva, el espionaje informático implica acceder y conocer datos de sistemas informáticos de manera indebida. Tanto el fraude informático como el sabotaje informático requieren este acceso y conocimiento previo de los datos. En el caso del fraude informático, para manipular o alterar datos o programas de sistemas de tratamiento automatizado de la información con el fin de causar un daño en intereses patrimoniales ajenos, es necesario un acceso y conocimiento indebido previo de

dichos datos. Por lo tanto, el espionaje informático se convierte en un "delito presupuesto" del fraude informático.

De manera similar, para destruir o inutilizar datos de sistemas informáticos en el sabotaje informático, también se requiere un acceso y conocimiento indebido previo de dichos datos. Así, el espionaje informático también se convierte en un "delito presupuesto" del sabotaje informático. Este vínculo entre el espionaje informático y el sabotaje informático es relevante en relación con el fraude informático, ya que, en ausencia de una norma específica que sancione este último delito en la Ley 19.223, del 7 de junio de 1993, se puede recurrir a la tipificación del sabotaje informático para evitar la impunidad.

Por otro lado, al analizar las relaciones concursales entre estos tres delitos (fraude, espionaje y sabotaje informático), se pueden distinguir dos tipos de vínculos: uno entre el espionaje informático y el sabotaje informático, y otro entre el espionaje informático y el fraude informático. En primer lugar, la sistemática de la Ley 19.223 sugiere la regulación de delitos de aplicación alternativa, y las penas para el espionaje informático y el sabotaje informático no prevén una regla explícita de acumulación aritmética. Esto sugiere la existencia de un concurso de leyes que se resuelve a favor del sabotaje informático según el principio de absorción. En segundo lugar, aunque no existe un tipo penal específico de fraude informático en el derecho chileno, las conductas que pueden calificarse como tales se subsumen en el tipo penal de sabotaje informático (ya que implican la modificación de datos). Por lo tanto, también se puede afirmar un concurso de leyes entre el espionaje informático y el sabotaje informático, que se resuelve a favor del sabotaje informático según el principio de absorción.

2.11.3. Fraude informático y estafa

El vínculo entre el fraude informático y la estafa es bastante evidente, al punto que los ordenamientos jurídicos alemán y español los regulan de manera sucesiva o conjunta,

respectivamente, pues parten de la base de que ambos afectan intereses patrimoniales ajenos, aunque a través de distintos medios. Esta forma de regulación ha llevado a que en la doctrina comparada se hable de tipos penales "paralelos" (Eisele, 2013; De la Mata Barranco y Hernández Díaz, 2010; Hilgendorf y Valerius, 2012; Picotti, 2013). En algunos casos, la legislación alemana alude a "estafa" y "estafa computacional" para diferenciar entre la estafa en sentido estricto y el fraude informático.

Sin embargo, esta referencia puede ser considerada impropia, ya que la estructura típica del fraude informático es diversa a la de la estafa (Faraldo Cabana, 2007). La estafa requiere un engaño, un error, una disposición patrimonial y un perjuicio patrimonial, elementos que deben estar vinculados por una relación de causalidad (Etcheberry, 2010; Kindhäuser, 1999). El error, entendido como una falsa representación de la realidad, solo puede ser cometido por una persona natural (Etcheberry, 2010; Jijena Leiva, 2008; Politoff, Matus y Ramírez, 2011). Conceptualmente, las máquinas no pueden ser engañadas en el sentido del tipo penal de estafa (Hernández Basualto, 2003).

Por este motivo, no puede castigarse como estafa la realización de conductas fraudulentas "respecto de" o "contra" un sistema de tratamiento automatizado de la información, ya que lo afectado es una computadora y no una persona. Estas conductas suelen corresponder a hipótesis de fraude informático, que se identifica con la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos.

Estas hipótesis deben distinguirse de los fraudes llevados a cabo "mediante" o "a través" de computadoras, que son subsumibles en el delito de estafa. Estos fraudes no se diferencian en términos relevantes de lo que se denomina "estafa telefónica", que es un fraude por engaño ejecutado a través de un teléfono. De manera similar, una estafa puede perpetrarse mediante la comunicación con la víctima a través de una computadora, por

ejemplo, mediante el envío de mensajes fraudulentos a través de un sitio de venta o subasta en internet.

La doctrina minoritaria, representada en Chile por Balmaceda Hoyos, sostiene que no existen inconvenientes para subsumir conductas constitutivas de fraude informático en el tipo penal de estafa (Balmaceda Hoyos, 2009). Esta tesis descarta que el error sea un elemento autónomo del ilícito y considera que el engaño no requiere como receptor a una persona física, sino que basta con que el falseamiento intencional de la realidad se exteriorice. Además, asume que quien efectúa la disposición patrimonial determinada por error no es la máquina, sino la persona natural que previamente la ha programado.

Sin embargo, esta tesis minoritaria choca con la forma en que el delito de estafa se encuentra tipificado en el ordenamiento jurídico penal, que parte de la base de que existe un sujeto que comete el fraude y otro que lo sufre. La estafa implica un vínculo entre personas, ya que solo entre ellas es posible que concurra el necesario proceso comunicativo de atribución de relevancia y significado a determinados actos y hechos. Este proceso comunicativo justifica que la estafa sea calificada como un "delito de comunicación", en el que debe verificarse una interacción comunicativa entre el autor del engaño y el disponente del patrimonio que incurre en error.

2.11.4. Uso fraudulento de tarjetas de pago y transacciones electrónicas

La Ley 21.234, promulgada el 29 de mayo de 2020, introdujo modificaciones significativas a la Ley 20.009, que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en casos de extravío, hurto, robo o fraude. Originalmente, la Ley 20.009 ya contemplaba el delito de uso indebido de tarjetas falsificadas o sustraídas y de sus claves, pero con la nueva ley, este delito fue trasladado y ampliado en el artículo 7.

El artículo 7, en su inciso segundo, establece sanciones para el uso fraudulento de tarjetas de pago y transacciones electrónicas, castigando a quienes, mediante engaño o simulación, obtengan o vulneren la información y medidas de seguridad de cuentas bancarias o tarjetas de pago para suplantar al titular y efectuar pagos o transacciones electrónicas.

Este tipo penal se relaciona con el fraude informático, ya que ambos delitos suelen involucrar transferencias electrónicas de fondos. Sin embargo, el uso fraudulento de tarjetas de pago y transacciones electrónicas requiere el empleo de tecnologías, lo que lo diferencia de los delitos informáticos en sentido estricto, que afectan directamente a los datos o sistemas informáticos.

Además, el artículo 7 incluye el elemento de engaño o simulación, lo que implica una interacción comunicativa entre personas, a diferencia del fraude informático, que se caracteriza por la manipulación de datos sin necesidad de interacción entre individuos. Aunque el artículo 7 menciona pagos o transacciones electrónicas, no siempre implica un fraude informático, ya que puede haber engaño sin manipulación de datos.

Otra diferencia clave es que el fraude informático requiere la provocación de un perjuicio patrimonial ajeno para que se considere consumado, mientras que el uso fraudulento de tarjetas de pago y transacciones electrónicas no establece exigencias subjetivas particulares y puede cometerse con dolo eventual.

En resumen, aunque el artículo 7 de la Ley 20.009 se relaciona con el fraude informático en cuanto al uso de tecnologías, ambos delitos difieren en su estructura típica, objeto material y elementos subjetivos.

2.12. Las dificultades en la investigación de delitos de fraude informático

La investigación del delito de fraude informático se refiere al proceso mediante el cual las autoridades y organismos especializados recopilan, analizan y presentan pruebas para identificar, procesar y condenar a los responsables de cometer fraudes a través de medios digitales. Este proceso incluye la identificación de las técnicas utilizadas por los delincuentes, la preservación de pruebas digitales, y la cooperación con otras entidades para rastrear y detener a los culpables. (Ávila Trivelli, 2023).

a. **Falta de Recursos Tecnológicos:** La falta de recursos tecnológicos se refiere a la insuficiencia de herramientas y sistemas tecnológicos necesarios para llevar a cabo investigaciones y operaciones de manera eficiente. En el contexto de la investigación de fraudes informáticos, esta carencia puede incluir la falta de software especializado, hardware adecuado y acceso a tecnologías avanzadas de análisis de datos. Según Mayer y Oliver (2020), la insuficiencia de recursos tecnológicos limita significativamente la capacidad de las instituciones para enfrentar y resolver casos de fraude informático de manera efectiva. (Mayer 2020 Pag.151-168).

b. **Falta de Recursos Humanos y Capacitación Insuficiente del Personal:** La falta de recursos humanos y la insuficiente capacitación del personal se refieren a la escasez de personal calificado y la falta de formación adecuada para enfrentar los desafíos del fraude informático. Esto incluye la necesidad de especialistas en ciberseguridad, analistas de datos y personal de TI con conocimientos avanzados en la detección y prevención de fraudes. Según Gutiérrez Francés (1991), la falta de capacitación especializada y la escasez

de personal capacitado son factores críticos que afectan la eficacia de las investigaciones de fraudes informáticos.

c. **Deficiencias en el Marco Legal:** Las deficiencias en el marco legal se refieren a la falta de leyes y regulaciones adecuadas para abordar y sancionar los fraudes informáticos. Un marco legal insuficiente puede dificultar la persecución y el castigo de los delincuentes, así como la protección de las víctimas. Según Miró Llinares (2013), la rápida evolución de la tecnología y las técnicas de ciberdelincuencia requiere una actualización constante de las leyes para mantener su eficacia en la lucha contra el fraude informático. Miró Llinares, F. (2013, Pág. 3-25)

2.13. La investigación del delito de fraude informático

se refiere al proceso mediante el cual las autoridades y organismos especializados recopilan, analizan y presentan pruebas para identificar, procesar y condenar a los responsables de cometer fraudes a través de medios digitales. Este proceso incluye la identificación de las técnicas utilizadas por los delincuentes, la preservación de pruebas digitales, y la cooperación con otras entidades para rastrear y detener a los culpables. (Ávila Trivelli, 2023).

a. **Identificación de las Modalidades Utilizadas por los Delincuentes:** La identificación de las modalidades utilizadas por los delincuentes se refiere al proceso de reconocer y catalogar las diferentes técnicas y métodos que los ciberdelincuentes emplean para cometer fraudes informáticos. Esto incluye el análisis de patrones de comportamiento, la detección de nuevas tácticas y la comprensión de cómo los delincuentes adaptan sus estrategias para evadir la detección. Según Mayer y Oliver (2020), la identificación

precisa de estas modalidades es crucial para desarrollar contramedidas efectivas y mejorar la seguridad cibernética.

b. **Preservación de Pruebas Digitales:** La preservación de pruebas digitales implica la recolección, almacenamiento y protección de datos electrónicos que pueden ser utilizados como evidencia en investigaciones de fraudes informáticos. Este proceso es fundamental para asegurar la integridad y autenticidad de las pruebas, permitiendo que sean admisibles en procedimientos legales. Según Gutiérrez Francés (1991), la preservación adecuada de pruebas digitales es un componente esencial de cualquier investigación de ciberdelincuencia, ya que garantiza que la evidencia no sea alterada o destruida.

c. **Cooperación Interinstitucional:** La cooperación interinstitucional se refiere a la colaboración y coordinación entre diferentes entidades, como agencias gubernamentales, empresas privadas y organizaciones internacionales, para combatir el fraude informático. Esta cooperación es esencial para compartir información, recursos y estrategias, y para coordinar esfuerzos en la lucha contra la ciberdelincuencia. Según Miró Llinares (2013), la cooperación interinstitucional es un factor clave para enfrentar los desafíos del fraude informático de manera efectiva, ya que permite una respuesta más rápida y coordinada ante las amenazas.

2.14. Marco conceptual

a. Activo Patrimonial: Conjunto de bienes y derechos que conforman el patrimonio de una persona, ya sea natural o jurídica.

b. Base de Datos: Conjunto de archivos organizados en formato digital que contienen información general o especializada, disponibles para múltiples usuarios.

c. Browser (Navegador): Programa informático utilizado para buscar y acceder a información en la World Wide Web (WWW). Los más comunes son Microsoft Explorer, Firefox y Opera.

d. Cookie: Archivo que se almacena en el ordenador del usuario cuando se conecta a un servidor o sistema, utilizado para registrar información sobre las páginas visitadas y preferencias personalizadas. Muchos usuarios consideran esto una invasión a su privacidad, ya que los sistemas generalmente no informan sobre el uso de estos datos. Existen programas que eliminan estos archivos automáticamente entre visitas.

e. Dialup (Conexión por Marcado): Método para acceder a Internet mediante una línea telefónica convencional a través de un módem, en lugar de usar una red local (LAN) o una línea telefónica fija. Es comúnmente utilizado en hogares sin una conexión avanzada contratada.

f. Firma Digital: Equivalente electrónico a una firma manuscrita, utilizada para autenticar la autoría o aprobación de un documento digital.

g. Documento Electrónico: Representación digital de hechos jurídicos relevantes que pueden ser almacenados, procesados o transmitidos electrónicamente.

h. HTTP (Protocolo de Transferencia de Hipertexto): Protocolo utilizado en Internet para solicitar y transmitir páginas web y otros tipos de información. Se indica al principio de una URL (por ejemplo, "http://") para que el navegador utilice este protocolo para acceder a la página solicitada.

i. Proveedor de Servicios de Internet (ISP): Entidad o empresa que proporciona acceso a Internet y otros servicios relacionados, como alojamiento web y administración de nombres de dominio.

j. Mensaje de Datos: Información generada, enviada, recibida, almacenada o comunicada mediante medios electrónicos, informáticos, ópticos o digitales.

k. Módem: Dispositivo que convierte los datos de una computadora en un formato que puede ser transmitido a través de líneas telefónicas u otros medios de comunicación.

l. Sistema Telemático: Conjunto de redes de telecomunicaciones que permiten la transmisión, recepción y procesamiento automatizado de información.

m. Sistema de Información: Conjunto de herramientas y procesos usados para generar, enviar, recibir, almacenar o archivar mensajes de datos.

n. Sistema Informático: Conjunto organizado de hardware, software y bases de datos utilizadas para procesar, almacenar y manejar datos de forma automatizada.

o. Sociedad de la Información: La transformación digital impulsada por las tecnologías de la información y las comunicaciones (TIC) ha creado una infraestructura global que facilita el intercambio de información, conocimientos y recursos. Esto ha impactado de manera profunda la manera en que las sociedades interaccionan, tanto en los países desarrollados como en los en desarrollo, al proporcionar nuevas oportunidades para el progreso social, económico y educativo.

p. Soporte Lógico: Elementos como tarjetas perforadas, cintas magnéticas o discos ópticos que se utilizan para almacenar información en un sistema informático.

q. Soporte Material: Cualquier elemento físico empleado para registrar o almacenar información en diferentes formatos.

r. Telemática: Término que hace referencia a la transmisión automatizada de información a través de redes de telecomunicaciones, combinando las áreas de telecomunicación e informática.

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Enfoque de investigación

Se tuvo un enfoque mixto, Hernández-Sampieri et al. (2014), enfatiza en que, “La meta de la investigación mixta no es reemplazar a la investigación cuantitativa ni a la investigación cualitativa, sino utilizar las fortalezas de ambos tipos de indagación, combinándolas y tratando de minimizar sus debilidades potenciales.” (p. 532)

3.2. Nivel de investigación

El presente trabajo de investigación es de ***nivel descriptivo-explicativo,*** ya que tiene como función primordial especificar las características del objeto de investigación. La investigación descriptiva se define como un método de investigación que describe las características de un determinado grupo, situación o fenómeno. El objetivo no es establecer relaciones causa-efecto, sino ofrecer una descripción detallada de la situación.

3.3. Tipo de investigación

La presente ***investigación es aplicada,*** ya que tiene por objetivo resolver un determinado problema o planteamiento específico, enfocándose en la búsqueda y consolidación del conocimiento para su aplicación y, por ende, para el enriquecimiento del desarrollo científico.

3.4. Método de la Investigación

Se usó el método deductivo es un procedimiento de investigación que utiliza un tipo de pensamiento que va desde un razonamiento más general y lógico, basado en leyes o principios, hasta un hecho concreto. Es decir, es un método lógico que sirve para extraer conclusiones a partir de una serie de principios.

3.5. Diseño de la investigación

Este estudio se considera no experimental, ya que no implica la alteración deliberada de ninguna variable, sino que se limita a observar y analizar el fenómeno en su ambiente natural, sin que el investigador intervenga activamente. Además, se califica como

retrospectivo, dado que los datos se recopilan a partir de registros previos, como los requerimientos de prisión preventiva ya solicitados, sin que el investigador esté involucrado en la recopilación en tiempo real.

3.6. Población y Muestra

3.6.1. Población

La población está constituida por 56 las investigaciones de fraude informático en la Fiscalía provincial penal corporativa de Huamanga desde enero a diciembre de 2023. (tabla 01)

La población de encuestados se encuentra constituida por abogados litigantes especializados en derecho penal y procesal penal, de la provincia de Huamanga, y por los fiscales de las seis fiscalías provinciales que integran la Fiscalía Provincial Penal Corporativa de Huamanga, del distrito Fiscal de Ayacucho.

3.6.2. Muestra

La muestra se conforma por 10 carpetas fiscales de fraude informático de la fiscalía provincial penal de huamanga desde enero a diciembre de 2023 y por 30 encuestados de los cuales, 18 son abogados con conocimientos especializados en derecho penal y procesal penal y 12 son fiscales de la Fiscalía Provincial Penal Corporativa de Huamanga, del Distrito Fiscal de Ayacucho.

3.6.2.1. Tipo de muestra

La presente investigación utiliza el tipo de **Muestreo no probabilístico,** ello debido a que la muestra no probabilística para el autor. **“**Es aquella muestra que se extrae de una población donde su selección no puede ser de manera aleatoria, si no que bajo ciertos parámetros establecidos bajo los criterios de la investigación**”**. (Sanchez, 2016, p. 180).

Asimismo, según **Hernández, Fernández y Baptista (2014)**, el muestreo no probabilístico es adecuado cuando el investigador selecciona intencionalmente a los participantes debido a sus características específicas, conocimiento o experiencias relacionadas con el objeto de estudio (p. 174). En el caso de la presente investigación, el

enfoque se centró en fiscales y abogados con experiencia en delitos de fraude informático, lo que requirió una selección deliberada de los participantes, del mismo modo, la selección de las 10 carpetas fiscales **de fraude informático.**

3.1. Variables e indicadores

3.1.1. Variable independiente

Las dificultades en la investigación de delitos de fraude informático: Las dificultades en la investigación de delitos de fraude informático se refieren a los obstáculos y limitaciones que enfrentan las autoridades y organismos encargados de investigar y perseguir este tipo de delitos. Estas dificultades pueden incluir la falta de recursos tecnológicos y humanos, la insuficiente capacitación del personal, las deficiencias en el marco legal, y la complejidad inherente a la naturaleza digital de las pruebas. (Ávila Trivelli, 2023).

3.1.2. Variable dependiente

Investigación de delitos de fraude informático: se refiere al proceso mediante el cual las autoridades y organismos especializados recopilan, analizan y presentan pruebas para identificar, procesar y condenar a los responsables de cometer fraudes a través de medios digitales. Este proceso incluye la identificación de las técnicas utilizadas por los delincuentes, la preservación de pruebas digitales, y la cooperación con otras entidades para rastrear y detener a los culpables. (Ávila Trivelli, 2023).

3.2. Operacionalización de variables e indicadores

Variables	Definición conceptual	Dimensiones	Indicadores	Items	Escala de medición
Variable independiente: Las dificultades en la investigación de delitos de fraude informático	Las dificultades en la investigación de delitos de fraude informático se refieren a los obstáculos y limitaciones que enfrentan las autoridades y organismos encargados de investigar y perseguir este tipo de delitos. Estas dificultades pueden incluir la falta de recursos tecnológicos y humanos, la insuficiente capacitación del personal, las deficiencias en el marco legal, y la complejidad inherente a la naturaleza digital de las pruebas. (Ávila Trivelli, 2023).	La falta de recursos tecnológicos	Disponibilidad de herramientas adecuadas para análisis forense digital Acceso a redes y sistemas seguros para el manejo de pruebas	1. ¿Las herramientas tecnológicas disponibles para el análisis de fraudes informáticos son suficientes y adecuadas? 2. ¿Existen redes y sistemas seguros para almacenar y analizar las pruebas en fraudes informáticos? 3. ¿El personal disponible es suficiente para abordar la carga de casos de fraude informático.? 4. ¿El equipo cuenta con la especialización necesaria para investigar fraudes informáticos? 5. ¿Es posible asignar personal especializado a los casos de fraude informático complejos?	LIKERT: 1: Siempre 2: casi siempre 3.Algunas veces 3: Nunca 4.Casi nunca
		La falta de recursos humanos e insuficiente capacitación del personal	Suficiencia de personal capacitado para investigar fraudes informáticos. Nivel de especialización del personal en delitos informáticos. Capacidad para asignar personal especializado a los casos de alta complejidad. Frecuencia y calidad de la capacitación en delitos informáticos:		
		Las deficiencias en el marco legal	Adecuación del marco legal para la persecución del fraude informático. Suficiencia de regulaciones específicas para delitos informáticos:		

Variables		Dimensiones			
Variable Dependiente: investigación de delitos de fraude informático.	La **investigación del delito de fraude informático** se refiere al proceso mediante el cual las autoridades y organismos especializados recopilan, analizan y presentan pruebas para identificar, procesar y condenar a los responsables de cometer fraudes a través de medios digitales. Este proceso incluye la identificación de las técnicas utilizadas por los delincuentes, la preservación de pruebas digitales, y la cooperación con otras entidades para rastrear y detener a los culpables. (Ávila Trivelli, 2023).	La identificación de las modalidades utilizadas por los delincuentes	Phishing Carding Suplantación de Identidad SIM Swapping Malware Thief Transfer Fake Apps Clonación de Tarjetas	6. ¿El personal recibe capacitación regular y adecuada sobre fraudes informáticos? 7. ¿Las leyes actuales son adecuadas para investigar y procesar casos de fraude informático? 8. ¿Existen suficientes regulaciones específicas que facilitan la investigación de fraudes informáticos? 9. ¿Existen colaboraciones frecuentes con otras instituciones en investigaciones de fraudes informáticos? 10. ¿El intercambio de información con otras entidades es eficiente y oportuno?	
		La preservación de pruebas digitales	Captura de pantalla, registro de correos electrónicos. Análisis de tráfico de red Clonación de disco duro, análisis forense Registro de llamadas, análisis de SIM Monitoreo de transacciones, registros bancarios.		
		La cooperación interinstitucional	Frecuencia de colaboración con entidades externas (por ejemplo, policía, fiscalía, instituciones financieras. Eficiencia en el intercambio de información con otras instituciones.		

CAPÍTULO VI: ANÁLISIS Y DISCUSIÓN DE RESULTADOS

4.1. Interpretación de resultados

Tabla 1: *Distribución de casos de fraude informático durante el periodo de enero a diciembre del 2023*

2023		
Cuenta de id_Único Fiscalía	**De_etapa**	**Fe_ing_ caso 2023**
1° FPPC HUAMANGA	INVESTIGACION PREPARATORIA	3
	ETAPA INTERMEDIA	1
	ETAPA DE JUZGAMIENTO	1
Total 1° FPPC HUAMANGA		**5**
2° FPPC HUAMANGA	INVESTIGACION PREPARATORIA	2
	ETAPA INTERMEDIA	1
Total 2° FPPC HUAMANGA		**3**
3° FPPC HUAMANGA	INVESTIGACION PREPARATORIA	7
	ETAPA INTERMEDIA	1
Total 3° FPPC HUAMANGA		8
4° FPPC HUAMANGA	INVESTIGACION PREPARATORIA	11
	ETAPA INTERMEDIA	2
	ETAPA JUZGAMIENTO	2
Total 4° FPPC HUAMANGA		**15**
5° FPPC HUAMANGA	INVESTIGACION PREPARATORIA	8
	ETAPA INTERMEDIA	1
Total 5° FPPC HUAMANGA		**9**
6° FPPC HUAMANGA	INVESTIGACION PREPARATORIA	11
	ETAPA INTERMEDIA	3
	ETAPA DE JUZGAMIENTO	2
Total 6° FPPC HUAMANGA		**16**
TOTAL GENERAL		**56**

Fuente: Fiscalía Provincial Penal Corporativa de Huamanga

En tabla uno se muestra la distribución de casos de fraude informático durante el periodo de enero a diciembre del 2023, siendo el total de 56 casos.

4.1.1. Resultados del análisis documental

Tabla 2: *Descripción de las Carpetas Fiscales*

C.F.	DATOS DE LA FICHA DOCUMENTAL
1	La denuncia policial verbal formulada por la persona de Victoria S.P por la presunta comisión del delito contra el Patrimonio en la modalidad de FRAUDE INFORMÁTICO, delito previsto y sancionado en el artículo 8 de la ley de Delitos Informáticos (ley 30096), en agravio de la denunciante; y, Conforme a la denuncia policial verbal interpuesta por Victoria S.P (69), se tiene que la denunciante el 05 de julio de 2023 a horas 16:00 aproximadamente se percató que en su cuenta de ahorros de su tarjeta de débito del BCP, había movimientos de retiros de dinero no reconocidos por la dueña de la tarjeta, la cual manifiesta que nunca ha utilizado su tarjeta física para hacer algún movimiento siendo el monto total sustraído de S/. 5000.00 soles. Tipicidad: *Se entiende por clonación el hecho de hacer una copia exacta de una cosa, en el caso en concreto se entiende por clonación de tarjetas de crédito, la consumación de un fraude, que consiste en crear una copia o almacenar datos de este medio de pago, para ser usado de manera dolosa suplantando la identidad del afectado.* ***Causa de archivamiento:*** **No se ha individualizado al imputado asimismo la denunciante no proporciono medios probatorios** Del análisis de los actuados recabados en sede policial, se puede apreciar que en el presente caso no existen suficientes elementos de prueba, que puedan ayudar al esclarecimiento de los hechos, y más aún a la debida identificación de los presuntos responsables y su grado de participación de cada uno de ellos; pues de los actuados remitidos por el Capitán PNP Ángel L. Medina Lázaro jefe del DEPINCRI-HUAMANGA, mediante Oficio N°5052-2023-VIII-MACREPOL/REGPOL-AYA/DIVINCRI-DEPINCRI-AREINCRI-G4., de fecha 12 de julio de 2023 **,** se tiene el acta de denuncia verbal de la ciudadana Victoria Sosa Pérez (69), en donde la denunciante **no proporciono los datos que puedan identificar individualmente a la persona que haya hecho uso de su tarjeta de débito del BCP para concretar los hechos materia de denuncia, asimismo la denunciante no proporciono medios probatorios (record del estado de cuenta) que acrediten que tercera persona haya hecho de su tarjeta de débito del BCP para sustraer dinero de su cuenta bancaria del BCP**
2	Conforme a la denuncia interpuesta por Andrés Ore Cahuana, quien refiere que en circunstancias que el día 06 de julio del 2023 en horas de la tarde, se encontraba revisando el saldo de su cuenta mediante la página de la Entidad Financiera Caja Huancayo – Huamanga, se percata de movimientos de transferencia por una suma total de S 30,000.00 soles, el mismo que no reconoce haber realizado dichas transferencias a nombre de Maribel Mónica Pérez Laura por el monto de S/ 5,000.00 soles; a Brynner Christohper Gressvel Cueva Villafuerte por el monto de S/ 10,000.00 soles y a Elvira Vanessa Norabuena Caldua por el monto de S/ 5,000.00 soles. ***Causa de archivamiento:*** **No aparecen indicios reveladores de la existencia de un delito.** En el presente caso, habiéndose realizado el análisis de los actuados recabados, **no se tiene medio de prueba alguno que acredite que las personas de Maribel Mónica Pérez Laura, Brynner Christohper Gressvel Cueva Villafuerte y Elvira Vanessa Norabuena Caldua, hayan realizado actos de diseño, introducción, alteración, borrado, supresión, clonación o manipulación en el funcionamiento de un sistema informático**, ya sea en calidad de autor o coautor, ni mucho menos que los denunciados hayan concertado para perpetrar los hechos denunciados

	No se ha individualizado al imputado
3	En el presente caso se advierte la Denuncia Electrónica N°06993: DL-2023-70574409-01de fecha 20 de septiembre de 2023, en donde se detalla que el 14 de agosto de 2023 la denunciante recibió un mensaje con un enlace en la cual le señalaban que el enlace pertenecía al Bono, la denunciante ingreso al link y esta le manda directamente al aplicativo Yape y de repente se elimina su cuenta de Yape, acto seguido la denunciante descargar de nuevo el aplicativo Yape y al ingresar a su cuenta se dio con la sorpresa que ya no tenía saldo en su cuenta de Yape, la denunciante señala que la persona de Jhon Kleiver Huayra Llantoy fue quien le robo. ***Causa de archivamiento:*** **No aparecen indicios reveladores de la existencia de un delito.** **No se ha individualizado al imputado** **La agraviada no asistió a declarar** **falta de persistencia en la incriminación de parte de la denunciante** en base a la denuncia interpuesta por la agraviada Anita Paredes Vargas, este Primer Despacho de la Tercera Fiscalía Provincial Penal Corporativa de Huamanga, mediante la Disposición Fiscal N° 01-2023 de fecha 26 de setiembre se dispuso aperturar investigación preliminar con la finalidad de recabar medios de prueba que coadyuven a la debida identificación de los presuntos responsables y su grado de participación de cada uno de ellos, Disposición Fiscal que fue notificada debidamente a la agraviada a su correo electrónico personal anitaparedesvargas09@gmail.com (fs. 10), correo electrónico señalado por la agraviada en su denuncia interpuesta por medio de la página Web denuncias Web del Ministerio Público, donde se le hace saber que a consecuencia de su denuncia se apertura diligencias preliminares, asimismo se le programó para el día 13 de octubre de 2023 a 10:00 horas a fin de que pueda rendir su declaración con respectos a los hechos que denunció, sin embargo **la agraviada Anita Paredes Vargas no ha concurrido a rendir su declaración programada para el día 13 de octubre de 2023 a 10:00 horas** de conformidad con las Actas de Inconcurrencia obrantes a folios 12, con esta situación se puede observar una **falta de persistencia en la incriminación de parte de la denunciante**, debido a que la persistencia en la incriminación es una garantía de certeza que no opera solo en casos en donde la víctima haya declarado en más de una ocasión, sino también tratándose de únicas en las que se expresa un relato sólido y verosímil; en ese sentido habiéndose efectuado los esfuerzos de recabar medios de pruebas que puedan ayudar en el presente caso, se ha teniéndose un resultado negativo, en consecuencia, de manera uniforme se advierte una imputación genérica e imprecisa
4	La denuncia policial verbal formulada por **María Luisa González** por la presunta comisión del delito contra el Patrimonio en la modalidad de **FRAUDE INFORMÁTICO**, delito previsto y sancionado en el artículo 8 de la ley de Delitos Informáticos (Ley 30096), en agravio de la denunciante; y, Conforme a la denuncia policial verbal interpuesta por María Luisa González (65), se tiene que la denunciante el **10 de agosto de 2023** a horas **11:30** aproximadamente, se percató que en su cuenta de ahorros de su tarjeta de débito del **Banco de Crédito del Perú (BCP)**, había movimientos de retiros de dinero no reconocidos por la dueña de la tarjeta. La denunciante afirma que nunca ha utilizado su tarjeta física para hacer algún movimiento, siendo el monto total sustraído de **S/. 7,500.00 soles**. **Tipicidad:** Se entiende por **clonación** el hecho de hacer una copia exacta de una cosa. En el caso en concreto, se refiere a la clonación de tarjetas de crédito, lo que representa la consumación de un fraude. Esto consiste en crear una copia o almacenar datos de este medio de pago para ser usado de manera dolosa, suplantando la identidad del afectado. **Causa de Archivamiento:**

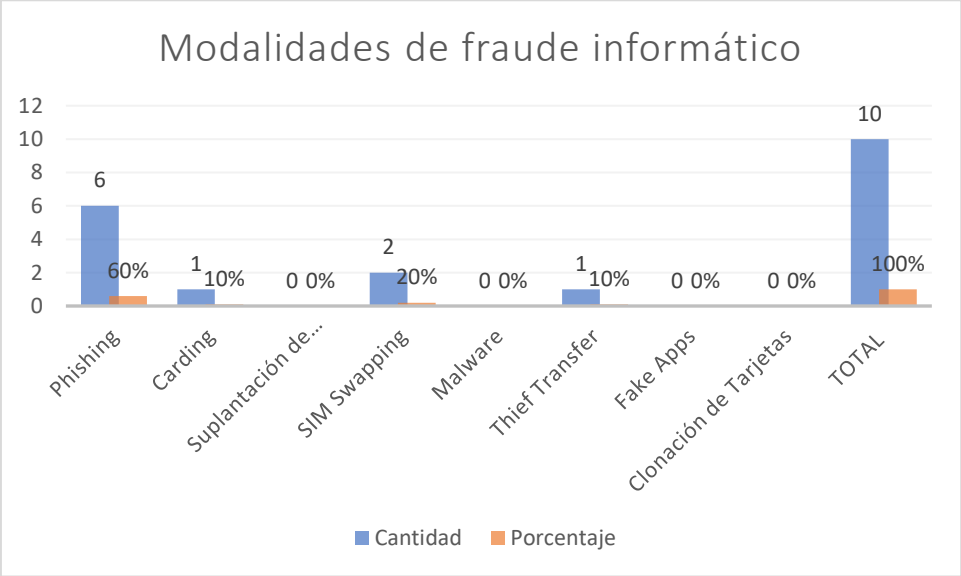
	• No se ha logrado individualizar al imputado. • La denunciante no proporcionó medios probatorios suficientes. Del análisis de los actuados recabados en sede policial, se aprecia que en el presente caso no existen suficientes elementos de prueba que puedan ayudar al esclarecimiento de los hechos, y menos aún a la debida identificación de los presuntos responsables y su grado de participación. De los actuados remitidos por el Capitán **PNP José R. Castillo Vilca**, jefe del **DEPINCRI-HUAMANGA**, mediante Oficio **N°4071-2023-VIII-MACREPOL/REGPOL-AYA/DIVINCRI-DEPINCRI-AREINCRI-G3**, de fecha **17 de agosto de 2023**, se tiene el acta de denuncia verbal de la ciudadana **María Luisa González (65)**, donde la denunciante no proporcionó datos que puedan identificar individualmente a la persona que haya hecho uso de su tarjeta de débito del **BCP** para concretar los hechos materia de la denuncia. Asimismo, la denunciante no proporcionó medios probatorios (como el récord del estado de cuenta) que acrediten que una tercera persona haya hecho uso de su tarjeta de débito del **BCP** para sustraer dinero de su cuenta bancaria.
5	Conforme a la denuncia interpuesta por **Jorge Luis Mendoza Arango**, quien refiere que, en circunstancias que el día **12 de agosto de 2023** en horas de la mañana, se encontraba revisando el saldo de su cuenta mediante la página de la **Entidad Financiera Caja Arequipa – Huamanga**, se percata de movimientos de transferencia por una suma total de **S/ 28,000.00 soles**, los cuales no reconoce haber realizado. Las transferencias fueron dirigidas a **Carla Jimena Solano Paredes** por el monto de **S/ 7,000.00 soles**; a **Luis Alejandro Campos Rivera** por el monto de **S/ 12,000.00 soles**, y a **Isabel Andrea Torres Ramírez** por el monto de **S/ 9,000.00 soles**. **Causa de Archivamiento:** • No aparecen indicios reveladores de la existencia de un delito. En el presente caso, habiéndose realizado el análisis de los actuados recabados, no se tiene medio de prueba alguno que acredite que las personas de **Carla Jimena Solano Paredes**, **Luis Alejandro Campos Rivera**, e **Isabel Andrea Torres Ramírez**, hayan realizado actos de diseño, introducción, alteración, borrado, supresión, clonación o manipulación en el funcionamiento de un sistema informático, ya sea en calidad de autor o coautor. Tampoco se ha encontrado evidencia que indique que los denunciados hayan concertado para perpetrar los hechos denunciados. • No se ha individualizado al imputado.
6	Conforme a la denuncia interpuesta por **David Mamani Cutipa**, un mototaxista, quien reporta haber sido víctima de un robo cibernético de **S/ 6,000** el pasado **11 de noviembre de 2023**. El denunciante detalla que el problema comenzó cuando su celular comenzó a presentar fallas en la señal. Tras contactar a **Movistar** para investigar el problema con su línea telefónica y no obtener solución, la entidad recomendó que adquiriera un nuevo chip en una agencia autorizada. El mismo día, **Mamani** compró un nuevo chip por la mañana y pudo utilizar sus aplicaciones sin problemas. Sin embargo, alrededor de las **2 p.m.**, recibió una llamada del banco **BBVA**, consultándole si había realizado una transferencia de **S/ 6,000**. Al recibir esta llamada, **Mamani** regresó a la agencia de Movistar, preocupado por la posibilidad de que le hubieran cambiado el chip para realizar el robo. El **12 de noviembre**, cuando fue a reclamar, recibió un reporte indicando que, a las **10:58 a.m.**, había adquirido el nuevo chip. No obstante, también apareció un reporte de que alguien había suplantado su identidad y comprado un chip a las **00:07 a.m.** **Causa de Archivamiento:** • **No aparecen indicios reveladores de la existencia de un delito.** • **No se ha individualizado al imputado.** • **La víctima no asistió a declarar.** • **Falta de persistencia en la incriminación por parte del denunciante.** En base a la denuncia interpuesta por **David Mamani Cutipa**, este Primer Despacho de la

	Tercera Fiscalía Provincial Penal Corporativa de Huamanga, mediante la **Disposición Fiscal N° 03-2023** de fecha **15 de noviembre de 2023**, dispuso la apertura de una investigación preliminar con la finalidad de recabar medios de prueba que ayuden a identificar a los presuntos responsables y determinar su grado de participación en el delito. Esta Disposición Fiscal fue notificada debidamente a la agraviada a su correo electrónico personal **davidmamani23@gmail.com** (fs. 8), dirección proporcionada en la denuncia presentada a través de la página Web del Ministerio Público. En la notificación, se informó a **Mamani** que, como consecuencia de su denuncia, se iniciaron diligencias preliminares, y se le programó una cita para el **22 de noviembre de 2023 a las 10:00 horas** para que pudiera rendir su declaración sobre los hechos denunciados. Sin embargo, el denunciante **David Mamani Cutipa** no asistió a la declaración programada para el **22 de noviembre de 2023**, según consta en las Actas de Inasistencia obrantes en folios 10. Esta situación revela una falta de persistencia en la incriminación por parte del denunciante, dado que la persistencia en la acusación es una garantía de certeza que no solo se aplica cuando la víctima ha declarado en varias ocasiones, sino también en casos donde se requiere un relato sólido y coherente. A pesar de los esfuerzos realizados para recabar medios de prueba que pudieran contribuir al esclarecimiento del caso, se obtuvo un resultado negativo. Por lo tanto, se observa una imputación genérica e imprecisa, y se recomienda el archivamiento del caso.
7	La Sexta Fiscalía Provincial Penal Corporativa de Huamanga en Huamanga, junto con el personal de la División de Investigación Criminal, llevó a cabo una orden judicial de allanamiento y descerraje en el domicilio de la imputada Magaly Infante Beltrán. Esta acción forma parte de la investigación preliminar por los delitos de hurto agravado, fraude informático y falsificación de documentos privados, en perjuicio de una cooperativa. La intervención se realizó en una vivienda situada en Avenida Señor de Quinuapata, en el distrito de Huamanga. Durante el allanamiento, el fiscal provincial Oliverio García Quilca descubrió y registró varios elementos clave: dinero en efectivo, tarjetas de crédito y débito, comprobantes de retiro de dinero efectuados por los socios de la cooperativa agraviada, así como diversos documentos relevantes para la investigación. Este material será utilizado como prueba en el proceso para esclarecer los hechos y determinar el grado de responsabilidad penal de la imputada. **Causa de Archivamiento:** • **No aparecen indicios reveladores de la existencia de un delito.** • **No se ha individualizado al imputado.** • **La víctima no asistió a declarar.** • **Falta de persistencia en la incriminación por parte del denunciante.**
8	De acuerdo con las declaraciones del afectado, el delito ocurrió al mediodía del domingo 7 de noviembre del presente año. El fraude se realizó a través de un supuesto pago a Uber el afectado se dirigió a la agencia de Interbank en Huamanga para denunciar el delito. En la agencia, fue atendido por una funcionaria del área de operaciones, quien le informó que el pago no había sido efectuado y que estaba en condición de saldo contable. La funcionaria le explicó que había un periodo mínimo de 48 horas para que el pago se hiciera efectivo. A pesar de la denuncia realizada el lunes 8 de noviembre, el día martes 9 el Banco procedió con el pago fraudulento. Actualmente, el Banco no reconoce su responsabilidad en el caso. **Causa de Archivamiento:** • **No aparecen indicios reveladores de la existencia de un delito.** • **No se ha individualizado al imputado.** • **La agraviada no asistió a declarar.** • **Falta de persistencia en la incriminación por parte de la denunciante.**
9	En el presente caso, se observa la **Denuncia** de fecha **28 de septiembre de 2023**, en la que se detalla que el **18 de agosto de 2023**, la denunciante recibió un mensaje con un enlace que supuestamente estaba relacionado con un bono económico. La denunciante, al ingresar al

	link, fue redirigida al aplicativo de Yape, y de repente, su cuenta de Yape fue eliminada. Posteriormente, la denunciante descargó nuevamente la aplicación y, al ingresar a su cuenta, descubrió que ya no tenía saldo disponible. La denunciante afirma que la persona de **Luis Enrique Ramos Cárdenas** fue quien cometió el robo. **5. Causa de Archivamiento:** • **No aparecen indicios reveladores de la existencia de un delito.** • **No se ha individualizado al imputado.** • **La agraviada no asistió a declarar.** • **Falta de persistencia en la incriminación por parte de la denunciante.** Basándose en la denuncia interpuesta por la agraviada **Lucía Rojas Fernández**, este Primer Despacho de la Tercera Fiscalía Provincial Penal Corporativa de Huamanga, mediante la **Disposición Fiscal N° 02-2023** de fecha **5 de octubre**, dispuso la apertura de una investigación preliminar con la finalidad de recabar medios de prueba que ayuden a la identificación de los presuntos responsables y su grado de participación. Esta Disposición Fiscal fue notificada debidamente a la agraviada a su correo electrónico personal **luciarojasfernandez23@gmail.com** (fs. 12), dirección que la agraviada proporcionó en su denuncia presentada a través de la página Web del Ministerio Público. En esta notificación, se informó a la denunciante que, como consecuencia de su denuncia, se iniciaron diligencias preliminares, y se le programó una cita para el **20 de octubre de 2023 a las 11:00 horas** para que pudiera rendir su declaración sobre los hechos denunciados. Sin embargo, la agraviada **Lucía Rojas Fernández** no compareció a rendir su declaración en la fecha programada, según consta en las Actas de Inasistencia obrantes en folios 14. Esta situación revela una falta de persistencia en la incriminación por parte de la denunciante, ya que la persistencia en la acusación es una garantía de certeza que no solo se aplica cuando la víctima ha declarado en múltiples ocasiones, sino también en casos en los que se requiere un relato sólido y coherente. En este sentido, a pesar de los esfuerzos por recabar medios de prueba que pudieran contribuir a este caso, se obtuvo un resultado negativo. En consecuencia, se observa de manera consistente una imputación genérica e imprecisa.
10	La denunciante refiere que ingresó a una página de una entidad bancaria conocida. El delincuente envío correos electrónicos de phishing a la denunciante, haciéndose pasar por el banco. En el correo, se les solicito que actualice su información personal y de seguridad a través del enlace proporcionado. Las víctimas, creyendo que el correo es legítimo, ingreso a la página falsa y proporcionan sus datos personales, incluyendo números de tarjeta de crédito, CVV, fechas de vencimiento y contraseñas. Con la información obtenida, el delincuente realizo compras en línea o transfiere dinero a cuentas controladas por él. La víctima se da cuenta del fraude cuando observa transacciones no autorizadas en su cuenta bancaria. Inmediatamente, contacta a su banco para reportar el incidente y bloquear su tarjeta. **Causa de Archivamiento:** • **No aparecen indicios reveladores de la existencia de un delito.** • **No se ha individualizado al imputado.** • **La víctima no asistió a declarar.** • **Falta de persistencia en la incriminación por parte del denunciante.**

***Tabla 3**: Modalidades de fraude informático*

	Cantidad	Porcentaje
Phishing	6	60%
Carding	1	10%
Suplantación de Identidad	0	0%
SIM Swapping	2	20%
Malware	0	0%
Thief Transfer	1	10%
Fake Apps	0	0%
Clonación de Tarjetas	0	0%
TOTAL	10	100%



En el Distrito Fiscal de Huamanga durante el año 2023, se han identificado varias modalidades de fraude informático, según se muestra en la Tabla 3. Las modalidades más comunes incluyen el phishing, que representa el 60% de los casos, y el Thief Transfer, con un 10%. El SIM Swapping también es significativo, con un 20% de los casos, mientras que el carding representa el 10%.

El phishing es la modalidad más prevalente, lo que indica una necesidad urgente de mejorar las campañas de concienciación y educación sobre seguridad digital entre la población. El Thief Transfer, aunque menos frecuente, sigue siendo una amenaza

significativa, subrayando la importancia de fortalecer las medidas de seguridad en las aplicaciones financieras. El SIM Swapping, con un 20% de los casos, destaca la necesidad de mejorar las medidas de seguridad en la gestión de tarjetas SIM y la verificación de identidad. Finalmente, el carding, aunque representa solo el 10% de los casos, resalta la importancia de implementar medidas de seguridad más robustas en las transacciones electrónicas.

***Tabla 4**: Métodos utilizados para recabar pruebas en delito de fraude informático*

C.F	Modalidad de Fraude Informático identificadas en las carpetas fiscales	Método Utilizados
1	Phishing	Captura de pantalla, registro de correos electrónicos. Análisis de tráfico de red
2	Carding	Clonación de disco duro, análisis forense
3	SIM Swapping	Registro de llamadas, análisis de SIM
4	Thief Transfer	Monitoreo de transacciones, registros bancarios.
5	Phishing	Captura de pantalla, registro de correos electrónicos. Análisis de tráfico de red
6	Phishing	Captura de pantalla, registro de correos electrónicos. Análisis de tráfico de red
7	Phishing	Captura de pantalla, registro de correos electrónicos. Análisis de tráfico de red
8	Phishing	Captura de pantalla, registro de correos electrónicos. Análisis de tráfico de red
9	Phishing	Captura de pantalla, registro de correos electrónicos. Análisis de tráfico de red
10	Phishing	Captura de pantalla, registro de correos electrónicos. Análisis de tráfico de red

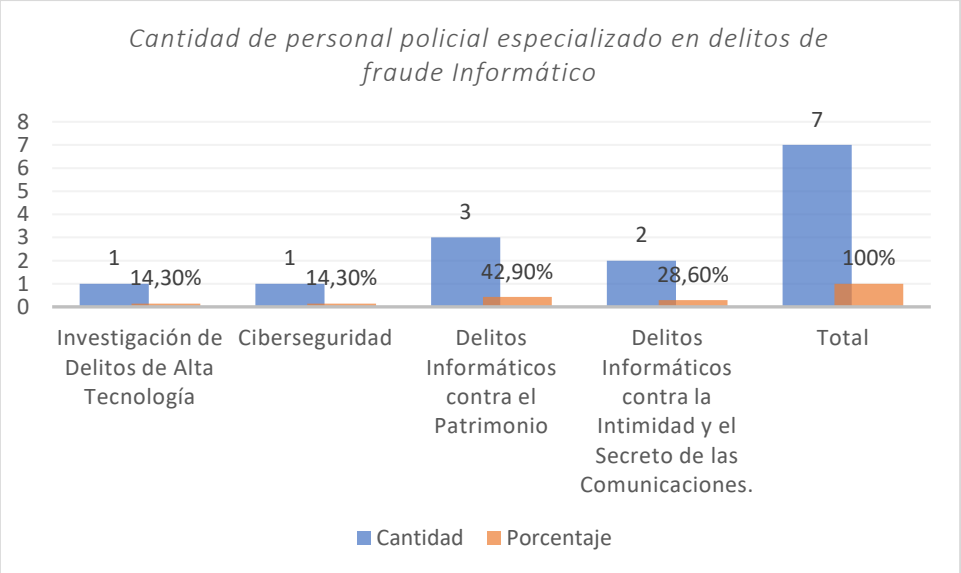
En el Distrito Fiscal de Huamanga durante el año 2023, se han identificado varias modalidades de fraude informático, cada una con métodos específicos para la preservación de pruebas digitales. Las modalidades más comunes incluyen el phishing, que representa

el 30% de los casos, y el Thief Transfer, con un 40%. El SIM Swapping también es significativo, con un 20% de los casos, mientras que el carding representa el 10%. Para el phishing, se utilizan métodos como la captura de pantalla, el registro de correos electrónicos y el análisis de tráfico de red para preservar las pruebas. En el caso del Thief Transfer, se emplean el monitoreo de transacciones y los registros bancarios. Para el SIM Swapping, se utilizan el registro de llamadas y el análisis de la tarjeta SIM, mientras que, para el carding, se recurre a la clonación de disco duro y el análisis forense.

***Tabla 5**: Cantidad de personal policial especializado en delitos de fraude Informático*

	Cantidad	Porcentaje
Investigación de Delitos de Alta Tecnología	1	14,3%
Ciberseguridad	1	14,3%
Delitos Informáticos contra el Patrimonio	3	42,9%
Delitos Informáticos contra la Intimidad y el Secreto de las Comunicaciones.	2	28,6%
Total	07	100%

Fuente: División de investigación criminal de la Policía Nacional del Perú (Huamanga)



La mayor parte del personal especializado en el Distrito Fiscal de Huamanga se enfoca en Delitos Informáticos contra el Patrimonio, con un 42.9%. Esto subraya la importancia de abordar fraudes que afectan directamente a personas y empresas. La Investigación de Delitos de Alta Tecnología y la Ciberseguridad, cada una con un 14.3%, están subrepresentadas, lo que podría limitar la capacidad de respuesta ante incidentes complejos. Los Delitos Informáticos contra la Intimidad y el Secreto de las Comunicaciones, con un 28.6%, reflejan una preocupación significativa por proteger la privacidad y la intimidad de los ciudadanos.

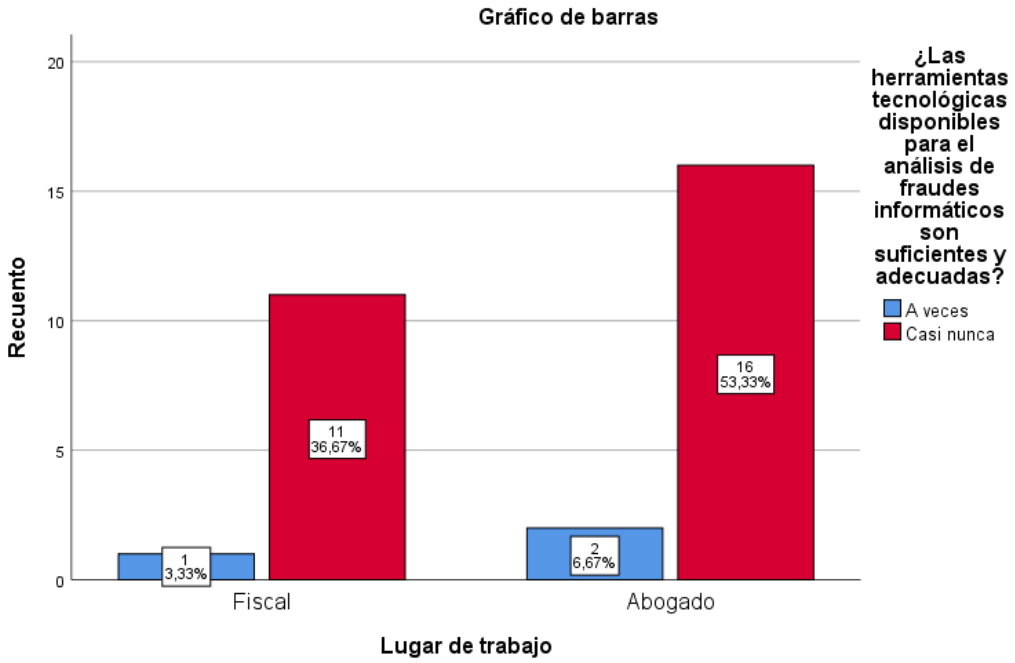
5.1.1. Resultados del cuestionario

Tabla 6 *¿Las herramientas tecnológicas disponibles para el análisis de fraudes informáticos son suficientes y adecuadas?*

Tabla cruzada Lugar de trabajo*¿Las herramientas tecnológicas disponibles para el análisis de fraudes informáticos son suficientes y adecuadas?

Recuento

		¿Las herramientas tecnológicas disponibles para el análisis de fraudes informáticos son suficientes y adecuadas?		
		A veces	Casi nunca	Total
Lugar de trabajo	Fiscal	1	11	12
	Abogado	2	16	18
Total		3	27	30



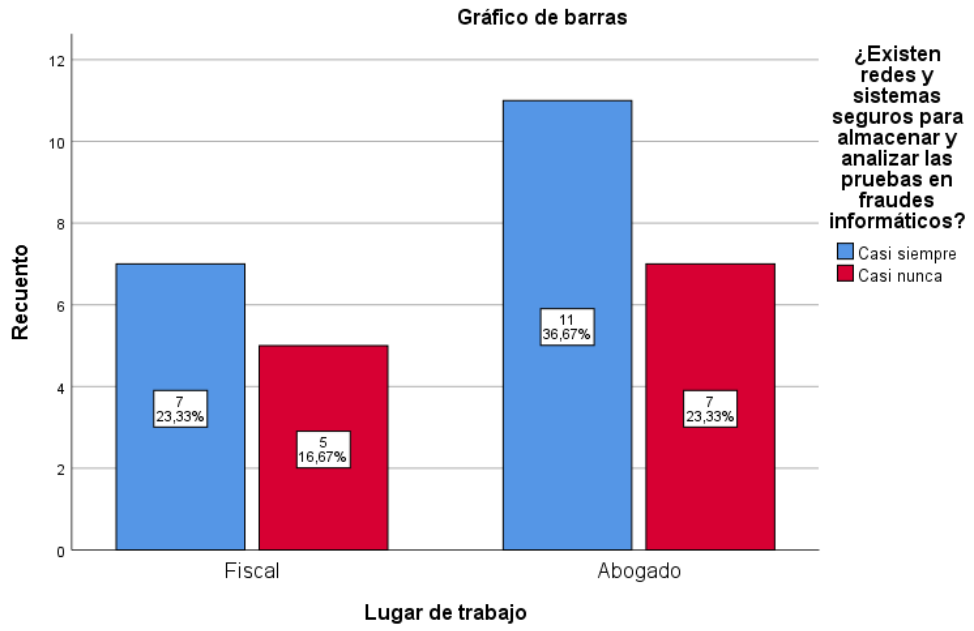
La Tabla 6 muestra que la mayoría de los fiscales y abogados consideran que las herramientas tecnológicas disponibles para el análisis de fraudes informáticos son insuficientes y no adecuadas. De los 30 encuestados, 27 creen que estas herramientas "casi nunca" son suficientes, mientras que solo 3 piensan que "a veces" lo son. Esta percepción generalizada de insuficiencia sugiere la necesidad de mejorar y actualizar las herramientas tecnológicas, así como de proporcionar una capacitación adecuada para su uso efectivo.

Tabla 7 *¿Existen redes y sistemas seguros para almacenar y analizar las pruebas en fraudes informáticos?*

Tabla cruzada Lugar de trabajo*¿Existen redes y sistemas seguros para almacenar y analizar las pruebas en fraudes informáticos?

Recuento

		¿Existen redes y sistemas seguros para almacenar y analizar las pruebas en fraudes informáticos?		
		Casi siempre	Casi nunca	Total
Lugar de trabajo	Fiscal	7	5	12
	Abogado	11	7	18
Total		18	12	30



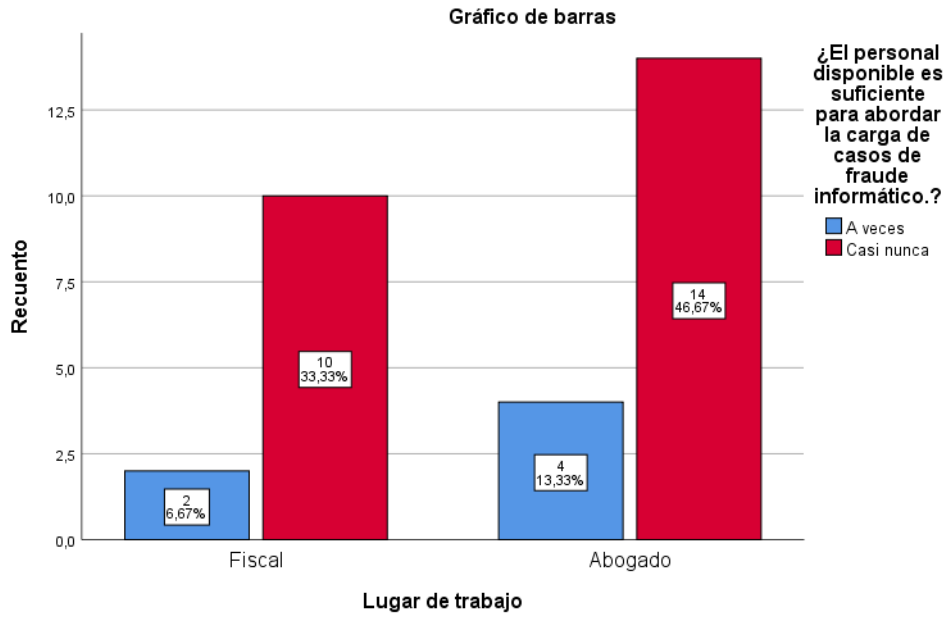
Según se muestra en la Tabla 7. La mayoría de los fiscales (58.3%) y abogados (61.1%) consideran que "casi siempre" existen estos sistemas seguros. Sin embargo, un porcentaje significativo de ambos grupos opina que "casi nunca" se cuenta con estas redes y sistemas seguros, lo que indica la necesidad de mejorar y actualizar las infraestructuras tecnológicas y de seguridad para garantizar la integridad y protección de las pruebas digitales.

Tabla 8 *¿El personal disponible es suficiente para abordar la carga de casos de fraude informático.?*

Tabla cruzada Lugar de trabajo*¿El personal disponible es suficiente para abordar la carga de casos de fraude informático.?

Recuento

		¿El personal disponible es suficiente para abordar la carga de casos de fraude informático.?		
		A veces	Casi nunca	Total
Lugar de trabajo	Fiscal	2	10	12
	Abogado	4	14	18
Total		6	24	30



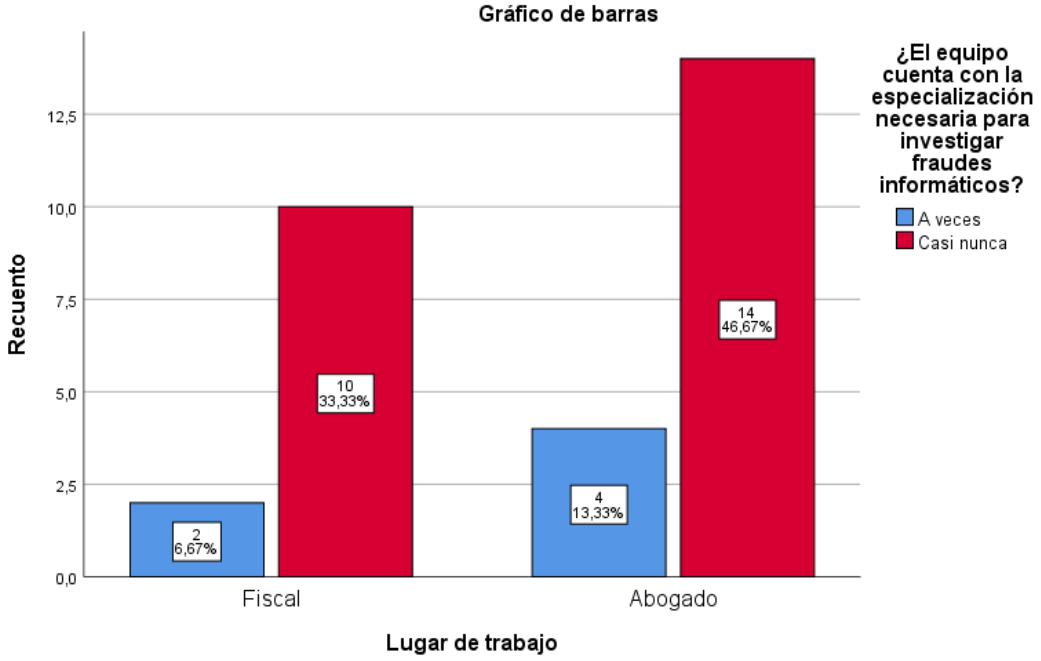
según se muestra en la Tabla 8. La mayoría de los fiscales (83.3%) y abogados (77.8%) consideran que "casi nunca" el personal es suficiente. Solo un pequeño porcentaje de fiscales (16.7%) y abogados (22.2%) creen que "a veces" el personal disponible es adecuado. Esta percepción generalizada de insuficiencia sugiere la necesidad de aumentar el personal especializado para manejar eficazmente la carga de casos de fraude informático.

Tabla 9 *¿El equipo cuenta con la especialización necesaria para investigar fraudes informáticos?*

Tabla cruzada Lugar de trabajo*¿El equipo cuenta con la especialización necesaria para investigar fraudes informáticos?

Recuento

		¿El equipo cuenta con la especialización necesaria para investigar fraudes informáticos?		
		A veces	Casi nunca	Total
Lugar de trabajo	Fiscal	2	10	12
	Abogado	4	14	18
Total		6	24	30



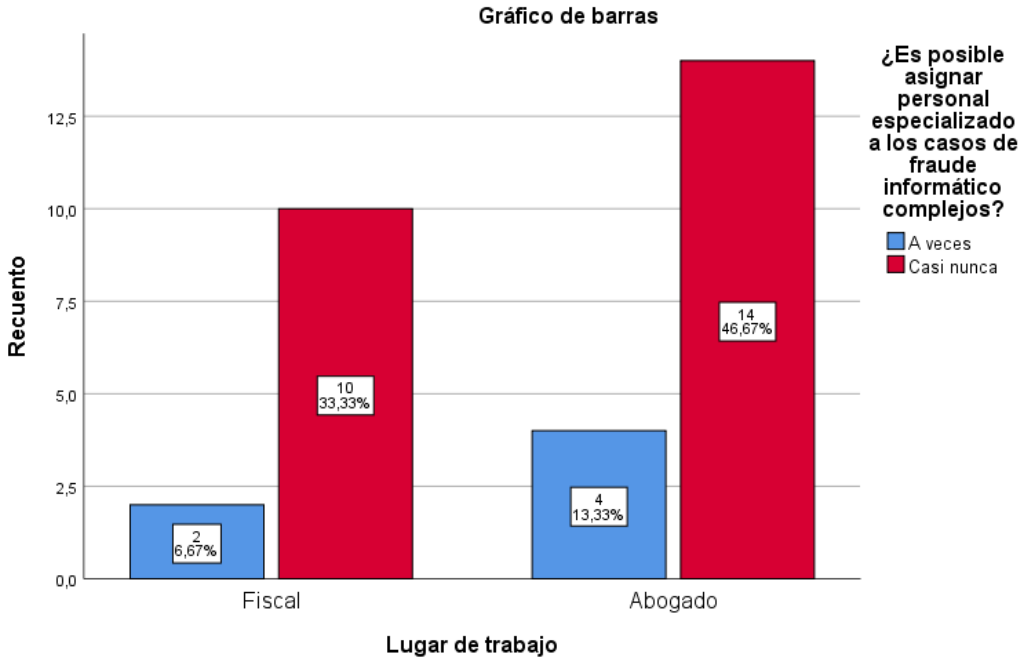
Según se muestra en la Tabla 9. La mayoría de los fiscales (83.3%) y abogados (77.8%) consideran que "casi nunca" el equipo tiene la especialización necesaria. Solo un pequeño porcentaje de fiscales (16.7%) y abogados (22.2%) creen que "a veces" el equipo cuenta con la especialización adecuada. Esta percepción generalizada de insuficiencia sugiere la necesidad de mejorar la capacitación y especialización del personal para abordar eficazmente los casos de fraude informático.

Tabla 10 *¿Es posible asignar personal especializado a los casos de fraude informático complejos?*

Tabla cruzada Lugar de trabajo*¿Es posible asignar personal especializado a los casos de fraude informático complejos?

Recuento

		¿Es posible asignar personal especializado a los casos de fraude informático complejos?		
		A veces	Casi nunca	Total
Lugar de trabajo	Fiscal	2	10	12
	Abogado	4	14	18
Total		6	24	30



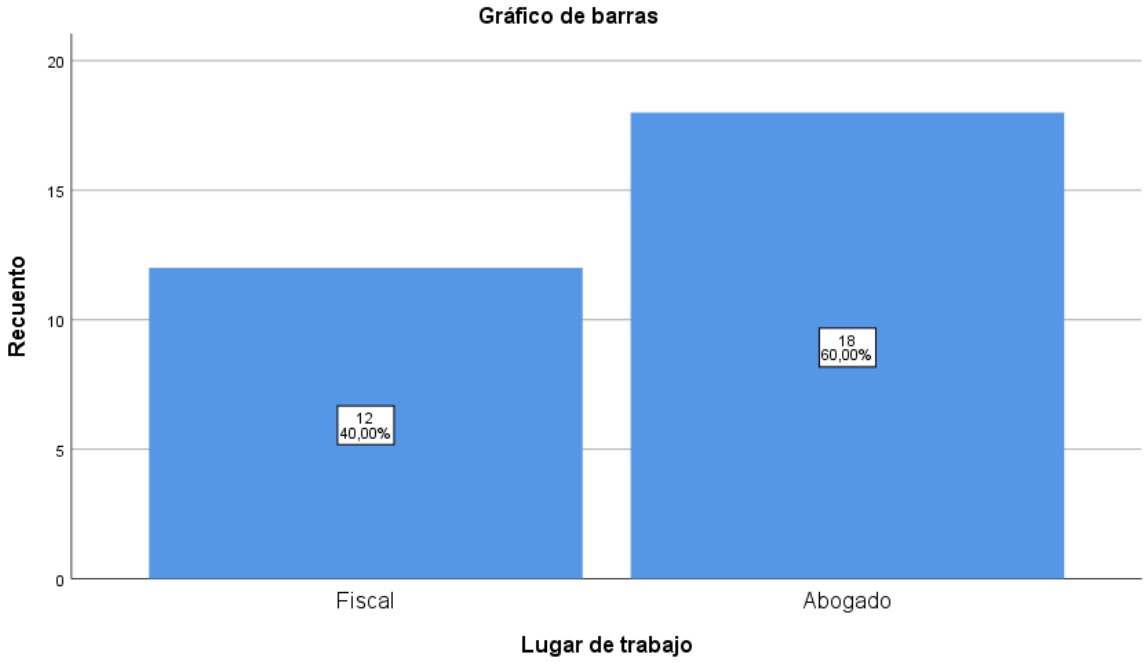
según se muestra en la Tabla 10. La mayoría de los fiscales (83.3%) y abogados (77.8%) consideran que "casi nunca" es posible asignar personal especializado a estos casos. Solo un pequeño porcentaje de fiscales (16.7%) y abogados (22.2%) creen que "a veces" es posible. Esta percepción generalizada de insuficiencia sugiere la necesidad de aumentar el personal especializado para manejar eficazmente los casos complejos de fraude informático.

Tabla 11 *¿El personal recibe capacitación regular y adecuada sobre fraudes informáticos?*

Tabla cruzada Lugar de trabajo*¿El personal recibe capacitación regular y adecuada sobre fraudes informáticos?

Recuento

		¿El personal recibe capacitación regular y adecuada sobre fraudes informáticos? Casi nunca	Total
Lugar de trabajo	Fiscal	12	12
	Abogado	18	18
Total		30	30



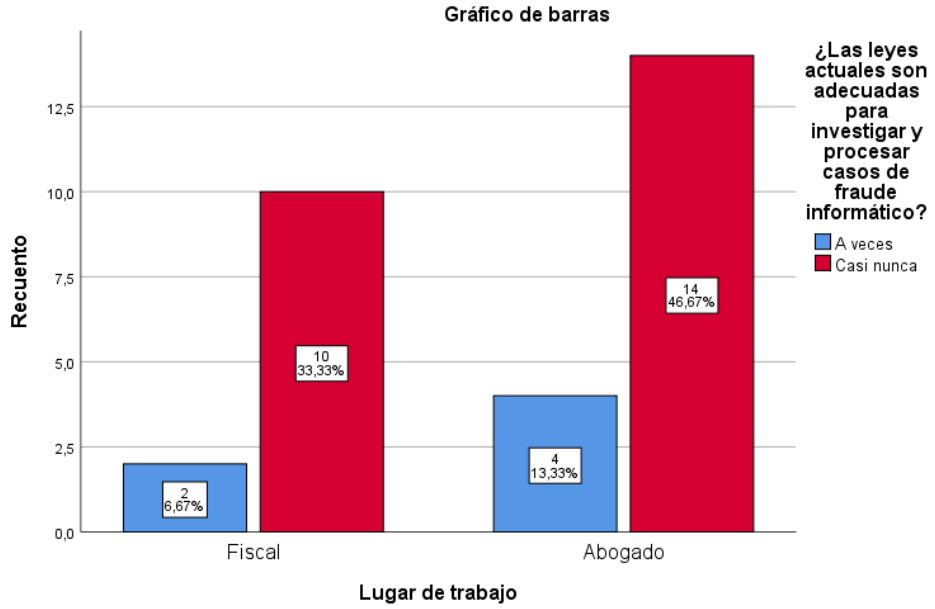
Según se muestra en la Tabla 11. Todos los fiscales (12 de 12) y abogados (18 de 18) consideran que "casi nunca" reciben capacitación regular y adecuada. Esta percepción unánime sugiere una necesidad urgente de implementar programas de capacitación continua y especializada para el personal encargado de investigar fraudes informáticos, con el fin de mejorar su eficacia y actualización en el manejo de estos casos.

Tabla 12 *¿Las leyes actuales son adecuadas para investigar y procesar casos de fraude informático?*

Tabla cruzada Lugar de trabajo*¿Las leyes actuales son adecuadas para investigar y procesar casos de fraude informático?

Recuento

		¿Las leyes actuales son adecuadas para investigar y procesar casos de fraude informático?		
		A veces	Casi nunca	Total
Lugar de trabajo	Fiscal	2	10	12
	Abogado	4	14	18
Total		6	24	30



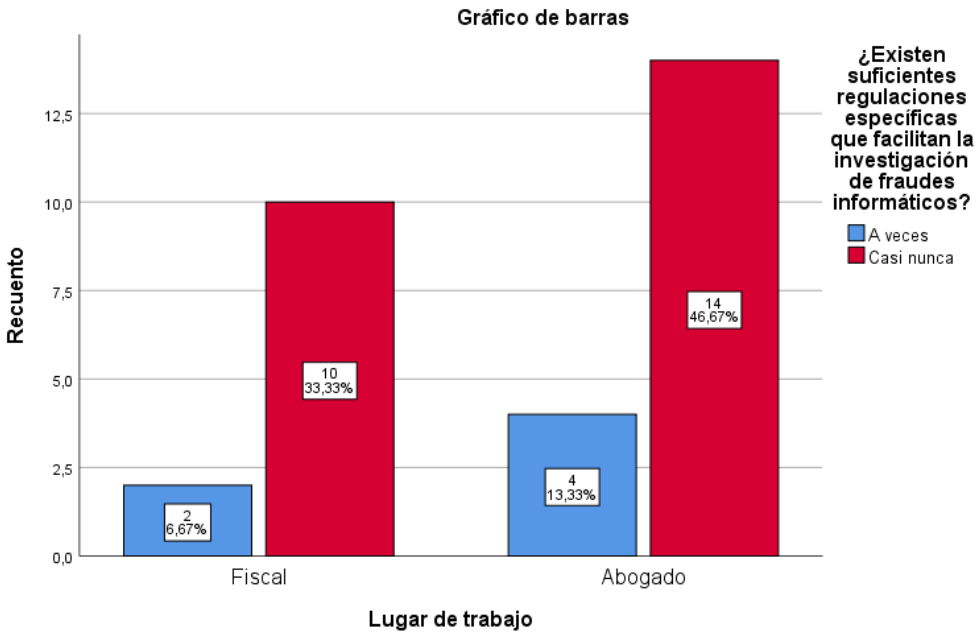
según se muestra en la Tabla 12. La mayoría de los fiscales (83.3%) y abogados (77.8%) consideran que "casi nunca" las leyes son adecuadas. Solo un pequeño porcentaje de fiscales (16.7%) y abogados (22.2%) creen que "a veces" las leyes actuales son suficientes. Esta percepción generalizada de insuficiencia sugiere la necesidad de actualizar y mejorar las leyes para abordar eficazmente los casos de fraude informático.

Tabla 13 *¿Existen suficientes regulaciones específicas que facilitan la investigación de fraudes informáticos?*

Tabla cruzada Lugar de trabajo*¿Existen suficientes regulaciones específicas que facilitan la investigación de fraudes informáticos?

Recuento

		¿Existen suficientes regulaciones específicas que facilitan la investigación de fraudes informáticos?		
		A veces	Casi nunca	Total
Lugar de trabajo	Fiscal	2	10	12
	Abogado	4	14	18
Total		6	24	30



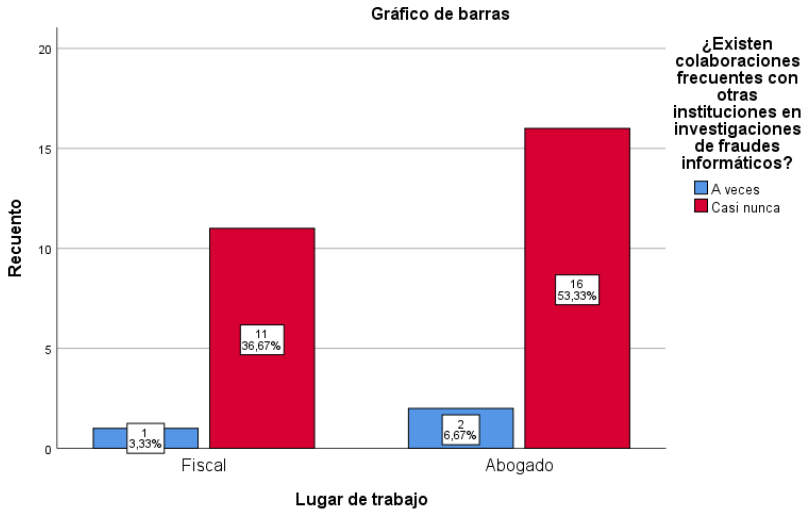
según se muestra en la Tabla 13. La mayoría de los fiscales (83.3%) y abogados (77.8%) consideran que "casi nunca" existen suficientes regulaciones específicas. Solo un pequeño porcentaje de fiscales (16.7%) y abogados (22.2%) creen que "a veces" las regulaciones son suficientes. Esta percepción generalizada de insuficiencia sugiere la necesidad de actualizar y mejorar las regulaciones para facilitar la investigación de fraudes informáticos.

Tabla 14 *¿Existen colaboraciones frecuentes con otras instituciones en investigaciones de fraudes informáticos?*

Tabla cruzada Lugar de trabajo*¿Existen colaboraciones frecuentes con otras instituciones en investigaciones de fraudes informáticos?

Recuento

		¿Existen colaboraciones frecuentes con otras instituciones en investigaciones de fraudes informáticos?		
		A veces	Casi nunca	Total
Lugar de trabajo	Fiscal	1	11	12
	Abogado	2	16	18
Total		3	27	30



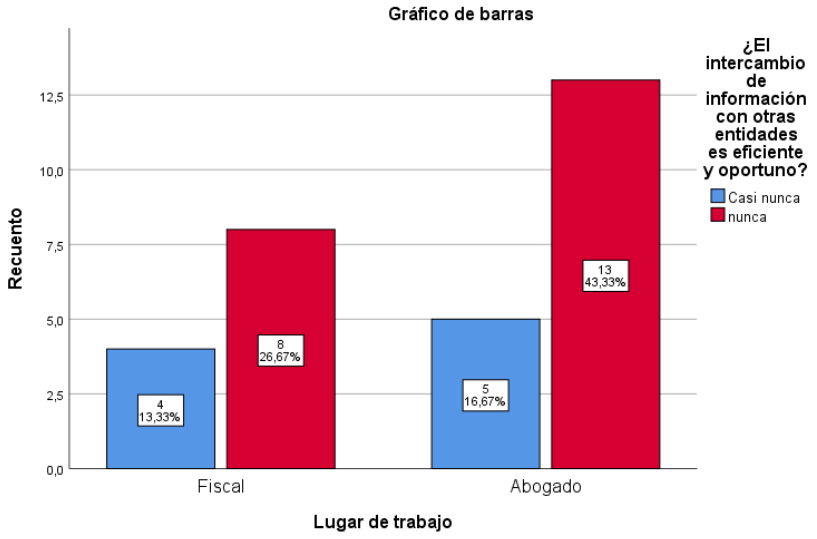
según se muestra en la Tabla 14. La mayoría de los fiscales (91.7%) y abogados (88.9%) consideran que "casi nunca" existen colaboraciones frecuentes. Solo un pequeño porcentaje de fiscales (8.3%) y abogados (11.1%) creen que "a veces" hay colaboraciones. Esta percepción generalizada de falta de colaboración sugiere la necesidad de fortalecer las alianzas interinstitucionales para mejorar la eficacia en la investigación de fraudes informático.

Tabla 15 *¿El intercambio de información con otras entidades es eficiente y oportuno?*

Tabla cruzada Lugar de trabajo*¿El intercambio de información con otras entidades es eficiente y oportuno?

Recuento

		¿El intercambio de información con otras entidades es eficiente y oportuno?		
		Casi nunca	nunca	Total
Lugar de trabajo	Fiscal	4	8	12
	Abogado	5	13	18
Total		9	21	30



En el Distrito Fiscal de Huamanga durante el año 2023, se evaluó la percepción sobre la eficiencia y oportunidad del intercambio de información con otras entidades en investigaciones de fraudes informáticos, según se muestra en la Tabla 15. La mayoría de los fiscales (66.7%) y abogados (72.2%) consideran que "nunca" el intercambio de información es eficiente y oportuno. Un porcentaje menor de fiscales (33.3%) y abogados (27.8%) creen que "casi nunca" lo es. Esta percepción generalizada de ineficiencia sugiere la necesidad de mejorar los mecanismos de intercambio de información entre entidades para facilitar la investigación de fraudes informáticos.

5.2. Discusión de resultados

A continuación, se procede a la discusión de los resultados, a partir de la integración de los siguientes elementos: objetivos, los resultados obtenidos, los antecedentes de la presente investigación y teniendo en cuenta las bases teóricas que se han tenido en cuenta como sustento para la presente investigación.

En cuanto al objetivo principal: según los resultados se puede apreciar diversos aspectos relacionados con la investigación de fraudes informáticos. Según la Tabla 6, la mayoría de los fiscales y abogados (90%) consideran que las herramientas tecnológicas disponibles son insuficientes y no adecuadas. La Tabla 7 muestra que, aunque la mayoría cree que "casi siempre" existen redes y sistemas seguros, un porcentaje significativo opina que "casi nunca" se cuenta con estos sistemas. La Tabla 8 revela que el 80% de los encuestados considera que el personal disponible es insuficiente para abordar la carga de casos de fraude informático.

En cuanto a la especialización del equipo, la Tabla 9 indica que el 80% de los fiscales y abogados creen que "casi nunca" el equipo tiene la especialización necesaria. La Tabla 10 muestra que el 80% de los encuestados opinan que "casi nunca" es posible asignar personal especializado a los casos complejos. La Tabla 11 destaca que todos los fiscales y abogados consideran que "casi nunca" reciben capacitación regular y adecuada.

La Tabla 12 señala que el 80% de los encuestados creen que las leyes actuales son inadecuadas para investigar y procesar casos de fraude informático. La Tabla 13 refleja que el 80% considera que "casi nunca" existen suficientes regulaciones específicas. La Tabla 14 muestra que el 90% de los fiscales y abogados opinan que "casi nunca" existen colaboraciones frecuentes con otras instituciones. Finalmente, la Tabla 15 revela que el 70% de los encuestados considera que "nunca" el intercambio de información con otras entidades es eficiente y oportuno. Estos hallazgos sugieren la necesidad de mejoras significativas en herramientas tecnológicas, personal especializado, capacitación, leyes,

regulaciones y colaboración interinstitucional para abordar eficazmente los fraudes informáticos.

En cuanto al primer objetivo secundario: En el Distrito Fiscal de Huamanga durante el año 2023, se identificaron varias dificultades técnicas que afectan la investigación del fraude informático. Según la Tabla 6, el 90% de los fiscales y abogados consideran que las herramientas tecnológicas disponibles son insuficientes y no adecuadas. La Tabla 7 muestra que, aunque la mayoría cree que "casi siempre" existen redes y sistemas seguros, un porcentaje significativo opina que "casi nunca" se cuenta con estos sistemas.

La Tabla 8 revela que el 80% de los encuestados considera que el personal disponible es insuficiente para abordar la carga de casos de fraude informático. En cuanto a la especialización del equipo, la Tabla 9 indica que el 80% de los fiscales y abogados creen que "casi nunca" el equipo tiene la especialización necesaria. La Tabla 10 muestra que el 80% de los encuestados opinan que "casi nunca" es posible asignar personal especializado a los casos complejos.

La Tabla 11 destaca que todos los fiscales y abogados consideran que "casi nunca" reciben capacitación regular y adecuada. La Tabla 12 señala que el 80% de los encuestados creen que las leyes actuales son inadecuadas para investigar y procesar casos de fraude informático. La Tabla 13 refleja que el 80% considera que "casi nunca" existen suficientes regulaciones específicas.

La Tabla 14 muestra que el 90% de los fiscales y abogados opinan que "casi nunca" existen colaboraciones frecuentes con otras instituciones. Finalmente, la Tabla 15 revela que el 70% de los encuestados considera que "nunca" el intercambio de información con otras entidades es eficiente y oportuno.

Estos resultados indican que las principales dificultades técnicas incluyen la insuficiencia de herramientas tecnológicas, la falta de personal especializado y capacitado, la inadecuación de las leyes y regulaciones, y la falta de colaboración y eficiencia en el

intercambio de información con otras entidades. Estas dificultades sugieren la necesidad de mejoras significativas en estos aspectos para abordar eficazmente los fraudes informáticos en el Distrito Fiscal de Huamanga.

En cuanto al segundo objetivo secundario: En el Distrito Fiscal de Huamanga durante el año 2023, se identificaron varios factores que limitan la eficacia de la investigación del delito de fraude informático. Según la Tabla 6, el 90% de los fiscales y abogados consideran que las herramientas tecnológicas disponibles son insuficientes y no adecuadas. La Tabla 7 muestra que, aunque la mayoría cree que "casi siempre" existen redes y sistemas seguros, un porcentaje significativo opina que "casi nunca" se cuenta con estos sistemas.

La Tabla 8 revela que el 80% de los encuestados considera que el personal disponible es insuficiente para abordar la carga de casos de fraude informático. En cuanto a la especialización del equipo, la Tabla 9 indica que el 80% de los fiscales y abogados creen que "casi nunca" el equipo tiene la especialización necesaria. La Tabla 10 muestra que el 80% de los encuestados opinan que "casi nunca" es posible asignar personal especializado a los casos complejos.

La Tabla 11 destaca que todos los fiscales y abogados consideran que "casi nunca" reciben capacitación regular y adecuada. La Tabla 12 señala que el 80% de los encuestados creen que las leyes actuales son inadecuadas para investigar y procesar casos de fraude informático. La Tabla 13 refleja que el 80% considera que "casi nunca" existen suficientes regulaciones específicas.

La Tabla 14 muestra que el 90% de los fiscales y abogados opinan que "casi nunca" existen colaboraciones frecuentes con otras instituciones. Finalmente, la Tabla 15 revela que el 70% de los encuestados considera que "nunca" el intercambio de información con otras entidades es eficiente y oportuno.

Estos factores incluyen la insuficiencia de herramientas tecnológicas, la falta de personal especializado y capacitado, la inadecuación de las leyes y regulaciones, y la falta de colaboración y eficiencia en el intercambio de información con otras entidades. Estas limitaciones sugieren la necesidad de mejoras significativas en estos aspectos para abordar eficazmente los fraudes informáticos en el Distrito Fiscal de Huamanga.

5.3. Contrastación de hipótesis

Hipótesis principal: se confirma la hipótesis principal ya que se han identificado varias dificultades significativas en la investigación de delitos de fraude informático. La falta de recursos tecnológicos adecuados y la escasa capacitación especializada del personal investigador en técnicas de ciberseguridad son los principales factores que contribuyen a estas dificultades. Según la Tabla 6, el 90% de los fiscales y abogados consideran que las herramientas tecnológicas disponibles son insuficientes y no adecuadas. La Tabla 7 muestra que, aunque la mayoría cree que "casi siempre" existen redes y sistemas seguros, un porcentaje significativo opina que "casi nunca" se cuenta con estos sistemas.

Además, la Tabla 8 revela que el 80% de los encuestados considera que el personal disponible es insuficiente para abordar la carga de casos de fraude informático. En cuanto a la especialización del equipo, la Tabla 9 indica que el 80% de los fiscales y abogados creen que "casi nunca" el equipo tiene la especialización necesaria. La Tabla 10 muestra que el 80% de los encuestados opinan que "casi nunca" es posible asignar personal especializado a los casos complejos.

La Tabla 11 destaca que todos los fiscales y abogados consideran que "casi nunca" reciben capacitación regular y adecuada. Esta falta de capacitación y recursos tecnológicos adecuados resulta en el archivo de las investigaciones de fraude informático, lo que a su

vez contribuye a la impunidad de estos delitos. Estos hallazgos sugieren la necesidad urgente de mejorar la capacitación del personal y actualizar las herramientas tecnológicas para abordar eficazmente los fraudes informáticos en el Distrito Fiscal de Huamanga.

Primera Hipótesis específica:

La hipótesis plantea que la ausencia de un marco normativo actualizado que contemple las nuevas modalidades de fraude digital limita la capacidad de los fiscales para actuar de manera efectiva. Según las tablas proporcionadas, esta hipótesis se confirma.

- Tabla 12: El 80% de los fiscales y abogados consideran que las leyes actuales son inadecuadas para investigar y procesar casos de fraude informático.
- Tabla 13: El 80% de los encuestados creen que "casi nunca" existen suficientes regulaciones específicas que faciliten la investigación de fraudes informáticos.

Estos resultados indican claramente que la falta de un marco normativo actualizado y la insuficiencia de regulaciones específicas son factores que limitan la eficacia de los fiscales en la investigación y procesamiento de fraudes informáticos en el Distrito Fiscal de Huamanga.

Segunda Hipótesis específica: La hipótesis plantea que la insuficiente coordinación interinstitucional y una infraestructura tecnológica deficiente limitan la eficacia en la investigación de fraudes informáticos. Según las tablas proporcionadas, esta hipótesis se confirma.

- Tabla 6: El 90% de los fiscales y abogados consideran que las herramientas tecnológicas disponibles son insuficientes y no adecuadas.

- Tabla 7: Aunque la mayoría cree que "casi siempre" existen redes y sistemas seguros, un porcentaje significativo opina que "casi nunca" se cuenta con estos sistemas.

- Tabla 14: El 90% de los fiscales y abogados opinan que "casi nunca" existen colaboraciones frecuentes con otras instituciones.

- Tabla 15: El 70% de los encuestados considera que "nunca" el intercambio de información con otras entidades es eficiente y oportuno.

Estos resultados indican claramente que tanto la insuficiente coordinación interinstitucional como la infraestructura tecnológica deficiente son factores que limitan la eficacia en la investigación de fraudes informáticos en el Distrito Fiscal de Huamanga.

.

CONCLUSIONES

a. Las herramientas tecnológicas disponibles para la investigación de fraudes informáticos son insuficientes y no adecuadas. Esta falta de recursos limita significativamente la capacidad de los investigadores para abordar estos delitos de manera efectiva.

b. Los fiscales y abogados consideran que no reciben capacitación regular y adecuada sobre fraudes informáticos. Además, creen que el equipo no tiene la especialización necesaria. Esta falta de capacitación y especialización contribuye a la ineficacia en la investigación de estos delitos.

c. Existe una percepción de que no hay colaboraciones frecuentes con otras instituciones y que el intercambio de información con otras entidades no es eficiente y oportuno. Esta falta de coordinación y colaboración interinstitucional dificulta la investigación y el procesamiento de fraudes informáticos.

d. Las leyes actuales son consideradas inadecuadas para investigar y procesar casos de fraude informático. Además, se percibe que no existen suficientes regulaciones específicas. Esta falta de un marco normativo actualizado limita la capacidad de los fiscales para actuar de manera efectiva y procesar a los responsables de estos delitos**.**

RECOMENDACIONES

a. Es crucial invertir en la actualización y adquisición de herramientas tecnológicas avanzadas para la investigación de fraudes informáticos. Esto incluye software de análisis de datos, sistemas de ciberseguridad y plataformas de colaboración interinstitucional.

b. Se debe establecer programas de capacitación regular y especializada para el personal encargado de investigar fraudes informáticos. Esto garantizará que los investigadores estén actualizados con las últimas técnicas y conocimientos en ciberseguridad y análisis de fraudes.

c. Es necesario mejorar la colaboración y el intercambio de información entre las diferentes entidades involucradas en la investigación de fraudes informáticos. Esto puede lograrse mediante la creación de protocolos claros de comunicación y la implementación de plataformas tecnológicas que faciliten el intercambio de datos de manera eficiente y segura.

Bibliografía

1. Alarcón y Barrera (2017). "Uso de internet y delitos informáticos en los estudiantes de la Universidad Pedagógica y Tecnológica de Colombia". Trabajo para la obtención del grado académico de maestro en informática educativa: https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf 26

2. 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

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. Cochachi Huamaní, Q. &. (2009). Metodología de la investigación pedagógica. Segunda edición. Editorial San Marcos.

8. 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

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

10. 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://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf

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. Mir Puig, S. (2017). Derecho Penal. Parte General. Tirant lo Blanch.

14. Pardo (2021) “Delitos Cibernéticos y Confidencialidad en las Redes Sociales, Ica-2020”: https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf

15. 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

16. Pérez Guzmán, J. M. (2019). Delitos regulados en leyes penales especiales. Gaceta Jurídica.

17. Rayón Ballesteros, M. &. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico. Escurialense.

18. Villavicencio Terreros, F. (2014). Delitos informáticos. Ius et Veritas

ANEXOS

MATRIZ DE CONSISTENCIA				
TÍTULO: La problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga 2023.				
PROBLEMA	OBJETIVOS	HIPÓTESIS	variables e indicadores	Metodología
Problema general ¿Cuáles son las principales dificultades que enfrenta el Distrito Fiscal de Huamanga en la investigación de delitos de fraude informático durante el año 2023? **Problemas específicos secundarios.** a. ¿Cuáles son las dificultades técnicas que afectan la investigación del fraude informático en el Distrito Fiscal de	**Objetivo general** Identificar cuáles son las principales dificultades que enfrenta el Distrito Fiscal de Huamanga en la investigación de delitos de fraude informático durante el año 2023. **Objetivos específicos secundario** a. Identificar cuáles son las dificultades técnicas que afectan la investigación del fraude informático en el Distrito Fiscal de Huamanga en el año 2023. b. Describir cuáles son factores que limitan la eficacia de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga en 2023.	**Hipótesis general** El Distrito Fiscal de Huamanga, enfrenta dificultades significativas en la investigación de delitos de fraude informático durante el año 2023, principalmente debido a la falta de recursos tecnológicos adecuados y la escasa capacitación especializada del personal investigador en técnicas de ciberseguridad ello termina con el archivo de las investigaciones de fraude informático y por ende impunidad del delito. **Hipótesis Específicas secundarias** a). La ausencia de un marco normativo actualizado que contemple las nuevas modalidades de fraude digital limita la capacidad de los	***Variable independiente*** **Las dificultades en la investigación de delitos de fraude informático** ***Variable dependiente*** **Investigación de delitos de fraude informático**	**Enfoque de investigación: mixto** **TIPO DE INVESTIGACIÓN:** La presente ***investigación es aplicada*** **NIVEL DE INVESTIGACIÓN:** El presente trabajo de investigación es de ***nivel descriptivo-explicativo*** **METODOS DE INVESTIGACIÓN** deductivo **DISEÑO DE INVESTIGACIÓN** No experimental **Técnica** Encuesta **procesamiento de datos** Software SPSS25 **INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN** • Ficha de recopilación de datos. • Fichas de Referencia Documental: Sub clasificación: FRD bibliográfica. FRD de sitios web. • Formato de cuestionario a abogados y Fiscales. **Población** • La población está constituida por 56 las investigaciones de fraude informático en

Huamanga en el año 2023? b. ¿Qué factores limitan la eficacia de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga en 2023?		fiscales para actuar de manera efectiva. b). La insuficiente coordinación interinstitucional entre las entidades encargadas de la persecución de estos delitos y una infraestructura tecnológica deficiente que dificulta la recolección y análisis de evidencia digital.		la fiscalía provincial penal de huamanga desde enero a diciembre de 2023. **Muestra** • La muestra se conforma por 10 carpetas fiscales de fraude informático de la fiscalía provincial penal de huamanga desde enero a diciembre de 2023 y por 30 encuestados de los cuales, 18 son abogados con conocimientos especializados en derecho penal y procesal penal y 12 son fiscales de la Fiscalía Provincial Penal Corporativa de Huamanga, del Distrito Fiscal de Ayacucho. **FUENTES DE INFORMACIÓN. –** • Bibliográficas, Sitios Web, Normas Legales, Doctrina, Jurisprudencia.

UNSCH FACULTAD DE DERECHO Y CIENCIAS POLITICAS ESCUELA PROFESIONAL DE DERECHO

CONSTANCIA DE ORIGINALIDAD N° 13 -2024-UNSCH-FDCP

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

CONSTANCIA DE ORIGINALIDAD

Autor	**Bach. LUIS EDUARDO BERROCAL ALFARO**
Para	***Título profesional***
Denominación de la tesis	**La problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga 2023.**
Evaluación de Originalidad	**16%**
Numero de trabajo	**2525001907**
Fecha	**19 de noviembre 2024**

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, 19 de noviembre de 2024

Mg. Iván Chumbe Carrera

La problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga 2023.

por Luis Eduardo BERROCAL ALFARO

Fecha de entrega: 19-nov-2024 08:47a.m. (UTC-0500)
Identificador de la entrega: 2525001907
Nombre del archivo: BORRADOR_DE_TESIS_final_3_.docx (436.49K)
Total de palabras: 21637
Total de caracteres: 124174

La problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga 2023.

INFORME DE ORIGINALIDAD

16%	18%	4%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	scielo.conicyt.cl Fuente de Internet	3%
2	anales.uchile.cl Fuente de Internet	2%
3	hdl.handle.net Fuente de Internet	2%
4	revistas.pucp.edu.pe Fuente de Internet	1%
5	repositorio.unsch.edu.pe Fuente de Internet	1%
6	repositorio.ucv.edu.pe Fuente de Internet	1%
7	repositorio.usanpedro.edu.pe Fuente de Internet	1%
8	Submitted to Universidad de San Martín de Porres Trabajo del estudiante	<1%

9	repositorio.uarm.edu.pe Fuente de Internet	<1 %
10	img.lpderecho.pe Fuente de Internet	<1 %
11	repositorio.ulasamericas.edu.pe Fuente de Internet	<1 %
12	roderic.uv.es Fuente de Internet	<1 %
13	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	<1 %
14	www.infobae.com Fuente de Internet	<1 %
15	Submitted to unsaac Trabajo del estudiante	<1 %
16	repositorio.espam.edu.ec Fuente de Internet	<1 %
17	apirepositorio.unh.edu.pe Fuente de Internet	<1 %
18	www.clubensayos.com Fuente de Internet	<1 %
19	atlasti.com Fuente de Internet	<1 %
20	www.law.cornell.edu	

	Fuente de Internet	<1 %
21	repositorio.une.edu.pe Fuente de Internet	<1 %
22	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
23	repositorio.unp.edu.pe Fuente de Internet	<1 %
24	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 16 (2000)", Brill, 2004 Publicación	<1 %
25	Submitted to Universidad de Xalapa A. C. Trabajo del estudiante	<1 %
26	www.crs.hsbc.com Fuente de Internet	<1 %
27	Submitted to Escuela de Posgrado Newman Trabajo del estudiante	<1 %
28	cdn.www.gob.pe Fuente de Internet	<1 %
29	Submitted to Universidad Tecnologica del Peru Trabajo del estudiante	<1 %
30	repositorio.utelesup.edu.pe Fuente de Internet	<1 %

31	www.slideshare.net Fuente de Internet	<1 %
32	www.youtube.com Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		

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

ACTA DE RECEPCIÓN DE EXAMEN DE SUSTENTACIÓN DE TESIS PARA LA TITULACIÓN DEL ASPIRANTE LUIS EDUARDO BERROCAL ALFARO

En la ciudad de Ayacucho, siendo las dieciséis horas del día 15 de Noviembre de 2024, se reunieron en el auditorio de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de San Cristóbal de Huamanga, los docentes: Hugo Ipurre Maldonado (Presidente) Walter Silva Medina, Luz Diana Gamboa Castro, Iván Chumbe Carrera y Marlene León Palacios (Miembros), integrantes del Jurado examinador de la tesis del aspirante Luis Eduardo Berrocal Alfaro, dando inicio a este acto académico el Presidente del jurado, quien designa a la docente Marlene León Palacio como Secretaria Docente. Seguidamente se da lectura la Resolución N° 354-2024-UNSCH-FDCP-D, de fecha 05 de noviembre de 2024; en su artículo primero de la parte resolutiva dispone la recepción del examen de sustentación de tesis y la conformación del Jurado. Continuando con el presente acto académico dispone la lectura de los artículos 23 y 25 del Reglamento de Grados y Títulos de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de San Cristóbal de Huamanga, que establece el procedimiento. Acto seguido el presidente del Jurado precisa que la sustentación de tesis tendrá una duración no menor de 30 minutos ni mayor de 1 hora; dejando a criterio y consideración de los Jurados el tiempo de duración de las preguntas y/o objeciones que consideren pertinentes. En este acto el presidente del Jurado autoriza al aspirante a iniciar la sustentación de tesis denominado: **La problemática de la investigación del delito de fraude informático en el Distrito Fiscal de Huamanga 2023**. Luego de la exposición por parte del aspirante se procede a realizar las preguntas y/o objeciones que consideren pertinentes los Jurados examinadores de mayor a menor antigüedad, los mismos que se refirieron al tema de la tesis.

Concluida las preguntas del examen de sustentación de tesis. El presidente del Jurado invita al aspirante y al público presente a abandonar el auditorio para dilucidar el resultado.

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

Concluidas las preguntas del examen de sustentación de tesis. Acto seguido el Jurado decide calificar con la nota de 13 (trece).

Realizado este acto académico el presidente de Jurado informa al titulando que ha sido aprobado.

Siendo las dieciocho horas del mismo día, se da por concluida el acto académico. Firmando en señal de conformidad.

Hugo Ipurre Maldonado
(presidente)

Luz Diana Gamboa Castro
(miembro)

Walter Silva Medina
(miembro)

Iván Chumbe Carrera
(miembro)

Marlene León Palacios
(miembro)