UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Provincial Penal Corporativa de Huamanga, 2023.

Para optar el título profesional de:
ABOGADO

PRESENTADO POR:

Bach. Carlos Francisco GOMEZ VILCATOMA

ASESOR:

Dr. Jesús Walter ESPINOZA ALTAMIRANO

AYACUCHO - PERÚ
2025

Dedicatoria

Dedico esta tesis a mi familia, especialmente a mis padres, quienes han sido mi mayor inspiración y sostén en todo momento. Y a todos aquellos que creen en la importancia de la educación como herramienta para transformar vidas y construir un futuro mejor.

Agradecimiento:

Agradezco, en primer lugar, a Dios por no soltarme en mis peores momentos, a mis padres por su apoyo incondicional y por haberme brindado las oportunidades para alcanzar mis metas. A mis profesores y asesores, por su guía, paciencia y conocimientos compartidos durante este proceso. A mi segunda familia, conformada por Obdulia, Rocío, Fabi y Abigail, quienes me acobijaron en su precioso hogar como uno más; a mis buenos amigos, por sus buenos deseos en este proceso de realización como profesional. Y finalmente, a todas aquellas personas que, de una u otra forma, creen y confían aún en mí.

ÍNDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El presente estudio tuvo como objetivo determinar cómo las dificultades en la individualización del ciberdelincuente influyen en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023. Se identificaron tres factores principales: la falta de herramientas tecnológicas avanzadas, la insuficiente capacitación del personal fiscal y los métodos de ocultamiento utilizados por los ciberdelincuentes.

La metodología incluyó un enfoque mixto, basado en encuestas a fiscales y abogados, así como en el análisis de carpetas fiscales. Los resultados evidenciaron que el 80% de los encuestados señaló la carencia de software de análisis forense, el 90% destacó la falta de capacitación especializada y el 80% consideró que las técnicas de anonimato y cifrado dificultan la identificación de los responsables. Como consecuencia, el 95.45% de los casos de fraude informático fueron archivados debido a la imposibilidad de individualizar a los ciberdelincuentes.

Se concluye que estas deficiencias generan impunidad y afectan la confianza en el sistema de justicia. Por ello, se recomienda la adquisición de herramientas tecnológicas avanzadas, la implementación de programas de capacitación especializada, el fortalecimiento de la cooperación interinstitucional y la creación de unidades especializadas en ciberdelincuencia dentro de la fiscalía. Este estudio contribuye a visibilizar las principales barreras en la investigación de delitos de fraude informático en Huamanga y propone soluciones concretas para mejorar la efectividad de las investigaciones y reducir la tasa de archivo de casos.

Palabras claves: fraude informático, ciberdelincuente, archivo fiscal.

ABSTRAC

The aim of this study was to determine how difficulties in identifying cybercriminals influence the filing of computer fraud crimes in the “Second Provincial Corporate Criminal Prosecutor's Office of Huamanga during 2023”. Three main factors were identified: the lack of advanced technological tools, insufficient training of prosecutorial staff, and the concealment methods used by cybercriminals.
The methodology included a mixed approach, based on surveys of prosecutors and lawyers, as well as on the analysis of prosecutorial files. The results showed that 80% of respondents indicated a lack of forensic analysis software, 90% highlighted the lack of specialized training, and 80% considered that anonymity and encryption techniques make it difficult to identify those responsible. As a result, 95.45% of computer fraud cases were archived due to the impossibility of identifying cybercriminals.

It is concluded that these deficiencies generate impunity and affect confidence in the justice system. Therefore, the acquisition of advanced technological tools, the implementation of specialized training programs, the strengthening of inter-institutional cooperation and the creation of specialized cybercrime units within the prosecution service are recommended. This study contributes to making visible the main barriers in the investigation of computer fraud crimes in Huamanga and proposes concrete solutions to improve the effectiveness of investigations and reduce the rate of case filing.

Keywords: computer fraud, cybercriminal, tax file.

INTRODUCCIÓN

En la era digital, el avance de la tecnología ha traído consigo nuevas formas de delincuencia, entre las cuales destaca el fraude informático. Este tipo de delito, caracterizado por su complejidad y anonimato, representan un desafío significativo para los sistemas de justicia, especialmente en regiones donde los recursos tecnológicos y humanos son limitados. En este contexto, la Segunda Fiscalía Provincial Penal Corporativa de Huamanga enfrenta una problemática particular: la dificultad para individualizar a los ciberdelincuentes, lo que influye directamente en la alta tasa de archivo de casos de fraude informático durante el año 2023.

El fraude informático no solo afecta a las víctimas en términos económicos, sino que también erosiona la confianza en las instituciones encargadas de impartir justicia. En Huamanga, la falta de herramientas tecnológicas avanzadas, la escasa capacitación en ciberseguridad y las limitaciones en la recopilación de pruebas son factores que dificultan la identificación y sanción de los responsables. Como resultado, un porcentaje significativo de denuncias son archivadas, dejando a las víctimas sin respuestas y permitiendo que los delincuentes operen con impunidad.

Esta investigación busca analizar cómo las dificultades en la individualización del ciberdelincuente influyen en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023. Para ello, se explorarán los obstáculos técnicos y operativos que enfrenta la fiscalía, así como las consecuencias de estas limitaciones en la eficacia de las investigaciones. Además, se propondrán posibles soluciones para fortalecer las capacidades de la institución y mejorar la respuesta ante este tipo de delitos.

El estudio se justifica por la necesidad de comprender y abordar un problema que afecta no solo a las víctimas directas, sino también a la sociedad en su conjunto. Al identificar las causas y efectos de la alta tasa de archivo de casos, se espera contribuir al desarrollo de estrategias que permitan una mayor eficacia en la lucha contra el fraude informático, fortaleciendo así el sistema de justicia y la confianza ciudadana.

En este sentido, la presente tesis se estructura en torno a tres ejes principales: el análisis de las dificultades en la individualización del ciberdelincuente, la evaluación de su impacto en el archivo de casos y la propuesta de medidas para mejorar la capacidad de investigación de la fiscalía. A través de este enfoque, se busca no solo diagnosticar el problema, sino también ofrecer soluciones prácticas que puedan ser implementadas en el corto y mediano plazo.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

A nivel global, el fraude informático se ha convertido en una de las principales amenazas para la seguridad y la economía. Según informes de la Unión Internacional de Telecomunicaciones (UIT, 2022), los ciberdelitos han aumentado exponencialmente en la última década, con pérdidas económicas que superan los $6 billones de dólares anuales. La dificultad para individualizar a los ciberdelincuentes es un problema común en la mayoría de los países, ya que estos operan de manera anónima, utilizando tecnologías avanzadas como el cifrado, las redes privadas virtuales (VPN) y las criptomonedas para evadir la detección.

Organismos internacionales como Interpol y Europol han destacado que la falta de cooperación entre países, la insuficiente capacitación de los cuerpos policiales y la ausencia de legislaciones actualizadas son factores que agravan el problema (Interpol, 2021; Europol, 2022). Además, la globalización de los delitos informáticos hace que los ciberdelincuentes actúen desde un país mientras afectan a víctimas en otro, lo que complica aún más su identificación y captura.

Asimismo, en el Perú, el fraude informático es uno de los delitos que más ha crecido en los últimos años. Según datos del Ministerio del Interior (2022), en ese año se registraron más de 15,000 denuncias por delitos informáticos, siendo el fraude una de las modalidades más recurrentes. Sin embargo, la tasa de resolución de estos casos es extremadamente baja, con un 85% de los casos archivados debido a la falta de pruebas y la dificultad para identificar a los responsables.

El Banco Central de Reserva del Perú (BCRP, 2022) ha alertado sobre el aumento de transacciones fraudulentas a través de plataformas digitales, lo que ha generado pérdidas millonarias para los usuarios y las instituciones financieras. A nivel nacional, las fiscalías y las fuerzas policiales enfrentan limitaciones en recursos tecnológicos, personal

especializado y coordinación interinstitucional, lo que dificulta la investigación y persecución de estos delitos.

Consecuentemente, en Huamanga - Ayacucho, el fraude informático se ha convertido en un problema creciente que afecta a la población local. La Segunda Fiscalía Provincial Penal Corporativa de Huamanga ha reportado un incremento significativo en las denuncias por fraude informático durante el año 2023. Sin embargo, la mayoría de estos casos son archivados debido a las dificultades para individualizar a los ciberdelincuentes.

Las limitaciones en nuestra ciudad son aún más pronunciadas que a nivel nacional, es así que, la fiscalía penal, quienes son los encargados de investigar este tipo de delitos, carece de herramientas tecnológicas avanzadas, como software de análisis forense y sistemas de rastreo de transacciones digitales. Además, el propio personal de la referida fiscalía no cuenta con la capacitación necesaria para enfrentar los desafíos que plantean los delitos informáticos, más aún el delito de fraude informático, la cual abarca el presente trabajo de investigación (Segunda Fiscalía Provincial Penal Corporativa de Huamanga, 2023). Esto se traduce en una alta tasa de archivo de casos, lo que genera desconfianza en la población y permite que los ciberdelincuentes operen con impunidad.

Un ejemplo concreto es el caso de una denunciante que, en diciembre de 2022, descubrió que se habían realizado transacciones fraudulentas en su cuenta bancaria por un monto aproximado de S/. 1,100 soles. A pesar de presentar la denuncia, el caso fue archivado debido a la imposibilidad de identificar a los responsables (Segunda Fiscalía Provincial Penal Corporativa de Huamanga, 2023). Este tipo de situaciones se repite con frecuencia en Huamanga, reflejando una problemática que requiere atención urgente.

1.2. Delimitación de la investigación

Delimitación espacial: El presente trabajo de investigación es abordado geográficamente en la Segunda Fiscalía Corporativa Penal de Huamanga.

Delimitación temporal: Esta comprenderá las Disposiciones de Archivo del delito de fraude informático (recabadas de las carpetas fiscales), investigación realizada en la

Segunda Fiscalía Provincial Penal Corporativa de Huamanga, durante el periodo de enero a diciembre del año 2023.

Delimitación conceptual o teórica: Los temas ejes que se desarrollaran en la presente investigación son la ciberdelincuencia, el delito de fraude informático, modalidades de fraude informático, dificultades en la individualización del ciberdelincuente y su influencia en los archivos a nivel preliminar de los delitos de fraude informático, en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga.

1.3. Formulación del problema

1.3.1. Problema principal

¿Cómo influyen las dificultades en la individualización del ciberdelincuente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023?

1.3.2. Problemas secundarios

1.3.2.1. Primer problema específico

¿De qué manera la falta de herramientas tecnológicas especializadas afecta la identificación de los ciberdelincuentes en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023?

1.3.2.2. Segundo problema específico

¿De qué manera la falta de capacitación de los fiscales influye en la individualización del ciberdelincuente y en la decisión de archivar los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023?

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Determinar cómo influyen las dificultades en la individualización del ciberdelincuente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023.

1.4.2. Objetivo Específico

1.4.2.1. Primer objetivo específico

Determinar de qué manera la falta de herramientas tecnológicas especializadas afecta la identificación de los ciberdelincuentes en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023.

1.4.2.2. Segundo objetivo específico

Determinar de qué manera la falta de capacitación de los fiscales influye en la individualización del ciberdelincuente y en la decisión de archivar los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga.

1.4.3. Justificación

La investigación sobre las dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023 se justifica por la creciente incidencia de este tipo de delitos y su impacto en la sociedad. En un mundo cada vez más digitalizado, el fraude informático representa una amenaza significativa para la seguridad económica y la confianza de los ciudadanos en las instituciones. Sin embargo, la falta de recursos tecnológicos, la escasa capacitación del personal y las limitaciones en la recopilación de pruebas han generado una alta tasa de archivo de casos, lo que deja a las víctimas sin respuestas y permite que los delincuentes operen con impunidad.

Este estudio busca identificar las causas específicas que dificultan la individualización de los ciberdelincuentes y analizar cómo estas limitaciones influyen en el archivo de los casos. Además, se propone ofrecer recomendaciones prácticas para fortalecer las capacidades de la fiscalía y mejorar la eficacia en la investigación de estos delitos. Aunado a ello, la investigación es relevante no solo para Huamanga, sino también para otras regiones del país que enfrentan problemas similares.

1.4.4. Importancia

El fraude informático afecta directamente a la población, generando pérdidas económicas y erosionando la confianza en el sistema de justicia. Al analizar las dificultades en la individualización de los ciberdelincuentes, este estudio busca contribuir a la protección de los derechos de las víctimas y a la restauración de la confianza ciudadana en las instituciones.

La investigación proporcionará información valiosa para la Segunda Fiscalía Provincial Penal Corporativa de Huamanga, permitiéndole identificar sus debilidades y fortalezas en la investigación del delito de fraude informático. Esto sentará las bases para la implementación de mejoras en recursos tecnológicos, capacitación del personal y coordinación interinstitucional.

Este estudio aportará al conocimiento académico sobre los desafíos que enfrentan las fiscalías en la lucha contra el fraude informático, especialmente en contextos con recursos limitados. Los hallazgos podrán ser utilizados como referencia para futuras investigaciones en el campo de la ciberseguridad y la justicia penal.

1.4.5. Viabilidad de la investigación

La realización de este trabajo de investigación representa un desafío personal para el autor, motivado por el interés que despertó en él, ya que se evidenció el fenómeno del fraude informático desde sus años de formación académica, interés que se intensificó al enfrentarse directamente con esta problemática en el ejercicio pre profesional. Esta experiencia permitió identificar serias deficiencias y dificultades en los procesos de

investigación relacionados con dicho delito, lo que conllevó la necesidad de abordar el tema de manera más profunda. Por estas razones, se planteó como objetivo principal recopilar, analizar y sistematizar información relevante sobre el fraude informático, a fin de contribuir al entendimiento de sus implicancias legales y operativas, y así aportar al desarrollo de mejores prácticas en su investigación y prevención.

1.4.6. Limitaciones del estudio

Al comenzar el presente trabajo, las actividades previas a la investigación han enfrentado desafíos metodológicos, las cuales fueron vencidos mediante estudios y capacitaciones por parte del investigador. Así también, se identificaron limitaciones al momento de la recolección de datos, ya que, el acceso a la información del Ministerio Público resulta ser dificultoso, más aún al acudir a realizar la revisión de las carpetas fiscales necesarias para su análisis.

Asimismo, se presentó dificultades al momento de la recolección de las encuestas directas realizadas al personal de la Segunda Fiscalía Provincial Penal Corporativa de Huamanga, considerando que muchos de ellos se encontraban con carga laboral y trabajos de campo. Sin embargo, todo ello fue superado durante el desarrollo de la investigación con una mejor programación al momento de recabar la información necesaria para la presente investigación.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de estudio

Como consecuencia de realizar una revisión crítica de estudios que precedentemente investigaron el tema investigado (Vara, 2015, p.95); por lo expuesto, en relación a las variables que se explicaron en páginas anteriores de la presente tesis, se consideró como trabajos previos, tanto internacionales, como nacionales, a los siguientes, de los que se extraen lo más importante:

2.1.1. Antecedentes internacionales

Peña (2023), estableció en su trabajo de investigación “Los delitos informáticos o cibernéticos y los perjuicios hacia el sistema financiero en Colombia”. En donde el estudio tuvo un enfoque cualitativo y concluyó que en Colombia los delitos informáticos han aumentado, afectando los derechos de los usuarios. Aunque el internet ha facilitado las transacciones financieras, también ha permitido fraudes y estafas. Los delincuentes, por ejemplo, se hacen pasar por agentes bancarios para engañar a las personas y robar su información. Este crecimiento de los ciberdelitos representa un problema de seguridad para el país, siendo el fraude el más común. Ante esto, el Estado debe tomar medidas para proteger a los usuarios y fortalecer las políticas criminales que sancionen estos delitos.

Carriedo (2022), en su tesis de maestría titulada “Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México” presentada en el MDTIC de la ciudad de México, realiza un análisis crítico del marco jurídico mexicano respecto a los ciberdelitos que podrían limitar la circulación de contenido en internet. El estudio compara la legislación vigente con los estándares internacionales en materia de derechos humanos, especialmente aquellos vinculados con la libertad de expresión. Para ello, se revisan los treinta y dos códigos penales estatales, el Código Penal Federal y diversas propuestas legislativas que, aunque no fueron aprobadas, generaron controversia por su potencial efecto censor. El objetivo central de la investigación consiste en determinar si las normas sobre delitos informáticos en México garantizan o vulneran los derechos

fundamentales. Asimismo, se evalúa si las restricciones al contenido digital se ajustan a los parámetros internacionales o si representan una amenaza para la libertad de expresión. Los resultados evidencian que, aunque algunas disposiciones se alinean con los estándares de derechos humanos, persisten vacíos normativos y propuestas legislativas que podrían propiciar prácticas de censura. En suma, el trabajo pone de relieve el delicado equilibrio entre la lucha contra los delitos informáticos y la protección de la libertad de información en el entorno digital.

Paguay & Granizo (2020), en su trabajo de investigación titulada “Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet”, desarrollada en la Universidad Nacional de Chimborazo (Riobamba, Ecuador), abordan el creciente impacto de los delitos informáticos en el contexto del comercio electrónico, en un entorno marcado por el avance tecnológico y el desarrollo de la informática en Ecuador. Su estudio identifica delitos como la estafa electrónica, la apropiación ilícita y los daños informáticos, los cuales se cometen mediante el uso de tecnologías digitales y son reconocidos tanto en el marco legal ecuatoriano como por organismos internacionales como la ONU y la Unión Europea. El objetivo principal de la investigación fue analizar las perspectivas regulatorias de estos delitos en el ámbito de las compras en línea, dada la aparición de nuevas formas de criminalidad en entornos digitales. Mediante un enfoque analítico-sintético, se examinaron disposiciones del Código Orgánico Integral Penal y de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Asimismo, se incorporó un caso práctico que evidencia la afectación de derechos en operaciones de comercio electrónico, lo cual resalta la necesidad de fortalecer y ampliar el marco regulatorio en materia de delitos informáticos en el país vecino de Ecuador.

2.1.2. Antecedentes nacionales

Carbajal (2022), en su tesis de maestría titulada “Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen”, analiza la problemática delictiva asociada al entorno digital, en el contexto de una revolución tecnológica que, si bien ha mejorado la comunicación y facilitado el desarrollo profesional y laboral, también ha generado nuevas amenazas para el orden social y jurídico. El estudio se centra en la necesidad de fortalecer la capacidad del Estado frente a la ciberdelincuencia,

particularmente a través de la creación de fiscalías especializadas en delitos informáticos. Estas unidades permitirían enfrentar con mayor eficacia los desafíos que presenta la investigación del fraude informático, tales como el anonimato del autor del delito, la escasa colaboración de las víctimas, la carencia de peritos especializados y la limitada formación de los fiscales en materia de criminalidad informática. La investigación concluye que los delitos informáticos representan una amenaza creciente para la sociedad, especialmente con la expansión del uso de tecnologías digitales, fenómeno que se intensificó durante la emergencia sanitaria provocada por la pandemia del COVID-19, cuando aumentaron significativamente las transacciones bancarias en línea. Frente a este panorama, se subraya la urgencia de implementar políticas públicas eficaces orientadas a combatir la ciberdelincuencia y proteger a los sectores más vulnerables frente a estos delitos.

Huamaní (2024), en su trabajo de investigación para obtener su grado de maestra, titulada “La regulación de los delitos informáticos en el derecho penal: desafíos y perspectivas futuras, 2023”; desarrolla un análisis centrado en los principales retos que enfrenta el derecho penal frente al avance de la ciberdelincuencia, así como en las proyecciones necesarias para su regulación eficaz. Su estudio revela que la normativa actual resulta, en muchos casos, insuficiente para responder a la constante evolución tecnológica y al creciente nivel de sofisticación de los delitos informáticos. En ese sentido, se evidencia la urgencia de actualizar de forma permanente el marco legal a fin de incorporar nuevas conductas delictivas emergentes. Asimismo, la investigación destaca la importancia de la cooperación internacional, considerando que los delitos informáticos no se limitan a fronteras nacionales y requieren una respuesta coordinada entre países para su prevención y sanción efectiva.

Sotomayor (2023), en su tesis titulada “La Calificación Fiscal en los Delitos Informáticos en el Distrito Fiscal de Lima Centro, 2019 – 2020”, presentada en la Universidad César Vallejo, Lima – Perú; analiza el tratamiento que se da a los delitos informáticos desde la etapa de calificación fiscal. Utilizando un enfoque cualitativo y aplicando la teoría fundamentada como diseño metodológico, la investigación se apoyó en entrevistas para profundizar en el análisis del fenómeno. Los hallazgos muestran que existen serias imprecisiones en la calificación fiscal de estos delitos, lo que ha generado que muchos casos inicialmente denunciados como delitos informáticos sean finalmente

formalizados bajo otras figuras penales, como el hurto agravado. Esta situación revela deficiencias en el proceso de calificación jurídica y plantea la urgencia de crear fiscalías especializadas en ciberdelincuencia, que cuenten con el conocimiento técnico y normativo necesario para abordar adecuadamente estos casos. Asimismo, se subraya la importancia de fortalecer el marco legal vigente, en particular la Ley Nº 30096, con el fin de garantizar una respuesta penal más eficiente frente a las amenazas que plantea el delito informático.

Matos (2022), en su tesis de grado denominado “Especialización de la investigación preparatoria en los delitos de fraudes informático”; llevó a cabo un análisis sobre la aplicación de la etapa de investigación preparatoria en los casos de fraude informático en el ámbito del Ministerio Público de Lima Norte. Empleando un enfoque cualitativo y bajo el diseño metodológico de la teoría fundamentada, el estudio recurrió a entrevistas y revisión documental para identificar las principales deficiencias en dicho proceso. Entre los resultados, se evidenció la necesidad de reformar la actual Ley de Delitos Informáticos, así como de mejorar la infraestructura y especialización del personal encargado de su investigación. La investigación también resalta la urgencia de fortalecer tanto al Ministerio Público como a la Policía Nacional del Perú, específicamente a la División de Investigación de Delitos de Alta Tecnología (Divindat), con el fin de lograr una respuesta más eficaz ante este tipo de criminalidad.

2.2. Bases Teóricas

2.2.1. Delitos informáticos

Para el autor Barrio (2017), los ciberdelitos o delitos informáticos comprenden conductas ilícitas que se desarrollan en el entorno digital, el cual es producto del uso de tecnologías informáticas. Esta categoría abarca tanto los delitos que afectan directamente a sistemas, datos o equipos informáticos, poniendo en riesgo su integridad, confidencialidad y disponibilidad; como aquellos delitos tradicionales que, mediante herramientas tecnológicas, encuentran nuevas formas de ejecución, tales como fraudes, amenazas o actos de coacción. En este sentido, los ciberdelitos representan una fusión entre elementos tecnológicos y modalidades delictivas convencionales, adaptadas al contexto digital.

Los delitos informáticos son conductas ilícitas que involucran el uso de tecnologías de la información y la comunicación (TIC) para cometer fraudes, acceder de manera no autorizada a sistemas, robar información, dañar redes o dispositivos, entre otras acciones ilegales. De esta manera se puede evidenciar que la definición de los delitos informáticos ha experimentado una evolución debido al rápido desarrollo de la tecnología y su aplicación en las diferentes actividades delictivas que se le pueda vincular.

2.2.1.1. Características de los delitos informáticos

Los delitos informáticos tienen características únicas que los diferencian de los delitos tradicionales y hacen que su persecución y prevención sean más complejas. A continuación, se detallan sus principales características con mayor profundidad:

a) Uso de tecnologías digitales

- Los delitos informáticos se cometen a través de computadoras, redes, software, dispositivos móviles y cualquier tecnología relacionada con la información y la comunicación.
- No requieren la presencia física del delincuente en la escena del crimen; basta con una conexión a Internet.
- Algunos delitos pueden ejecutarse mediante códigos maliciosos sin intervención humana directa, como en el caso de los bots y virus informáticos.

b) Intangibilidad de la evidencia

- A diferencia de los delitos tradicionales, donde las pruebas suelen ser físicas, en los delitos informáticos la evidencia es digital.
- La evidencia digital puede ser fácilmente modificada, eliminada o encriptada, lo que complica su recolección y análisis.

- Se requiere de técnicas especializadas de informática forense para recuperar y autenticar pruebas en dispositivos o redes.

c) Dificultad en la identificación del autor

- Los ciberdelincuentes utilizan herramientas para ocultar su identidad, como VPN (Redes Privadas Virtuales), proxys anónimos, redes TOR, entre otros.
- La suplantación de identidad y el uso de cuentas falsas dificultan el rastreo del verdadero responsable.
- En algunos casos, los ataques provienen de dispositivos "zombies" controlados remotamente por los atacantes, lo que desvía la responsabilidad legal.

d) Alcance global y transaccionalidad

- Un delito informático puede afectar a víctimas en distintos países sin que el atacante se desplace físicamente.
- Esto genera problemas de jurisdicción y cooperación internacional entre organismos de seguridad y justicia.
- Por ejemplo, un fraude bancario puede ser cometido desde Europa contra una víctima en América Latina, usando servidores en Asia.

e) Automatización y escalabilidad

- Los delitos informáticos pueden realizarse a gran escala, afectando a miles o millones de víctimas en cuestión de minutos.
- Se pueden usar programas automatizados (bots, malware, ransomware) para ejecutar ataques sin intervención directa del delincuente.
- Ejemplo: Un ataque de phishing puede ser enviado por correo masivo a miles de personas con solo presionar un botón.

f) Evolución constante y sofisticación

- La tecnología cambia constantemente, lo que permite a los delincuentes desarrollar nuevas estrategias para evadir la detección.
- Cada año aparecen nuevas formas de malware, fraudes cibernéticos, técnicas de hacking y exploits de vulnerabilidades.
- Ejemplo: Con el auge de la inteligencia artificial, han surgido delitos como la falsificación de identidad con deepfake o la manipulación de audios y videos.

g) Dificultad en la regulación y persecución legal

- En muchos países, las leyes sobre delitos informáticos están desactualizadas o tienen vacíos legales.
- La persecución de los delincuentes puede complicarse debido a la necesidad de colaboración internacional.
- Algunos delitos son difíciles de tipificar porque evolucionan más rápido que la legislación (ejemplo: delitos con criptomonedas o en el metaverso).

h) Daño económico y social significativo

- Los delitos informáticos pueden generar pérdidas económicas multimillonarias en empresas, bancos e individuos.
- Afectan la confianza en los sistemas digitales y pueden desestabilizar sectores clave como la banca, la salud o la seguridad pública.
- También pueden causar daños psicológicos en las víctimas, como en casos de ciberacoso, sextorsión o difusión de material íntimo sin consentimiento.
- Estas características hacen que los delitos informáticos sean una de las principales amenazas en el mundo digital actual. Por ello, es clave reforzar

la ciberseguridad, mejorar las leyes y educar a la población sobre cómo prevenir estos delitos.

2.2.2. Ley de Fraude Informático (30096)

La Ley N° 30096, denominada Ley de Delitos Informáticos, fue aprobada en Perú el 22 de octubre de 2013 con la finalidad de prevenir y castigar actos ilegales que comprometan la seguridad de los sistemas y la información digital. Además, busca proteger otros bienes jurídicos que puedan ser vulnerados a través del uso de tecnologías de la información y comunicación.

2.2.2.1. Delitos contra datos y sistemas informáticos

a. **Acceso ilícito:** "El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa." (Art.2, Ley 30096).

b. **Atentado a la integridad de datos informáticos**: "El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa". (Art. 3, Ley 30096).

c. **Atentado contra la integridad de sistemas informáticos**: "El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa". (Art. 4, Ley 30096).

2.2.2.2. Delitos informáticos contra la indemnidad y libertad sexuales

a. **Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos** "El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de seis ni mayor de nueve años. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años. En todos los casos se impone, además, la pena de inhabilitación conforme a los numerales 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11 del artículo 36 del Código Penal." (Art. 5, Ley 30096).

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

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

a. **Interceptación de datos informáticos** "El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena

privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública". (Art. 7, Ley 30096).

2.2.2.4. Delitos informáticos contra el patrimonio

a. **Fraude informático**: "El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa". (Art. 8, Ley 30096).

b. **Préstamos informáticos extorsivos:** "El que, a través de plataformas digitales, internet u otro medio análogo induce u obliga mediante amenaza, intimidación, engaño o ardid a aceptar dinero o bienes, simulando un contrato de mutuo o cualquier otro con el fin de obtener una ventaja indebida, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años". (Art. 8-A, Ley 30096).

2.2.2.5. Delitos informáticos contra la fe pública:

a. **Dentro de este delito se encuentra la suplantación de identidad,** "El que, mediante las tecnologías digitales suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral o de cualquier otra índole, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de

edad y resulte algún perjuicio, material, moral o de cualquier otra índole.” (Art. 9, Ley 30096).

2.2.3. Fraude informático

El fraude informático es un delito en el que una persona manipula sistemas, datos o programas informáticos con el objetivo de obtener un beneficio económico indebido o causar un perjuicio a otra persona o entidad.

Desde el punto de vista legal, este delito ocurre cuando alguien engaña o altera información digital para apropiarse de dinero, bienes o servicios de manera ilícita. Puede incluir acciones como el uso de programas para modificar registros bancarios, el robo de información financiera o el acceso no autorizado a sistemas para cometer estafas.

Mayer y Oliver (2020) señalan que, en muchas ocasiones, el fraude informático es erróneamente asociado con delitos en grado de tentativa o frustración. Los autores destacan que, dentro de las distintas formas de fraude informático, existen dos modalidades relevantes: **phishing** y **pharming**, caracterizadas por su ocurrencia dentro del ámbito bancario.

2.2.3.1. Modalidades del fraude informático

El fraude informático es una de las principales amenazas en el ámbito digital, donde los delincuentes emplean diversas técnicas para obtener información sensible o realizar transacciones ilícitas sin el consentimiento de las víctimas. Estas modalidades se han diversificado con el avance de la tecnología y la expansión del uso de plataformas digitales, afectando tanto a individuos como a empresas e instituciones financieras. A continuación, se presentan algunas de las formas más comunes de fraude informático:

a. Phishing

El phishing es una técnica fraudulenta que consiste en el envío de correos electrónicos, mensajes de texto o notificaciones falsas que aparentan provenir de entidades legítimas, como bancos, plataformas de pago o servicios en línea. El objetivo es engañar a

los usuarios para que revelen información confidencial, como contraseñas, datos bancarios o credenciales de acceso.

b. Pharming

El pharming es una modalidad más sofisticada que implica la manipulación del tráfico web. En este caso, los ciberdelincuentes alteran el sistema de nombres de dominio (DNS) o infectan el dispositivo de la víctima con malware para redirigirla automáticamente a un sitio web falso, sin que esta lo perciba. A diferencia del phishing, en el que el usuario debe hacer clic en un enlace malicioso, en el pharming la víctima es llevada directamente al sitio fraudulento, incluso si escribe la dirección correcta en su navegador. Este método es particularmente peligroso en el ámbito bancario, ya que permite el robo de credenciales y datos financieros sin levantar sospechas.

c. Clonación de tarjetas (Skimming)

El skimming es una técnica utilizada para obtener ilegalmente la información de tarjetas de crédito o débito. Los delincuentes instalan dispositivos en cajeros automáticos o en terminales de pago de establecimientos comerciales para copiar la banda magnética de las tarjetas cuando los usuarios realizan transacciones. En algunos casos, también utilizan cámaras ocultas para capturar el número de identificación personal (PIN). Con esta información, pueden crear tarjetas clonadas y realizar compras o retiros fraudulentos sin que el titular lo note de inmediato.

d. Fraude en comercio electrónico

El auge de las compras en línea ha dado lugar a diversas formas de fraude en el comercio electrónico. Entre ellas, destacan la venta de productos inexistentes, la suplantación de identidad para realizar compras fraudulentas y el uso de sitios web falsos que imitan tiendas legítimas para robar datos de pago. También es común que los estafadores se aprovechen de plataformas de pago electrónico para ofrecer servicios falsos y desaparecer una vez que han recibido el dinero.

e. Ransomware con fines de extorsión

El ransomware es un tipo de software malicioso que bloquea el acceso a los archivos o sistemas de la víctima mediante cifrado, exigiendo un pago (ransom) a cambio de su liberación. Aunque este tipo de ataque no siempre está directamente vinculado con el fraude financiero, su objetivo es obtener dinero de manera ilícita a través de la extorsión. En algunos casos, los ciberdelincuentes amenazan con divulgar información sensible si no se paga el rescate, lo que agrava las consecuencias para la víctima.

f. Ingeniería social

La ingeniería social es una estrategia basada en la manipulación psicológica para engañar a las personas y hacer que revelen información confidencial o realicen acciones que comprometan su seguridad. A diferencia de otros métodos que dependen del uso de tecnología avanzada, la ingeniería social explota la confianza y la falta de conocimiento de la víctima. Algunos ejemplos incluyen llamadas telefónicas donde los estafadores se hacen pasar por empleados de bancos para obtener datos personales o correos electrónicos en los que suplantan identidades de conocidos para solicitar dinero.

g. Fraude con criptomonedas y activos digitales

Con el crecimiento del mercado de criptomonedas, han surgido nuevas formas de fraude informático relacionadas con estos activos. Entre ellas se encuentran las estafas de inversión, en las que los delincuentes prometen rendimientos extraordinarios a cambio de que las víctimas inviertan su dinero en plataformas fraudulentas. También es frecuente el uso de malware para robar billeteras digitales y la creación de tokens falsos para engañar a compradores inexpertos.

2.2.4. Anonimato del ciberdelincuente

El artículo 336, numeral 1, del Código Procesal Penal establece que, para iniciar formalmente una investigación preparatoria, deben concurrir ciertos requisitos, tales como la existencia de indicios que sugieran la comisión de un delito, la prescripción de la acción penal, la identificación del presunto responsable y, de ser necesario, el cumplimiento de los

requisitos de procedibilidad. En consecuencia, la individualización del sujeto involucrado en un acto delictivo resulta un elemento esencial para continuar con la indagación penal. (Código Procesal Penal, 2024).

En la actualidad, una de las problemáticas más relevantes que favorecen la proliferación de la ciberdelincuencia es el anonimato. La falta de identificación del autor del delito es una de las principales características de este tipo de ilícitos, ya que los delincuentes informáticos suelen ocultar su verdadera identidad y ubicación al momento de cometer sus actos. Según la Defensoría del Pueblo (2023), esto representa un obstáculo considerable para las autoridades encargadas de la investigación y persecución de los crímenes cibernéticos.

A pesar de que cada dispositivo digital conectado a internet cuenta con un identificador único denominado dirección IP, existen diversas técnicas que permiten ocultar o alterar dicho identificador, dificultando la detección de los ciberdelincuentes. Entre los métodos empleados para evadir el rastreo se encuentran las conexiones mediante redes wifi públicas, el uso de servidores proxy y redes privadas virtuales (VPN), así como la implementación de redes botnet (Barrio, 2017). Estos mecanismos constituyen un reto significativo para los operadores de justicia, quienes deben enfrentar múltiples dificultades al intentar identificar y localizar a los responsables de delitos informáticos.

Espinoza (2023), señala que los factores que imposibilitan la lucha contra la cibercriminalidad, es el anonimato potencial del autor y a la vez la ejecución a distancia que son propios del medio digital. De esta manera, se hallan dificultades para detectar al autor del delito de fraude informático, siendo de esta manera, dificultoso su persecución penal.

2.2.4.1. Uso de identidades falsas y cuentas fraudulentas

El anonimato en el ámbito digital no solo dificulta la identificación de los ciberdelincuentes, sino que también permite la ejecución de fraudes sin que se pueda responsabilizar directamente al titular de la cuenta utilizada. En algunos casos, las cuentas receptoras de transferencias fraudulentas no pertenecen a los verdaderos perpetradores, sino a terceros que han sido engañados o cuyos datos han sido sustraídos para fines ilícitos (Espinoza Calderón, 2023).

Un método comúnmente utilizado en este tipo de delitos es la creación de sitios web fraudulentos que simulan ser plataformas oficiales de entidades bancarias. A través de estas páginas falsas, los delincuentes solicitan información confidencial a las víctimas, como números de tarjetas, contraseñas y claves token. Una vez que las personas ingresan sus datos, los estafadores obtienen acceso a sus cuentas bancarias y pueden sustraer los fondos sin dejar rastro inmediato (Defensoría del Pueblo, 2023).

2.2.4.2. Factores que contribuyen a la vulnerabilidad informática

De acuerdo con Villavicencio (2014), existen varios factores que aumentan la vulnerabilidad en el entorno digital, las cuales son:

- La inexistencia de un sistema jerárquico de control en la red que permita verificar la información que circula en ella.
- El crecimiento constante del número de usuarios que desconocen los riesgos asociados al uso de la tecnología.
- La posibilidad de mantener el anonimato en el ciberespacio, lo que dificulta la identificación de los responsables de actos ilícitos.
- El acceso irrestricto a la información, lo que permite la manipulación de datos y el ataque a sistemas informáticos.

Por otro lado, la Interpol, institución conformada por organismos policiales de 194 países, ha identificado seis factores adicionales que favorecen la ciberdelincuencia (Defensoría del Pueblo, 2023):

- **Mayor conectividad:** El creciente número de usuarios en línea, muchos de los cuales desconocen los principios básicos de seguridad digital, expone más datos personales a posibles ataques.
- **Expansión de la movilidad:** El uso de dispositivos móviles ha incrementado el número de transacciones y comunicaciones digitales sin las medidas de protección adecuadas.

- **Interconectividad global:** La proliferación de dispositivos inteligentes ha generado más puntos vulnerables que pueden ser explotados por los ciberdelincuentes.

- **Mayor sofisticación del delito:** Los ciberdelincuentes han perfeccionado sus métodos y ofrecen sus conocimientos a terceros a cambio de una compensación económica, sin importar si se trata de actividades ilícitas.

- **Falta de denuncia:** Muchas víctimas no reportan los delitos informáticos debido al desconocimiento de los procedimientos, la percepción de ineficacia de las autoridades o la vergüenza de haber sido estafadas.

- **Dificultades en la cooperación internacional:** Dado que los ciberdelitos suelen cometerse desde distintas jurisdicciones, las investigaciones pueden ser complejas y prolongadas, lo que retrasa o impide la captura de los responsables.

El anonimato en el ciberespacio es una de las principales razones por las cuales los delitos informáticos quedan impunes. Si el Ministerio Público no logra identificar e individualizar a los responsables, la investigación no puede continuar, lo que conlleva al archivo del proceso (Código Procesal Penal, 2024). En este sentido, la falta de regulación efectiva y la dificultad para rastrear a los ciberdelincuentes representan desafíos significativos para las autoridades. Es fundamental fortalecer las capacidades técnicas de las entidades encargadas de la seguridad digital y fomentar la cooperación internacional con el objetivo de reducir la impunidad en este tipo de delitos. Asimismo, se debe tener en cuenta que, para archivar un delito de fraude informático a causa de falta de indicios reveladores del delito, el Ministerio Público debe conducir la realización de diligencias preliminares, orientadas a la búsqueda de indicios o datos que permitan determinar la existencia del delito. En este sentido, el inciso 1 del artículo 336 del Código Procesal Penal establece que la formalización de la investigación preparatoria se basa en la teoría de la imputación concreta, concepto que, según Francisco Celis Mendoza Ayma, se refiere a *“la atribución más o menos fundada que se le hace a una persona de un acto presuntamente punible”.* Ayma (2023)

2.2.5. Factores que favorecen la ciberdelincuencia

Según Segrera & Cano (2010), uno de los principales inconvenientes que enfrenta el sistema judicial en la lucha contra los delitos informáticos es la insuficiente formación de los operadores jurídicos. No todos cuentan con conocimientos profundos en esta materia, lo que representa un reto significativo. Es crucial trabajar en este aspecto para garantizar la existencia de especialistas con las competencias necesarias en este campo del derecho (p. 221).

Dada la complejidad y evolución constante de los delitos informáticos, se requiere la presencia de expertos con formación actualizada en tecnologías de la información y las comunicaciones. La ausencia de estas habilidades dificulta la adecuada persecución penal de estos crímenes. En este sentido, la falta de capacitación puede llevar a que los jueces no logren interpretar correctamente las pruebas digitales, lo que afecta la resolución de los casos. Por ello, es imprescindible implementar programas de formación especializada dirigidos a jueces, fiscales, policías y abogados, pues un conocimiento insuficiente en esta área podría generar obstáculos en los procesos de investigación y sanción de los responsables.

Espinoza Calderón (2022) sostiene que resulta fundamental reforzar la formación de los futuros profesionales del derecho desde el ámbito universitario, promoviendo la incorporación del Derecho Informático como una asignatura obligatoria en los planes curriculares de las facultades de Derecho. Este curso debería incluir contenidos clave como el comercio electrónico, la firma digital, los documentos electrónicos, los delitos informáticos y la prueba digital, todos ellos indispensables para una comprensión integral de los ciberdelitos en el contexto jurídico actual.

Asimismo, la capacitación en delitos informáticos no debe estar restringida únicamente a fiscalías especializadas, sino extenderse a todas las fiscalías, comisarías, juzgados y demás organismos judiciales, ya que estas infracciones pueden ocurrir en cualquier lugar del país. Además, es fundamental promover la formación del público en general a través de campañas de sensibilización en instituciones educativas, asociaciones

y medios de comunicación. En suma, resulta indispensable fomentar una cultura digital que incentive el uso responsable y seguro del internet en toda la sociedad.

En relación con los retos que plantea la investigación del ciberdelito, el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (2010) destacó que la colaboración ágil y efectiva entre distintos países es un elemento clave. Este aspecto cobra especial relevancia en delitos cibernéticos, donde la evidencia digital tiende a desaparecer en poco tiempo. Los procedimientos burocráticos pueden representar un obstáculo significativo para las investigaciones, ya que muchos acuerdos de cooperación internacional aún dependen de trámites extensos y complejos. En este sentido, es crucial implementar mecanismos que permitan respuestas inmediatas ante incidentes y solicitudes de colaboración.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa establece en su capítulo III diversas directrices para la consolidación de un marco legal que favorezca la cooperación internacional en la investigación de delitos informáticos. Entre los puntos destacados, se resalta la importancia de emplear medios de comunicación rápidos, como el correo electrónico y el fax, y la necesidad de contar con puntos de contacto disponibles las 24 horas del día para atender solicitudes de otros Estados (art. 35).

Tejada (2017) señala que enfrentar eficazmente los delitos informáticos exige no solo contar con un marco legal adecuado que facilite las labores investigativas, sino también aprovechar de forma estratégica los recursos tecnológicos para mejorar la capacidad de respuesta ante estas conductas ilícitas. Uno de los principales obstáculos identificados es la lentitud en la obtención de información por parte de los proveedores de servicios de internet, quienes aún no disponen de sistemas eficientes para responder a solicitudes legales como las órdenes de retención de datos. A ello se suma una cierta reticencia de estas empresas a proporcionar información sobre sus usuarios, lo cual representa una barrera significativa para el avance de las investigaciones penales.

Así también, en años pasados, las problemáticas vinculadas a la criminalidad informática solían abordarse exclusivamente mediante programas y controles tecnológicos, bajo la premisa de que la solución debía provenir de la misma tecnología. No obstante, con

la evolución de los sistemas de seguridad y prevención, los ciberdelincuentes han desarrollado nuevas estrategias para sortearlos. Ante esta realidad, los operadores de justicia deben adquirir conocimientos especializados para realizar investigaciones y procesos judiciales efectivos en esta materia. A pesar del aumento de los delitos informáticos, sigue habiendo una notable escasez de profesionales capacitados para identificarlos, analizarlos y procesarlos judicialmente (Segrera & Cano, 2010, p. 222).

En resumen, hacer frente a los delitos informáticos requiere una estrategia integral que incluya la capacitación técnica de los operadores de justicia, la continua adecuación de las leyes vigentes y la consolidación de la colaboración a nivel internacional. Solo a través de un enfoque articulado y cooperativo se podrá abordar de manera efectiva este fenómeno en constante transformación.

2.2.6. Estrategias para combatir los Delitos Informáticos

Una lucha efectiva contra los delitos informáticos requiere la aplicación de múltiples estrategias que aborden tanto la prevención como la persecución penal. Estas estrategias deben incluir marcos normativos sólidos, capacitación especializada, cooperación internacional y el uso de tecnologías avanzadas. A continuación, se presentan las principales estrategias para combatir este fenómeno delictivo.

2.2.6.1. Fortalecimiento del Marco Legal

Uno de los principales desafíos en la lucha contra los delitos informáticos es la falta de legislación adecuada o su desactualización frente a la evolución de las tecnologías. Es fundamental que los países actualicen constantemente sus normativas para tipificar correctamente los ciberdelitos y establecer sanciones proporcionales. La adopción del Convenio de Budapest sobre ciberdelincuencia ha sido una de las iniciativas más relevantes a nivel internacional, ya que proporciona directrices para la criminalización de diversas conductas ilícitas en el entorno digital. Asimismo, resulta clave regular la recolección y preservación de la evidencia digital para garantizar su validez en los procesos judiciales.

2.2.6.2. Capacitación y Especialización de los Operadores de Justicia

La correcta investigación y persecución de los delitos informáticos depende, en gran medida, del conocimiento técnico de los jueces, fiscales, policías y abogados. Sin embargo, la falta de especialización en derecho informático y ciberseguridad representa una barrera para el procesamiento efectivo de estos casos. Por ello, es imprescindible la implementación de programas de formación contínua en prueba digital, ciberseguridad y normativa informática. Además, la creación de fiscalías y unidades policiales especializadas contribuiría a mejorar la respuesta ante este tipo de delitos. A nivel universitario, la incorporación de materias sobre Derecho Informático y delitos cibernéticos en los planes de estudio ayudaría a formar nuevos profesionales capacitados en la materia.

2.2.6.3. Cooperación Internacional

Dado que los delitos informáticos suelen trascender fronteras, la cooperación internacional es fundamental para su combate. La rápida asistencia entre países facilita la identificación y captura de ciberdelincuentes, especialmente en casos donde se requiere la preservación inmediata de pruebas digitales. Es crucial que los Estados establezcan acuerdos de cooperación judicial para agilizar los trámites burocráticos en estos casos. Organismos como INTERPOL, Europol y el Grupo de Trabajo sobre Delitos Cibernéticos de la ONU desempeñan un papel clave en la coordinación de esfuerzos globales. Además, el establecimiento de puntos de contacto 24/7 permite una respuesta inmediata ante incidentes transnacionales.

2.2.6.4. Uso de tecnología para la prevención y persecución

El desarrollo y uso de herramientas tecnológicas avanzadas es esencial para combatir el cibercrimen. La aplicación de inteligencia artificial y análisis forense digital permite detectar patrones de comportamiento sospechosos y rastrear la actividad de ciberdelincuentes. Asimismo, los sistemas de monitoreo en tiempo real pueden ayudar a prevenir ataques informáticos y detectar fraudes en plataformas digitales. La creación de bases de datos centralizadas con información sobre delincuentes informáticos también facilita la identificación y el seguimiento de estos actores en el ciberespacio.

2.2.6.5. Concienciación y educación digital

Una de las estrategias más efectivas en la lucha contra los delitos informáticos es la prevención mediante la educación y concientización de la sociedad. Múltiples víctimas caen en fraudes y ataques informáticos por desconocimiento de las amenazas existentes. Es fundamental realizar campañas de sensibilización dirigidas a empresas, estudiantes y ciudadanos en general, promoviendo prácticas seguras como el uso de contraseñas robustas, autenticación en dos pasos y cifrado de datos. De la misma forma, es importante que las instituciones educativas integren la enseñanza de seguridad digital en sus programas de formación.

2.2.6.6. Regulación y responsabilidad de Empresas Tecnológicas

Las empresas que ofrecen servicios digitales juegan un rol crucial en la prevención de los delitos informáticos. Es necesario que los proveedores de servicios de internet (ISP) colaboren con las autoridades en la entrega de información relevante para la investigación de estos delitos. También se debe exigir a las plataformas digitales la implementación de medidas de seguridad, autenticación reforzada y mecanismos de detección de fraudes. La creación de protocolos de retención y entrega de datos en investigaciones criminales permitiría agilizar la identificación de ciberdelincuentes sin vulnerar la privacidad de los usuarios.

2.2.6.7. Creación de Centros de Respuesta ante Incidentes Cibernéticos (CSIRT)

Los Centros de Respuesta ante Incidentes Cibernéticos (CSIRT) son organismos especializados en la detección, análisis y mitigación de ataques informáticos. Estos centros operan en coordinación con entidades gubernamentales y privadas para responder de manera eficaz a incidentes de ciberseguridad. La implementación de protocolos de acción rápida permite minimizar el impacto de ataques cibernéticos masivos, protegiendo infraestructuras críticas y datos sensibles. Además, los CSIRT pueden desempeñar un papel clave en la formación de personal especializado en ciberseguridad.

El combate contra los delitos informáticos requiere una estrategia integral que combine la actualización de normativas, la especialización de operadores de justicia, la cooperación internacional, el uso de tecnología avanzada y la educación digital. La colaboración entre Estados, empresas tecnológicas y ciudadanos es esencial para mitigar el impacto de estos crímenes y fortalecer la seguridad en el entorno digital.

2.3. Marco conceptual

a. **Ciberdelincuencia:** Es el conjunto de actividades ilícitas que se cometen a través de medios informáticos o en el entorno digital, particularmente utilizando redes como Internet. Estas conductas delictivas pueden incluir desde el acceso no autorizado a sistemas o datos (hacking), la sustracción de información personal o financiera, hasta delitos más complejos como el fraude electrónico, la suplantación de identidad, la distribución de malware y el ciberacoso. La ciberdelincuencia representa un desafío creciente para la seguridad jurídica y tecnológica, ya que evoluciona constantemente al ritmo del desarrollo tecnológico y la globalización de la información.

b. **Fraude Informático:** Es toda conducta ilícita que, mediante la manipulación o el uso indebido de sistemas informáticos, redes electrónicas o datos digitales, tiene como finalidad obtener un beneficio económico indebido o causar perjuicios a terceros. Este tipo de fraude se caracteriza por el uso de herramientas tecnológicas para acceder, alterar, eliminar, o introducir información en sistemas computarizados, de forma intencionada y sin autorización, con el fin de engañar o generar pérdidas económicas a individuos, empresas o entidades gubernamentales.

c. **Individualización del Ciberdelincuente:** Es el proceso mediante el cual se busca identificar de manera precisa y concreta al autor o responsable de una conducta delictiva cometida a través de medios informáticos o digitales. Este proceso implica la recolección, análisis y validación de evidencias digitales con el objetivo de establecer la identidad del sujeto activo, su grado de participación en el hecho delictivo, y su relación directa con los dispositivos o redes utilizados para perpetrar el delito. Desde una perspectiva técnico-jurídica, la individualización requiere la

aplicación de técnicas de informática forense, rastreo digital, análisis de direcciones IP, uso de metadatos, y otras herramientas tecnológicas que permitan vincular una acción digital a una persona física o jurídica. Este procedimiento es crucial para garantizar el debido proceso, la responsabilidad penal, y la administración de justicia en los casos de ciberdelincuencia.

d. **Archivo de Casos:** El archivo de casos es una figura jurídica que se refiere a la decisión de suspender o no continuar con la investigación de un hecho presuntamente delictivo, ya sea por falta de pruebas suficientes, inexistencia del hecho punible, imposibilidad de identificar al autor, o por otros motivos contemplados en la legislación penal o procesal correspondiente. En el contexto de la ciberdelincuencia, el archivo de casos puede estar relacionado con la dificultad para obtener pruebas digitales, la imposibilidad de individualizar al ciberdelincuente, o la falta de cooperación internacional, lo que limita la eficacia del sistema penal frente a los delitos informáticos.

e. **Cooperación Interinstitucional:** Se refiere al conjunto de acciones, mecanismos y estrategias coordinadas entre dos o más instituciones, ya sean públicas o privadas, con el propósito de compartir información, recursos, capacidades técnicas y operativas para alcanzar objetivos comunes. En el ámbito de la investigación criminal y, en particular, de la lucha contra la ciberdelincuencia, la cooperación interinstitucional resulta fundamental para enfrentar eficazmente fenómenos delictivos complejos, transnacionales y tecnológicamente avanzados.

f. **Impacto Social:** Se entiende como el conjunto de efectos, consecuencias o transformaciones que una acción, fenómeno, política, programa o suceso produce en la estructura, el funcionamiento y el bienestar de una sociedad o de un grupo social específico. Este impacto puede manifestarse en distintos ámbitos, como el económico, cultural, político, psicológico o tecnológico, y puede tener consecuencias tanto positivas como negativas, inmediatas o a largo plazo. En el contexto de la ciberdelincuencia, el impacto social se refleja en el aumento de la percepción de inseguridad digital, la pérdida de confianza en los sistemas tecnológicos, el daño a la reputación de personas o instituciones, la afectación a

derechos fundamentales como la privacidad, y la generación de nuevas formas de exclusión o vulnerabilidad.

g. **Phishing:** Es una modalidad de fraude informático que consiste en el envío de comunicaciones falsas, generalmente a través de correos electrónicos, mensajes de texto o sitios web falsificados, con el objetivo de engañar a las personas para que revelen información confidencial, como contraseñas, números de tarjetas de crédito, credenciales bancarias o datos personales.

h. **Carding:** Es una forma de ciberdelito que consiste en la obtención, tráfico y uso no autorizado de datos de tarjetas de crédito o débito con el fin de realizar transacciones fraudulentas. Esta práctica implica el acceso ilegal a información financiera confidencial mediante diversas técnicas, como el phishing, el uso de malware, la interceptación de comunicaciones electrónicas, o la compra de datos robados en mercados ilícitos de la dark web. Los individuos que se dedican al carding, conocidos como carders, utilizan esta información para realizar compras en línea, transferencias, o incluso para clonar tarjetas físicas.

i. **Ciberseguridad:** Es el conjunto de estrategias, medidas, prácticas y tecnologías destinadas a proteger los sistemas informáticos, redes, dispositivos electrónicos, programas y datos frente a accesos no autorizados, ataques maliciosos, daños o cualquier forma de uso indebido. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información digital, así como preservar la seguridad de las infraestructuras tecnológicas frente a amenazas tanto internas como externas.

j. **Fiscal:** Es el funcionario público encargado de dirigir, promover y ejercer la acción penal en representación del Estado, con el fin de investigar los delitos, proteger los intereses de la sociedad y garantizar el respeto a los derechos fundamentales durante el proceso penal. El representante del Ministerio Público tiene la responsabilidad de coordinar la investigación de los hechos delictivos, en colaboración con las fuerzas policiales y peritos especializados, así como de reunir y presentar pruebas ante los tribunales. En el contexto de la ciberdelincuencia, el rol

del fiscal adquiere particular relevancia, ya que debe enfrentar desafíos como la complejidad técnica de los delitos informáticos, la recolección de evidencia digital, y la cooperación interinstitucional e internacional para identificar e imputar a los responsables.

k. **Diligencias preliminares:** Son el conjunto de actuaciones procesales iniciales que realiza el Ministerio Público (fiscal) con el fin de verificar la existencia de un hecho delictivo, identificar a sus presuntos autores y reunir los elementos básicos de prueba que justifiquen el inicio formal de un proceso penal. Estas diligencias constituyen una fase previa a la imputación formal y tienen como finalidad determinar si existen méritos suficientes para ejercer la acción penal. En el contexto de la ciberdelincuencia, las diligencias preliminares revisten especial importancia debido a la naturaleza volátil de la evidencia digital, la necesidad de actuar con rapidez para preservar datos, y la frecuente intervención de múltiples jurisdicciones o actores tecnológicos (como proveedores de servicios en línea).

l. **Investigación preparatoria:** Viene a ser una etapa del proceso penal, la cual tiene por objeto determinar la existencia de delitos y la individualización de los presuntos autores. Además, tiene por finalidad preparar la acusación, determinando la prueba relevante que se producirá en el juicio. Esta se encuentra regulada en el artículo 321° del Código Procesal Penal.

m. **Persecución penal:** Es el conjunto de actos procesales y jurídicos que realiza el Estado, a través del Ministerio Público (fiscalía), con el fin de investigar, identificar, acusar y sancionar a los responsables de la comisión de un delito, en observancia del debido proceso y las garantías constitucionales. Esta función forma parte esencial del ius puniendi del Estado y tiene como propósito asegurar la vigencia del orden jurídico, la protección de los derechos fundamentales y la restauración de la legalidad vulnerada.

n. **Protocolo de internet:** Comúnmente conocido por sus siglas IP (Internet Protocol), es un conjunto de reglas que rigen el formato, direccionamiento y envío de datos a través de redes digitales, especialmente en Internet. Este protocolo permite que los

dispositivos conectados a una red (como computadoras, teléfonos, servidores o routers) se identifiquen mediante una dirección única, conocida como dirección IP, y puedan comunicarse entre sí de manera efectiva y ordenada. En el ámbito de la ciberdelincuencia, las direcciones IP juegan un rol clave en la identificación y rastreo de actividades delictivas en línea, ya que permiten ubicar el origen de una conexión, dispositivo o usuario, aunque su precisión puede verse afectada por el uso de tecnologías como VPNs, proxys, o redes TOR. El análisis forense de direcciones IP forma parte de las técnicas de informática forense utilizadas en las investigaciones preliminares y en la persecución penal de delitos informáticos, siendo fundamental para la individualización del ciberdelincuente.

o. **Sistema informático:** Son conjuntos organizados de componentes tecnológicos y lógicos diseñados para la captura, procesamiento, almacenamiento, transmisión y gestión de información digital. Estos sistemas están conformados por elementos tanto hardware (equipos físicos como computadoras, servidores, redes, etc.) como software (programas, aplicaciones y sistemas operativos), y operan bajo reglas y procedimientos que permiten el funcionamiento automatizado de tareas y procesos.

p. **SIM Swapping:** Conocido como el intercambio o duplicación de tarjeta SIM, es una técnica de ciberdelincuencia mediante la cual un atacante consigue transferir el número telefónico de una víctima a una tarjeta SIM en su poder, generalmente a través del engaño o manipulación de empleados de una operadora de telefonía móvil, o mediante el uso de información personal previamente obtenida de forma ilícita. Una vez que el delincuente controla el número telefónico, puede recibir los mensajes de verificación (SMS), llamadas y notificaciones de seguridad, lo que le permite acceder a cuentas bancarias, redes sociales, correos electrónicos u otros servicios protegidos mediante mecanismos de autenticación de dos factores, que utilizan el número móvil como medio de verificación.

q. **Thief Transfer:** Es una modalidad de fraude cibernético mediante la cual un delincuente informático transfiere de manera ilícita fondos, activos digitales o información confidencial desde la cuenta de una víctima hacia otra cuenta controlada por el propio atacante o por terceros (a menudo denominados mulas).

Esta operación suele ejecutarse luego de vulnerar sistemas informáticos, acceder ilegalmente a plataformas bancarias o de pago, o mediante el uso de credenciales robadas.

r. **Software malicioso:** El software malicioso, también conocido como malware (abreviación de malicious software), se define como cualquier programa o código informático diseñado con la intención de dañar, interrumpir, robar o, en general, realizar acciones no autorizadas sobre sistemas, redes o dispositivos informáticos. Este tipo de software puede adoptar múltiples formas, tales como virus, gusanos, troyanos, ransomware, spyware, adware y rootkits, entre otros. Su principal objetivo suele ser comprometer la confidencialidad, integridad o disponibilidad de la información, así como afectar el funcionamiento normal de los sistemas afectados. El software malicioso representa una de las principales amenazas a la seguridad informática y su estudio es fundamental para el desarrollo de estrategias de prevención, detección y mitigación en entornos digitales.

s. **Criptomonedas:** Son un tipo de activo digital que utiliza la criptografía como mecanismo de seguridad para realizar transacciones financieras, controlar la creación de nuevas unidades y verificar la transferencia de activos. Estas monedas digitales operan sobre redes descentralizadas basadas en tecnología blockchain (cadena de bloques), lo que elimina la necesidad de intermediarios tradicionales, como bancos o entidades gubernamentales. Entre las criptomonedas más conocidas se encuentran Bitcoin, Ethereum y Litecoin. Las criptomonedas permiten transacciones rápidas, globales y en muchos casos anónimas, aunque su uso también plantea desafíos en términos de regulación, seguridad y volatilidad del mercado.

CAPÍTULO III: HIPÓTESIS Y VARIABLES

3.1. Formulación de hipótesis

3.1.1. Hipótesis General

Las dificultades en la individualización del ciberdelincuente influyen significativamente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023, debido a la falta de herramientas tecnológicas especializadas y la insuficiente capacitación de los fiscales, lo que limita la identificación y persecución de los responsables.

3.1.2. Hipótesis Específicas

a. Primera Hipótesis específica

La falta de herramientas tecnológicas especializadas dificulta la identificación de los ciberdelincuentes en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023, lo que impide obtener pruebas suficientes y contribuye al archivo de los casos de fraude informático.

b. Segunda Hipótesis específica

La insuficiente capacitación de los fiscales afecta negativamente la individualización del ciberdelincuente, lo que limita la efectividad de la investigación y aumenta la probabilidad de que los casos de fraude informático sean archivados en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023.

3.2. Variables e indicadores

3.2.1. Variable Independiente

Dificultades en la individualización del ciberdelincuente: Se refiere a los obstáculos técnicos, operativos y legales que enfrenta la Segunda Fiscalía Provincial Penal

Corporativa de Huamanga para identificar y localizar a los responsables de delitos de fraude informático. Estas dificultades incluyen la falta de recursos tecnológicos, la escasa capacitación del personal, la complejidad de los métodos utilizados por los ciberdelincuentes y las limitaciones en la cooperación interinstitucional.

3.2.1.1. Dimensiones e indicadores de la variable independiente

a. Recursos Tecnológicos

- Disponibilidad de software de análisis forense.
- Uso de herramientas de rastreo de IP y transacciones digitales.
- Acceso a bases de datos y sistemas de inteligencia.

b. Capacitación del Personal

- Nivel de especialización en ciberseguridad del personal de la fiscalía.
- Frecuencia de capacitaciones en delitos informáticos.
- Conocimiento de técnicas de investigación digital.

c. Métodos de los Ciberdelincuentes

- Uso de tecnologías avanzadas (VPN, cifrado, criptomonedas).
- Anonimato en la red (cuentas falsas, identidades ocultas).
- Complejidad de las transacciones fraudulentas.

d. Cooperación Interinstitucional

- Colaboración con entidades especializadas (policía, empresas tecnológicas).
- Intercambio de información con organismos nacionales e internacionales.
- Coordinación con instituciones financieras para rastrear transacciones.

3.2.1.2. Variable Dependiente

Archivo de los delitos de fraude informático: Se refiere a la decisión de la fiscalía de cerrar o archivar un caso de fraude informático debido a la falta de pruebas, la imposibilidad de identificar a los responsables o la insuficiencia de recursos para continuar la investigación. Esta variable refleja la inoperancia de las investigaciones y la incapacidad de la fiscalía para resolver este tipo de delitos.

3.2.1.3. Dimensiones e indicadores de la variable dependiente

a. Tasa de Archivo de Casos

- Porcentaje de casos archivados respecto al total de denuncias ingresadas.
- Número de casos archivados por falta de pruebas.
- Número de casos archivados por dificultad en la individualización del ciberdelincuente.

b. Causas de Archivo:

- Falta de pruebas concretas (transacciones no rastreables, ausencia de testigos).
- Dificultad para identificar a los responsables (anonimato, uso de tecnologías avanzadas).
- Limitaciones en recursos humanos y tecnológicos.

c. Impacto del Archivo:

- Nivel de insatisfacción de las víctimas con el proceso de investigación.
- Percepción de impunidad entre la población.
- Desconfianza ciudadana en el sistema de justicia penal.

3.3. Operacionalización de variables e indicadores

Variables	Dimensiones	Indicadores	Ítems	Escala de medición
Variable independiente: Dificultades en la individualización del ciberdelincuente.	**Recursos Tecnológicos**	• Disponibilidad de software de análisis forense. • Uso de herramientas de rastreo de IP y transacciones digitales. • Acceso a bases de datos y sistemas de inteligencia.	**1.** ¿La falta de recursos tecnológicos (software de análisis forense, herramientas de rastreo) dificulta la individualización de los ciberdelincuentes? **2.** ¿El personal de la fiscalía carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva? **3.** ¿Los métodos utilizados por los ciberdelincuentes (anonimato, cifrado) hacen casi imposible su identificación? **4.** ¿La falta de cooperación interinstitucional (con policía, empresas tecnológicas, etc.) afecta negativamente la investigación de estos delitos?	LIKERT: 1 = Nunca 2 = Casi nunca 3 = Algunas veces 4 = Casi siempre 5 = Siempre
	Capacitación del Personal	• Nivel de especialización en ciberseguridad del personal de la fiscalía. • Frecuencia de capacitaciones en delitos informáticos. • Conocimiento de técnicas de investigación digital.		

	Métodos de los Ciberdelincuentes	• Uso de tecnologías avanzadas (VPN, cifrado, criptomonedas). • Anonimato en la red (cuentas falsas, identidades ocultas). • Complejidad de las transacciones fraudulentas.	**5.** ¿La mayoría de los casos de fraude informático se archivan debido a la imposibilidad de identificar a los responsables? **6.** ¿La fiscalía no cuenta con herramientas tecnológicas avanzadas para rastrear transacciones fraudulentas? **7.** ¿El personal de la fiscalía no recibe capacitación constante en técnicas de investigación digital? **8.** ¿La falta de elementos de convicción (transacciones no rastreables, ausencia de testigos) es la principal razón por la que los casos se archivan? **9.** ¿La dificultad para identificar a los responsables (anonimato, uso de tecnologías avanzadas) lleva al archivo de la mayoría de los casos? **10.** ¿El archivo de casos de fraude informático genera impunidad?	
	Cooperación Interinstitucional	• Colaboración con entidades especializadas (policía, empresas tecnológicas). • Intercambio de información con organismos nacionales e internacionales. • Coordinación con instituciones financieras para rastrear transacciones.		
Variables	Dimensiones	Indicadores		
Variable Dependiente: Archivo de los delitos de fraude informático.	**Tasa de Archivo de Casos**	• Porcentaje de casos archivados respecto al total de denuncias ingresadas. • Número de casos archivados por falta de pruebas.		

		• Número de casos archivados por dificultad en la individualización del ciberdelincuente.		
	Causas de Archivo	• Falta de pruebas concretas (transacciones no rastreables, ausencia de testigos). • Dificultad para identificar a los responsables (anonimato, uso de tecnologías avanzadas). • Limitaciones en recursos humanos y tecnológicos.		
	Impacto del Archivo	• Nivel de insatisfacción de las víctimas con el proceso de investigación. • Percepción de impunidad entre la población. • Desconfianza ciudadana en el sistema de justicia penal.		

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1. 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)

4.2. 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.

4.3. Tipo de investigación

La presente ***investigación es aplicada,*** ya que tiene por finalidad 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.

En otras palabras, no sólo busca explicar de qué manera influyen las dificultades en la individualización del ciberdelincuente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023, sino que además propone soluciones que coadyuven a superar dichas dificultades.

4.4. Método de la Investigación

Se usó el ***método deductivo****,* el cual 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.

4.5. Diseño de la investigación

Este estudio se considera ***no experimental***, porque 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 las disposiciones de archivo en casos de fraude informático ya solicitados, sin que el investigador esté involucrado en la recopilación en tiempo real.

4.6. Universo, población y muestra

4.6.1. Universo

Conformado por todos los casos de fraude informático del Distrito Fiscal de Ayacucho durante el 2023.

4.6.2. Población

La población está constituida por los 37 casos reportados de fraude informático en la Segunda Fiscalía Penal Corporativa de Huamanga, durante el año 2023, (figura 01).

4.6.3. Muestra

La muestra se conforma por 20 carpetas fiscales en casos de fraude informático, investigados en la Segunda Fiscalía Penal Corporativa de Huamanga, durante el año 2023.

4.6.3.1. Tipo de muestra

La presente investigación utiliza el tipo de Muestreo ***no probabilístico***, para el autor 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. 189-191). 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 20 carpetas fiscales se basó en la disponibilidad de los casos, no en un proceso aleatorio o sistemático.

Asimismo, el tipo de muestreo no probabilístico 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". (Sánchez, 2016, p. 180)

4.7. Técnicas, instrumentos y fuentes de recojo de la información

4.7.1. Técnicas de recolección de datos

4.7.1.1. Técnica de Encuesta

"La técnica de la encuesta nos permite recoger información objetiva, las mismas que nos sirve poder responder a nuestros objetivos planteados en el presente trabajo de investigación. La encuesta es considerada una técnica (también instrumento) de investigación que permite dar respuesta a un problema tanto en términos descriptivos como de relación de variable tras la recolección de información sistemática". (Arazamendi, 2013, p. 121)

4.7.1.2. Técnica de Análisis documental

La técnica de análisis documental implica el examen sistemático y detallado de documentos, textos, o registros para obtener información relevante sobre un tema específico. Los instrumentos utilizados en el análisis documental varían según el contexto y los objetivos de la investigación.

4.7.2. Instrumentos de recojo de datos

4.7.2.1. Instrumento Cuestionario

(Sánchez, 2016, p. 193), señala que el instrumento del cuestionario "Es un conjunto de preguntas presentadas en un documento con el propósito que sean respondidas por las personas de quienes se busca obtener la información, a diferencia del interrogatorio verbal,

este es por medio escrito". Ello, con la finalidad de realizar preguntas predefinidas a los participantes (personal Fiscal y abogados), quienes respondieron para la comprobación de las hipótesis del trabajo de investigación.

4.7.2.2. Instrumento de ficha de análisis de documentos

Para la obtención de datos se utilizó la ficha de análisis de documentos aplicada a las disposiciones de archivo del delito de fraude informático, siendo este el proceso de descripción física o externa de un documento, permite la identificación inequívoca del documento. Actúa sobre el soporte e identifica los datos externos de un documento que lo distinguen de otro, proporcionando una identificación individual.

4.7.3. Fuentes

Se utilizó como fuentes de investigación en el presente trabajo, libros especializados en materia de derecho penal, procesal penal y delitos informáticos; asimismo, carpetas fiscales archivadas y consentidas sobre el delito de fraude informático; y finalmente, personal fiscal y abogados para la recolección de datos en las encuestas elaboradas.

- **Fuentes Primarias:** Disposiciones de archivo en casos de Fraude informático durante el año 2023, en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga.

- **Fuentes Secundarias:** Bibliografía, sitios web, normas legales.

4.8. Proceso de validación y confiabilidad de los instrumentos

Según el autor Carrasco, se debe tener en cuenta que los instrumentos que se emplean en el trabajo de investigación, deben contener ciertas características que garantice el logro del objetivo planteado, pues es menester que estos sean adecuados y pertinentes de acuerdo al diseño metodológico; en ese sentido, previo a la aplicación de dichos instrumentos, es necesario cotejar su eficacia y confiabilidad. Por lo que, la validación de aquellos tiene por objetivo que la medición de las variables estudiadas se realice con la mayor objetividad y legitimidad posible (Carrasco, 2006).

Siendo así, en el presente trabajo de investigación, se recurrió a personal fiscal encargado de investigar los delitos de fraude informático; y, a abogados litigantes que desde su experiencia en la práctica han podido contrastar las dificultades que se tiene respecto a este tipo de delito; y justamente ello coadyuvó para la validación de los instrumentos de la investigación consistente en los ítems de preguntas impresas. De igual forma, se recurrió a la validación del instrumento de investigación consistente en la ficha de análisis documental, mediante la cual se procedió a realizar el análisis de las carpetas fiscales del delito de fraude informático.

4.9. Procesamiento de datos recolectados

Clasificación: En cuanto al diseño de las interrogantes para el recojo de datos, estas se elaboraron de acuerdo a la variable postulada, tanto independiente como dependiente.

Codificación: Las respuestas señaladas para las preguntas están codificadas en orden correlativo del 1 al 5 de la siguiente manera, para lo cual se va utilizar la escala de Likert:

1. **Nunca**
2. **Casi nunca**
3. **Algunas veces**
4. **Casi siempre**
5. **Siempre**

4.10. Tabulación

En relación a la tabulación de datos se usó SPSS Statistics, a través de la codificación de cada respuesta obtenida, de las preguntas realizadas y las tablas; la cual se construirá en base a una tabla de frecuencia, conforme a los datos que se hayan obtenido de la tabulación, donde se tomará en cuenta la frecuencia porcentual; ello nos permitirá poder elaborar los gráficos; que serán trabajados en representaciones gráficas; los mismos que nos va poder permitir un mejor entendimiento de los resultados, hecho que nos concederá una comprensión global, rápida y directa de la información que aparece en cifras.

CAPÍTULO V: ANÁLISIS Y DISCUSIÓN DE RESULTADOS

5.1. Interpretación de resultados

Figura 1: Denuncias ingresadas por delitos informáticos, periodo 2022-2023

DISTRITO FISCAL DE AYACUCHO
AREA DE GESTION DE INDICADORES

DISTRITO FISCAL DE AYACUCHO
FISCALIAS PROVINCIALES PENALES CORPORATIVAS DE HUAMANGA
DENUNCIAS INGRESADAS POR DELITOS INFORMÁTICOS
PERIODO: 2022 - 2023

FISCALIA	AÑO		Total general
	2022	2023	
1° FPPC HUAMANGA	1	28	29
2° FPPC HUAMANGA	19	37	56
3° FPPC HUAMANGA	33	39	72
4° FPPC HUAMANGA	23	20	43
5° FPPC HUAMANGA	34	35	69
6° FPPC HUAMANGA	17	39	56
Total general	**127**	**198**	**325**

FUENTE: Sistema de Gestión Fiscal - SGF

Figura 1: Denuncias ingresadas por delitos informáticos, periodo 2022-2023

Fuente: *Fiscalía Provincial Penal Corporativa de Huamanga.*

La **Figura 01** presentada muestra la cantidad de denuncias ingresadas por delitos informáticos en las Fiscalías Provinciales Penales Corporativas de Huamanga durante los años 2022 y 2023. Teniendo como datos que, en el 2022 se registraron 127 denuncias por delitos informáticos, mientras que en 2023 la cifra aumentó a 198, lo que representa un crecimiento considerable en el periodo de estos dos años.

Tabla 1: ***Cantidad de casos archivados***

FISCALIA	DENUNCIAS INGRESADAS	ARCHIVADOS
1° FPPC HUAMANGA	28	26
2° FPPC HUAMANGA	37	34
3° FPPC HUAMANGA	39	37
4° FPPC HUAMANGA	20	20
5° FPPC HUAMANGA	35	34
6° FPPC HUAMANGA	39	38
TOTAL	198	189

La tabla 1 presenta un resumen de las denuncias ingresadas y los casos archivados en las diferentes Fiscalías Provinciales Penales Corporativas (FPPC) de Huamanga durante el año 2023. Los datos muestran que, de un total de 198 denuncias ingresadas, 189 casos fueron archivados, lo que representa una tasa de archivo exponencial. Este alto porcentaje de casos archivados sugiere que existen dificultades significativas en la investigación y persecución de los delitos de fraude informático en la región.

Tabla 2: ***Datos de la Ficha documental extraídas de las Disposiciones de Archivo de la Segunda Fiscalía Provincial Penal Corporativa de Huamanga.***

C.F	DENUNCIA	INVESTIGADO	RESULTADO
465-2023	De los actuados remitidos por la DIVINCRI de Ayacucho, se tiene que el día 23 de diciembre de 2022, al realizar una operación de retiro de dinero en un cajero automático de su cuenta de ahorros N° 04-093-633186 (Banco de la Nación), se dio con la sorpresa de que solo tenía un saldo de S/. 57.00 Soles. En ese momento, se apersonó a una ventanilla del Banco de la Nación, donde le informaron que	L.Q.R.R.	No procede formalizar y continuar con la investigación porque **No se ha individualizado al imputado**

	se habían realizado compras, retiros y compras por internet los días 13, 14, 15 y 18 de diciembre de 2022. El dinero sustraído asciende a la suma de S/. 1,100 soles aproximadamente, del cual la denunciante no tuvo conocimiento y que fueron realizados sin su consentimiento.		**Modalidad Carding**
328-2023	Conforme a la denuncia interpuesta por Karen Esthefany Tenorio Berrocal, el 12 de julio de 2022 a horas 13:30 aproximadamente, habrían hackeado su cuenta de "Facebook" haciéndose pasar por su persona para solicitar dinero a sus contactos de dicha red social, manifestando que su madre se encontraba mal de salud y que necesitaba dinero. En consecuencia, los amigos que recibieron ese mensaje depositaron la suma de S/. 420.00 soles al número de Yape 947875436, línea que se encuentra a nombre de Juan Dany Salcedo Chacnama. Posteriormente, la agraviada se percató del hecho y procedió a interponer la denuncia correspondiente.	L.Q.R.R.	La agraviada no fue a declarar **No se ha individualizado al imputado** **Phishing**
340-2023	Fluye de los actuados que, el día 30 de diciembre de 2022, circunstancias en que su teléfono celular había amanecido sin señal por la mañana, percatándose a las 09:00 horas aproximadamente, luego el denunciante pensó que se trataba de un fraude informático, motivo por el cual sacó la consulta de su cuenta de tarjeta de débito del Banco de la Nación, dándose con la sorpresa de que habían realizado nueve movimientos, llegando a extraer sus ahorros. Asimismo, el denunciante indica que fue a la empresa BITEL para averiguar sobre la señal de su teléfono, le indicaron que migró el 29 de diciembre de 2022, cuya migración no fue realizada por el agraviado.	L.Q.R.R.	El agraviado no fue a declarar **No se ha individualizado al imputado** **SIM Swapping**

341-2023	Fluye de los actuados remitidos por la comisaría de Ayacucho-DEPINCRI, que el agraviado habría sido víctima del delito contra el patrimonio en la modalidad de fraude informático, toda vez que el denunciante fue al Banco de la Nación a retirar dinero, se dio con la sorpresa de que su tarjeta de débito se encontraba suspendida. Luego, al consultar, le indicaron que la suspensión fue porque se realizaban movimientos seguidos desde el día 06 de diciembre hasta el día 15 de diciembre de 2022, llegando a realizar desembolsos, los mismos que no fueron realizados por el agraviado.	L.Q.R.R.	**No se ha individualizado al imputado** **Carding**
350-2023	El denunciante Arom Yoberty Luján Gutiérrez refiere que el 31 de diciembre del 2022, le llegó una notificación a su correo de su tarjeta de crédito "Visa" del Banco de la Nación, donde se le indica que realizó compras por internet a las 21:58 horas en la página "DID FOOD, GROUPPRAISE.COM" por un monto total de S/. 556.96 (quinientos cincuenta y seis con noventa y seis soles) realizados en seis operaciones, las cuales el agraviado desconoce y no fueron realizadas por él.	L.Q.R.R.	**No se ha individualizado al imputado** **Carding**
371-2023	Se tiene que el ciudadano Hipólito Daniel Flores Jiménez formuló su denuncia sobre la presunta comisión del delito de Fraude Informático, señalando que, el día 17 de julio del 2022 a las 08:23 horas aproximadamente, se acercó al cajero automático del B.C.P. para retirar dinero, empero su tarjeta fue rechazada. Por lo que dos personas de sexo masculino se acercaron a ofrecerle ayuda, es así que al ingresar la tarjeta nuevamente, esta se quedó atorada en el referido cajero y solo expulsó un voucher en el que señalaba “por favor acérquese a las oficinas de su banco”.	L.Q.R.R.	**El agraviado no fue a declarar** **Carding**

	Luego de lo cual, el agraviado se retiró del lugar, instantes en que observó mediante su banca móvil instalada en su equipo celular, se percató de que se habían realizado cuatro (04) operaciones de retiro por la suma total de S/5,140.34 soles, no obstante, dicha operación no la realizó él.		
442-2023	La denunciante señala que al introducir su tarjeta visualizó que en la pantalla se mostraba el mensaje “la cuenta no está autorizada”, por lo que se dirigió a la ventanilla del Banco donde se le informó que la cuenta estaba bloqueada por compras extrañas. Al solicitar su estado de cuenta, observó que los días 21 y 22 de diciembre del 2022 se habían realizado compras en un establecimiento de comida rápida por un valor de S/ 858.00 soles.	L.Q.R.R.	La agraviada no fue a declarar **No se ha individualizado al imputado** **Carding**
444-2023	Conforme a la denuncia presentada por Joel Luján Huaraca, se imputa a L.Q.R.R. ya que el denunciante habría sido víctima del delito contra el patrimonio en la modalidad de fraude informático, toda vez que el pasado 29 de diciembre del 2022 a las 14:00 horas aproximadamente, le llegó un mensaje a su correo personal *(JOELUJANH@GMAIL.COM)* sobre dos movimientos realizados de su cuenta de ahorros N°04415120155 del Banco de la Nación, y de su otra tarjeta de Visa Débito N°4214-1002-5521-0529, indicando que habían realizado dos movimientos de compras por internet, haciendo una suma de S/134.99 nuevos soles. Por lo que el denunciante acudió a las instalaciones de la comisaría PNP a interponer su denuncia.	L.Q.R.R.	**No se ha individualizado al imputado** **Phishing**
560-2023	La denunciante Yolanda Palomino Landa, el 10 de diciembre del 2022, refiere que se acercó al cajero central	L.Q.R.R.	**No se ha individualizado al imputado**

	de BCP para ingresar su tarjeta, obteniendo una respuesta negativa indicando que no tenía saldo suficiente. Al realizar su reclamo en la entidad BCP, el 02 de enero del 2023 le informaron que se habían realizado retiros en un cajero de otro banco, ubicado en la agencia Ayacucho, utilizando la tarjeta de número de cuenta BCP Nº 22073984955-077. Los retiros fueron los siguientes: el 09 de diciembre del 2022 a las 13:51 horas por la suma de S/. 700.00 soles; el 09 de diciembre del 2022 a las 13:52 horas por la suma de S/. 700.00 soles; el 09 de diciembre del 2022 a las 13:53 horas por la suma de S/. 700.00 soles; y el 09 de diciembre del 2022 a las 13:54 horas por la suma de S/. 700.00 soles, retirando un total de S/. 3,500.00 (tres mil quinientos soles). Ante esto, la denunciante presentó su denuncia ante la PNP.		**Carding**
967-2023	La denunciante Surama Ferrel Lizarma de Sauñe señala que, siendo aproximadamente las 17:46 horas del 10 de marzo de 2023, personas no identificadas realizaron una compra por el monto de S/ 158.60 soles por internet desde una página del Banco de la Nación de su cuenta N°4214100294978590, mediante el aplicativo “RAPPI”. Este hecho lo descubrió el día siguiente, 11 de marzo de 2023, cuando acudió a un agente ubicado por las inmediaciones del mercado Mariscal Cáceres con la finalidad de hacer un retiro de S/ 300.00 soles, dándose con la sorpresa de que no tenía saldo suficiente para realizar el retiro. Motivo por el cual, el día 28 de marzo de 2023, acudió al Banco de la Nación, donde le indicaron que posiblemente había sido víctima de clonación de tarjeta, razón por la cual se apersonó a interponer su denuncia.	L.Q.R.R.	**No se ha individualizado al imputado** **Thief Transfer**

979-2023	Conforme se tiene de los actuados, el ciudadano Luis Miguel Huamani Morales señaló que el día 21 de marzo del 2023 en horas de la noche, recibió un mensaje de su amigo Roy Enrique Jáuregui Cano, quien le envió el link https://facebook.comln.xyz/57388wOTM0NzE3ODEw, indicándole que ingresara a dicha dirección y le enviara la foto de la persona que aparecía. Motivo por el cual ingresó a dicho link, que lo dirigió a una página de Google y seguidamente a un perfil de Facebook registrado a nombre de Daniela Álvarez Rodríguez. Asimismo, el día 22 de marzo del 2023 a las 12:00 horas aproximadamente, recibió una llamada telefónica del número de celular 927 039 787, que pertenece a su amigo Cristian Jimy Tineo Tineo, quien le preguntó "¿para qué necesitas dinero?", a lo cual respondió "yo no necesito dinero". Enseguida, su amigo le indicó que recibió un mensaje desde su perfil de Messenger pidiendo dinero, por lo que, de inmediato, procedió a revisar sus mensajes de Messenger y se percató de que había seis (06) chats archivados con las cuentas Frederick, Juanse, Pariona, María, Deivy, Henry, de cuyas personas se desconocen sus apellidos y a quienes se les escribía solicitando dinero. De dichas personas, realizaron el depósito: Deivy Miguel Vargas, celular 934 589 055, por el monto de S/ 100 soles, y Fredy, de quien se desconocen sus apellidos, celular 946 314 371, por el monto de S/ 10.00 soles, a la persona de Elizabeth Margot Pawelczyk Gómez, mediante el aplicativo "YAPE".	L.Q.R.R.	**No se ha individualizado al imputado** **Phishing**

1371-2023	La denuncia realizada por Richard Jhony Fernández Vizarreta. Según su relato, el 13 de junio de 2023, alrededor de las 11:00 horas, estaba almorzando en el local llamado "TRADICIÓN" en el Barrio de Andamarca. Después de pagar su consumo, a las 16:48 horas, recibió un mensaje de texto en su número telefónico 948153373 indicando que una compra en línea en PYU'Adidas por S/1,875.00 soles no se había procesado debido a falta de saldo. Al desconocer esta operación, se comunicó con el Banco Interbank para verificar su cuenta de ahorro y descubrió que se habían realizado una compra por S/1,019.00 soles y cuatro pagos por consumo de S/190.00 soles cada uno a nombre de "CLUB 55", sumando un total de S/1,779.00 soles. Este hecho fue denunciado para su investigación correspondiente.	L.Q.R.R.	**No se ha individualizado al imputado** **Thief Transfer**
1554-2023	Los hechos investigados relacionados con el agraviado César Godofredo Vallejo Cuya. El 11 de junio de 2023, alrededor de las 20:00 horas, revisó su banca móvil y notó que se había realizado una compra no reconocida por él, por un monto de S/. 588.49 soles. No pudo bloquear su cuenta en ese momento debido a que se encontraba de viaje. Posteriormente, el 21 de junio de 2023, se percató de otra compra no reconocida, esta vez por un monto de S/. 218.56 soles. El agraviado desconoce las compras realizadas y a los responsables de las mismas. Estos hechos fueron investigados para determinar lo ocurrido.	L.Q.R.R.	**No se ha individualizado al imputado** **Thief Transfer**
1565-2023	Los hechos denunciados por Diego Edgar Hurtado Gonzales. El 18 de junio de 2023, alrededor de las 18:20 horas, mientras revisaba su correo Gmail, se percató de que se habían realizado varias transferencias desde su	L.Q.R.R.	**No se ha individualizado al imputado** **Carding**

	tarjeta Interbank a través del aplicativo PLIN. Estas transferencias, por un monto total de S/. 771.00 soles, fueron dirigidas a una cuenta YAPE a nombre de Alicia Esmeralda Salazar Laynes. Hurtado Gonzales asegura que no realizó dichas transferencias, por lo que procedió a bloquear su cuenta para evitar más transacciones no autorizadas. Este incidente fue denunciado para su investigación correspondiente.		
1627-2023	Los hechos investigados en relación con la denuncia presentada por Wilber Flores Huamán. El 11 de agosto de 2023, recibió una transferencia de S/ 70,000.00 soles por la venta de su carro, la cual se depositó en su cuenta N° 440-337963088 del Banco Interbank. Ese mismo día, retiró S/. 20,000.00 soles, dejando un saldo de S/. 50,000.00 soles. Sin embargo, el 15 de agosto de 2023, al revisar su cuenta, se le informó que su saldo era de S/. 43,000.00 soles, debido a retiros no autorizados realizados los días 12, 13 y 14 de agosto por montos de S/. 1,036.50, S/. 1,726.50, S/. 1,726.50 y S/. 634.20 soles, respectivamente. Flores Huamán presentó un reclamo ante INDECOPI y, el 8 de septiembre de 2023, acudió al Banco Interbank, donde le informaron que no le devolverían su dinero y que debía presentar una denuncia, ya que los movimientos se realizaron utilizando el correo electrónico giovanidelacruz2023@outlook.com. Además, precisó que no utilizó ningún aplicativo electrónico, no compartió información con nadie, no prestó su tarjeta y solo informó a su hijo, Noé Flores Ventura, de 30 años, sobre el dinero	L.Q.R.R.	**No se ha individualizado al imputado** **Phishing**

	en su cuenta. Estos hechos fueron investigados para determinar lo ocurrido.		
2003-2023	Los hechos denunciados por Walter Gotardo Infante Vivanco. El 16 de septiembre de 2023, alrededor de las 07:00 horas, se dirigió a un cajero automático del Banco de la Nación en la Av. Independencia para realizar un retiro de su cuenta de ahorro. Al llegar, notó que un sujeto desconocido merodeaba el cajero. Al intentar retirar dinero, el cajero no le permitió realizar la operación. Solicitó ayuda al sujeto para expulsar su tarjeta, quien le indicó que limpiaría el chip de la tarjeta en su camisa antes de devolvérsela. Posteriormente, Infante Vivanco intentó usar otro cajero, pero el sistema no aceptó su tarjeta y la retuvo. Acudió al Banco de la Nación para anular y cambiar su clave, recibiendo una nueva tarjeta. Al solicitar un retiro, le informaron que no tenía saldo suficiente. Al revisar sus movimientos, observó en un baucher que se habían realizado varias compras en diferentes establecimientos comerciales por un monto aproximado de S/ 8,000.00 soles, a pesar de que él aseguraba tener un saldo de aproximadamente S/ 10,000.00 soles. Estos hechos fueron denunciados para su investigación.	L.Q.R.R.	**No se ha individualizado al imputado** **Carding**
2024-2023	El 15 de setiembre a horas 8:30 el agraviado recibió una llamada telefónica de un número desconocido (974 037 439). Al contestar, una persona que se identificó como José Armando Curo Chaves, con DNI 71142513, afirmó ser empleado del Banco Pichincha y ofreció un préstamo de S/.10,000.00 soles con un interés del 8.65%. El agraviado accedió a solicitar un préstamo de S/.5,000.00	L.Q.R.R.	**No se ha individualizado al imputado** **Phishing**

	soles y proporcionó información solicitada, como sus boletas de pago, número de DNI y número de cuenta interbancaria del Banco Interbank. Al no tener su número de CCI (Código de Cuenta Interbancario), el agraviado ingresó a su aplicación móvil para obtenerlo. En ese momento, recibió un correo electrónico informándole sobre una transferencia interbancaria. Al revisar su aplicación, descubrió que su cuenta estaba vacía y que se habían retirado S/.5,385.49 soles. Reclamó a la persona que lo llamó, quien le dijo que era común y que probablemente el Banco Interbank había retenido su dinero. Ante esto, el agraviado decidió presentar una denuncia ante la policía.		
2068-2023	El 12 de setiembre de 2023, el agraviado recibió una llamada de un número (946 400 1132) de una persona que afirmó ser trabajadora del banco "Pichincha" en Lima. Esta persona le ofreció un préstamo de S/.1,000.00 soles. Al aceptar, le solicitaron ciertos requisitos, que el agraviado envió a través de WhatsApp al número 946 400 132. Los requisitos incluían una fotocopia de su DNI y un recibo de agua. Después de enviar los documentos, le informaron que había cumplido con todos los requisitos y que debía recoger el dinero en la Av. Mariscal Cáceres N°905, donde también tendría que firmar algunos documentos. El 15 de septiembre, al verificar su estado de cuenta en el BCP, el agraviado notó que se había depositado un monto de S/.4,605.00 soles, supuestamente por la empresa constructora "JB". Este hecho fue denunciado para su investigación.	L.Q.R.R.	**No se ha individualizado al imputado** **Phishing**

2093-2023	El hecho denunciado por Reider Huacce Prado. El 3 de septiembre de 2023, alrededor de las 23:00 horas, perdió su tarjeta de crédito del Banco de Crédito (BCP) mientras se encontraba en las inmediaciones del Jr. Asamblea con la Av. Mariscal Cáceres. El 14 de septiembre de 2023, personal del banco le notificó a través de su correo electrónico sobre compras no reconocidas realizadas en distintas licorerías y establecimientos por un monto total de S/ 8,300.00 soles. Ante esta situación, Huacce Prado acudió a la delegación policial para presentar su denuncia. Este hecho fue registrado en la Denuncia Directa N° 703.	L.Q.R.R.	**No se ha individualizado al imputado** **Carding**
150-2023	Los hechos denunciados por una persona cuyo número de celular es 966121920. El 27 de diciembre de 2022, a las 13:10 horas, recibió un mensaje de texto indicando que se había registrado un cambio de SIM card en una tienda Movistar. El mensaje sugería que, si no reconocía el cambio, solicitara un bloqueo al 104. Inmediatamente después de recibir el mensaje, el denunciante llamó al 104, donde un especialista verificó el mensaje y le informó que había un problema en el sistema y que no debía preocuparse. El 18 de diciembre de 2022, el denunciante se percató de que no tenía servicio de celular para realizar o recibir llamadas. Volvió a contactar al 104 varias veces sin obtener una solución. Finalmente, alrededor de las 16:00 horas, llamó nuevamente al 104 y le indicaron que podría ser un problema con el chip y que debía acudir a una agencia telefónica en Ayacucho. Sin embargo, no encontró ninguna agencia disponible en la ciudad. El 28 de diciembre, a las 17:00 horas, la operadora del 104 continuó	L.Q.R.R.	**No se ha individualizado al imputado** **SIM Swapping**

brindando asistencia. Este incidente fue denunciado para su investigación y resolución.

Después de recibir un mensaje sobre un cambio no autorizado de SIM card, el denunciante solicitó la suspensión de su línea telefónica con la orden 1059817935. Posteriormente, al intentar usar un cajero automático del Banco de la Nación, descubrió que su tarjeta estaba bloqueada.

El 29 de diciembre de 2022, acudió a la agencia central del Banco de la Nación en el Jr. 28 de julio, donde le informaron que la tarjeta había sido bloqueada por fraude y le proporcionaron un código (625554) para anular la línea telefónica. Ese mismo día, solicitó la anulación de su línea telefónica, recibiendo el código de baja 1060451527ª.

El 30 de diciembre, el denunciante regresó al Banco de la Nación para solicitar el desbloqueo de su tarjeta. Después de verificar su identidad, se desbloqueó la tarjeta y se le entregó una nueva. Al revisar su cuenta, se percató de que solo quedaba un saldo de S/. 3,477.52 y que se habían realizado movimientos no reconocidos, incluyendo retiros y transferencias en nueve oportunidades entre el 27 y el 28 de diciembre de 2022. El banco le sugirió presentar una denuncia o reclamo en el área administrativa para investigar los movimientos no autorizados. Finalmente, el denunciante retiró todo el dinero restante de su cuenta.

***Tabla 3**: Cantidad del 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 **Tabla 3** muestra la distribución del personal policial especializado en delitos de fraude informático en Huamanga. Contando con solo **7** policías de investigación en total, se evidencia de esta manera una limitada capacidad para enfrentar estos ciberdelitos, que se detalla de la siguiente manera:

- **Delitos contra el Patrimonio** concentra el mayor número de especialistas (3 policías, 42.9%), reflejando de esta forma un enfoque prioritario en fraudes económicos.
- **Delitos contra la Intimidad y Comunicaciones** tiene 2 policías de investigación (28.6%), indicando de este modo, atención moderada a violaciones de privacidad.
- **Investigación de Alta Tecnología** y **Ciberseguridad** cuentan con solo 1 policía de investigación cada uno (14.3%), lo que sugiere una falta de recursos para abordar ciberataques complejos y prevenir amenazas digitales.

Esto pone de manifiesto la limitada disponibilidad de efectivos policiales especializados, especialmente en sectores clave como la ciberseguridad y las tecnologías avanzadas, lo cual constituye un obstáculo relevante para el desarrollo de investigaciones y la prevención eficaz de delitos informáticos en la región. Esta carencia podría ser uno de los factores que contribuyen a la elevada proporción de casos archivados, como se observa en la Tabla 1.

***Tabla 4:** Modalidad de Fraude Informático identificadas en las Carpetas Fiscales*

MODALIDAD DE FRAUDE INFORMÁTICO IDENTIFICADAS EN LAS CARPETAS FISCALES	CANTIDAD
PHISHING	6
CARDING	8
SIM SWAPPING	2
THIEF TRANSFER	4
TOTAL	**20**

La **Tabla 4** presenta las modalidades de fraude informático identificadas en las Carpetas Fiscales, con un total de **20 casos** registrados. A continuación, se analizan las tendencias y su relevancia:

Carding: Con **8 casos** (40%), es la modalidad más frecuente. Esto refleja un alto nivel de fraude relacionado con el uso no autorizado de tarjetas de crédito o débito, lo que sugiere la necesidad de fortalecer los sistemas de seguridad en transacciones financieras. **Phishing**: Con **6 casos** (30%), es la segunda modalidad más común. Esto indica que los delincuentes están utilizando técnicas de ingeniería social para obtener información confidencial de las víctimas, como contraseñas o datos bancarios. Es crucial implementar campañas de concienciación para prevenir este tipo de ataques. **Thief Transfer**: Con **4 casos** (20%), esta modalidad representa un problema significativo en transferencias fraudulentas de fondos. Esto podría estar relacionado con la falta de controles de seguridad en las operaciones bancarias en línea. **SIM Swapping**: Con solo **2 casos** (10%), es la modalidad menos frecuente. Sin embargo, su impacto puede ser severo, ya que permite a los delincuentes tomar control de líneas telefónicas para acceder a cuentas bancarias y otros servicios, aunque es menos común, no debe subestimarse. De esta forma se aprecia que, el **carding** y el **phishing** son las modalidades predominantes, lo que subraya la

importancia de mejorar la seguridad en transacciones financieras y la educación en ciberseguridad. La presencia de **thief transfer** y **SIM swapping**, aunque en menor medida, también requiere atención para prevenir futuros incidentes.

Resultado del Cuestionario

Tabla 5: ¿La falta de recursos tecnológicos (software de análisis forense, herramientas de rastreo) dificulta la individualización de los ciberdelincuentes?

Recuento

		¿La falta de recursos tecnológicos (software de análisis forense, herramientas de rastreo) dificulta la individualización de los ciberdelincuentes?			
		Algunas veces	Casi siempre	Siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	1	7	1	9
	Abogado	1	9	1	11
Total		2	16	2	20

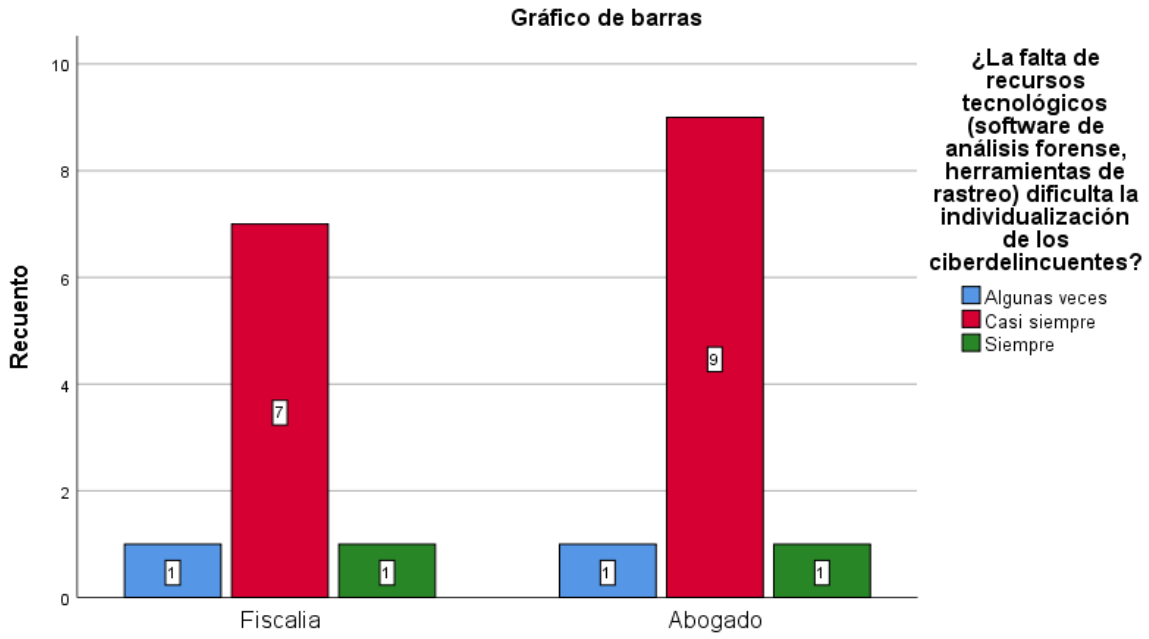

Figura 2: ¿La falta de recursos tecnológicos (software de análisis forense, herramientas de rastreo) dificulta la individualización de los ciberdelincuentes?

La **Tabla 5** y la **Figura 2** analizan si la falta de recursos tecnológicos, como software de análisis forense y herramientas de rastreo, dificulta la individualización de los ciberdelincuentes. Los resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**.

Casi siempre (16 respuestas, 80%): La mayoría de los encuestados, tanto fiscales como abogados, consideran que la falta de recursos tecnológicos **casi siempre** dificulta la identificación de los ciberdelincuentes. Esto refleja una percepción generalizada de que la carencia de herramientas especializadas es un obstáculo significativo en la investigación respecto a delitos de fraude informático. **Algunas veces (2 respuestas, 10%)**: Un pequeño porcentaje de los encuestados cree que la falta de recursos tecnológicos **solo algunas veces** dificulta la individualización de los ciberdelincuentes. Esto podría indicar que, en ciertos casos, otros factores (como la capacitación del personal o la colaboración interinstitucional) pueden compensar parcialmente la falta de tecnología. **Siempre (2 respuestas, 10%)**: Un número reducido de encuestados considera que la falta de recursos tecnológicos **siempre** es un impedimento para identificar a los ciberdelincuentes.

***Tabla 6:** ¿El personal de la fiscalía carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva?*

Recuento

		¿El personal de la fiscalía carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva?		
		Algunas veces	Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	1	8	9
	Abogado	1	10	11
Total		2	18	20

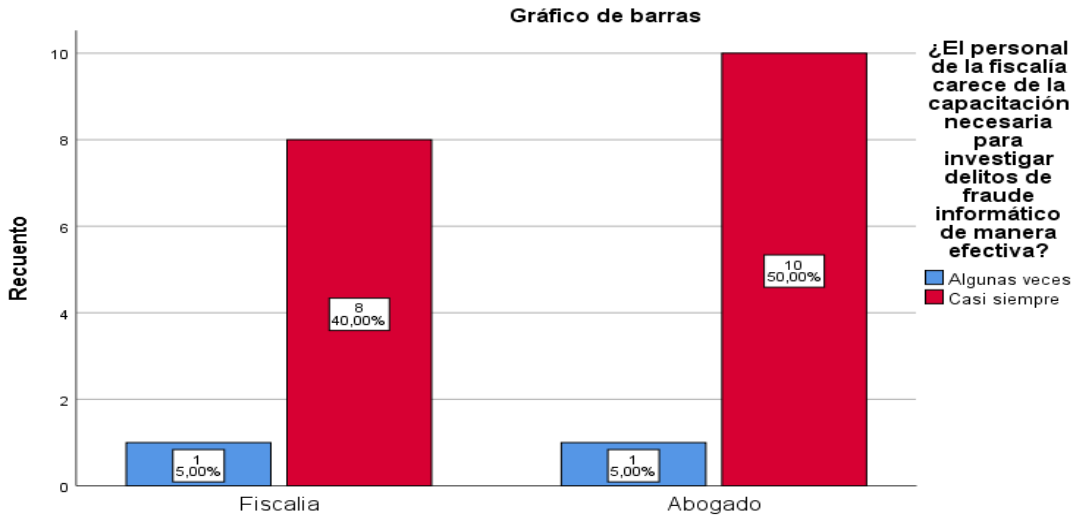

Figura 3: ¿El personal de la fiscalía carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva?

La **Tabla 6** y la **Figura 3** examinan si el personal de la fiscalía carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva. Los

resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**.

Casi siempre (18 respuestas, 90%): La gran mayoría de los encuestados, tanto fiscales como abogados, consideran que el personal de la fiscalía **casi siempre** carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva. Esto indica una percepción generalizada de que la falta de formación especializada es un problema recurrente que dificulta la investigación de estos delitos. **Algunas veces (2 respuestas, 10%)**: Un pequeño porcentaje de los encuestados cree que la falta de capacitación **solo algunas veces** es un problema. Esto podría sugerir que, en ciertos casos, el personal cuenta con algún nivel de formación o que otros factores (como la experiencia práctica) pueden compensar parcialmente esta carencia. Existe una **percepción mayoritaria** de que el personal de la fiscalía no está suficientemente capacitado para investigar delitos de fraude informático de manera efectiva.

Tabla 7: ¿Los métodos utilizados por los ciberdelincuentes (anonimato, cifrado, criptomonedas) hacen casi imposible su identificación?

Recuento

		¿Los métodos utilizados por los ciberdelincuentes (anonimato, cifrado, criptomonedas) hacen casi imposible su identificación?		
		Algunas veces	Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	2	7	9
	Abogado	2	9	11
Total		4	16	20

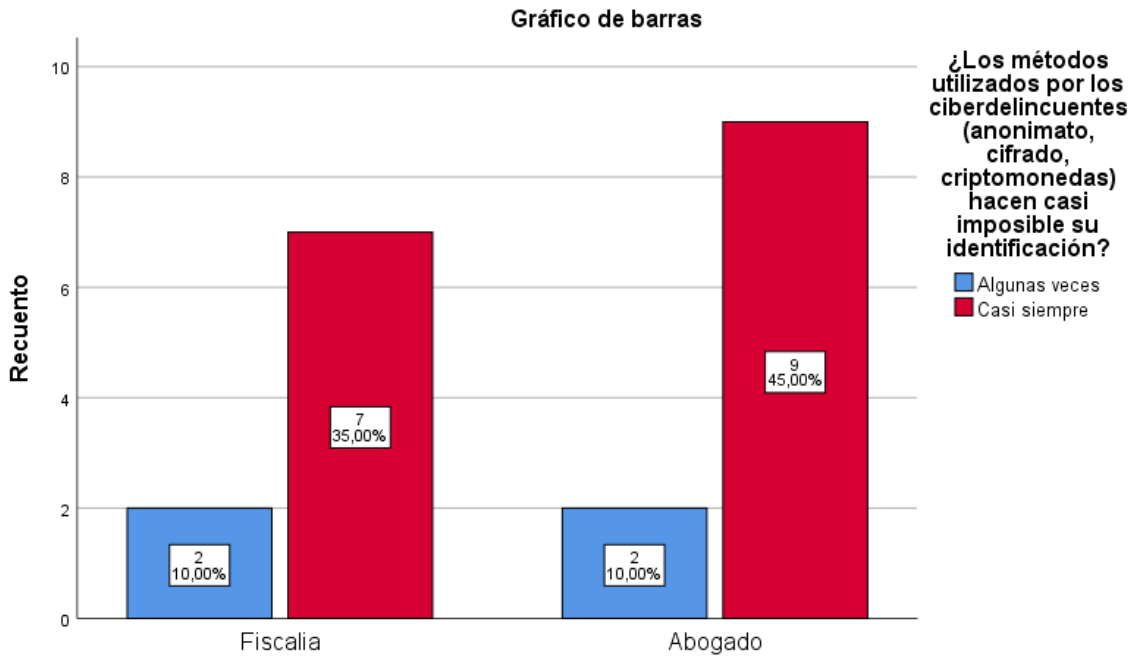

Figura 4: ¿Los métodos utilizados por los ciberdelincuentes (anonimato, cifrado, criptomonedas) hacen casi imposible su identificación?

La **Tabla 7** y la **Figura 4** analizan si los métodos utilizados por los ciberdelincuentes, como el anonimato, el cifrado y el uso de criptomonedas, hacen casi imposible su identificación. Los resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**. **Casi siempre (16 respuestas, 80%)**: La mayoría de los encuestados, tanto fiscales como abogados, consideran que los métodos utilizados por los ciberdelincuentes **casi siempre** dificultan su identificación. Esto refleja una percepción generalizada de que las técnicas avanzadas de ocultamiento, como el cifrado y el uso de criptomonedas, representan un desafío significativo para las investigaciones. **Algunas veces (4 respuestas, 20%)**: Un porcentaje menor de los encuestados cree que estos métodos **solo algunas veces** complican la identificación de los delincuentes. Existe una **percepción mayoritaria** de que los métodos utilizados por los ciberdelincuentes, como el anonimato, el cifrado y las criptomonedas, hacen dificultoso su identificación.

Tabla 8: ¿La falta de cooperación interinstitucional (con policía, empresas tecnológicas, etc.) afecta negativamente la investigación de estos delitos?

Recuento

		¿La falta de cooperación interinstitucional (con policía, empresas tecnológicas, etc.) afecta negativamente la investigación de estos delitos?		
		Algunas veces	Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	2	7	9
	Abogado	2	9	11
Total		4	16	20

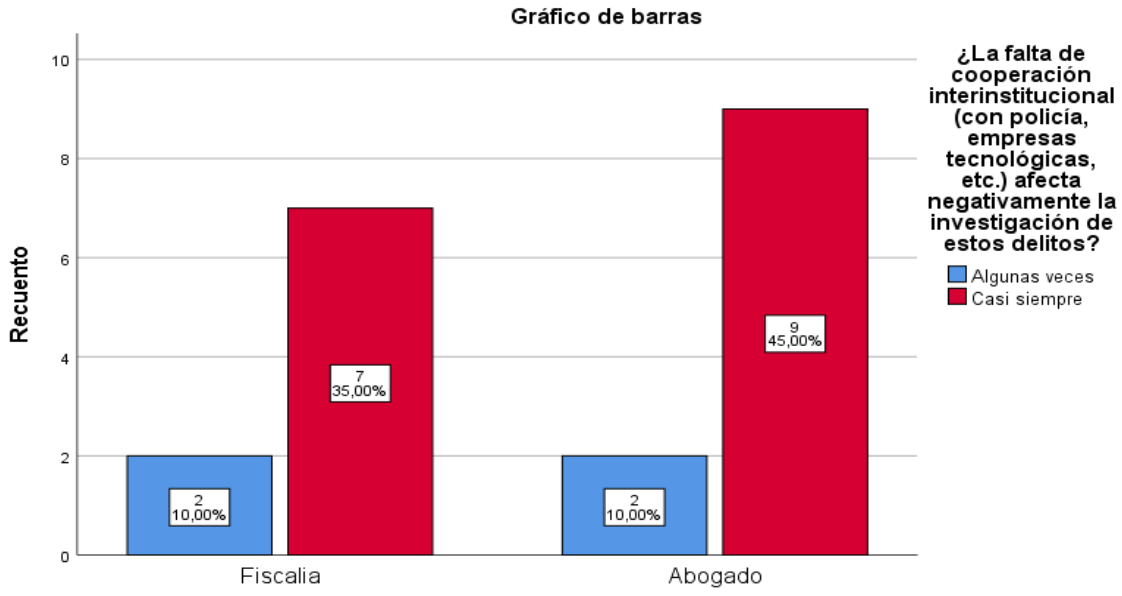

Figura 5: ¿La falta de cooperación interinstitucional (con policía, empresas tecnológicas, etc.) afecta negativamente la investigación de estos delitos?

La **Tabla 8** y la **Figura 5** analizan si la falta de cooperación interinstitucional (con la policía, empresas tecnológicas, etc.) afectan negativamente la investigación de los delitos de fraude informático. Los resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**. **Casi siempre (16 respuestas, 80%)**: La mayoría de los encuestados, tanto fiscales como abogados, consideran que la falta de cooperación interinstitucional **casi siempre** afecta negativamente la investigación de estos delitos. Esto indica una percepción generalizada de que la falta de colaboración entre instituciones es un obstáculo significativo para la efectividad de las investigaciones. **Algunas veces (4 respuestas, 20%)**: Un porcentaje menor de los encuestados cree que la falta de cooperación **solo algunas veces** tiene un impacto negativo. Esto podría sugerir que, en ciertos casos, se logra establecer algún nivel de colaboración, aunque no de manera consistente o suficiente. Existe una **percepción mayoritaria** de que la falta de cooperación interinstitucional afecta negativamente la investigación de los delitos de fraude informático.

Tabla 9: ¿La mayoría de los casos de fraude informático se archivan debido a la imposibilidad de identificar a los responsables?

Recuento

		¿La mayoría de los casos de fraude informático se archivan debido a la imposibilidad de identificar a los responsables?		
		Algunas veces	Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	2	7	9
	Abogado	2	9	11
Total		4	16	20

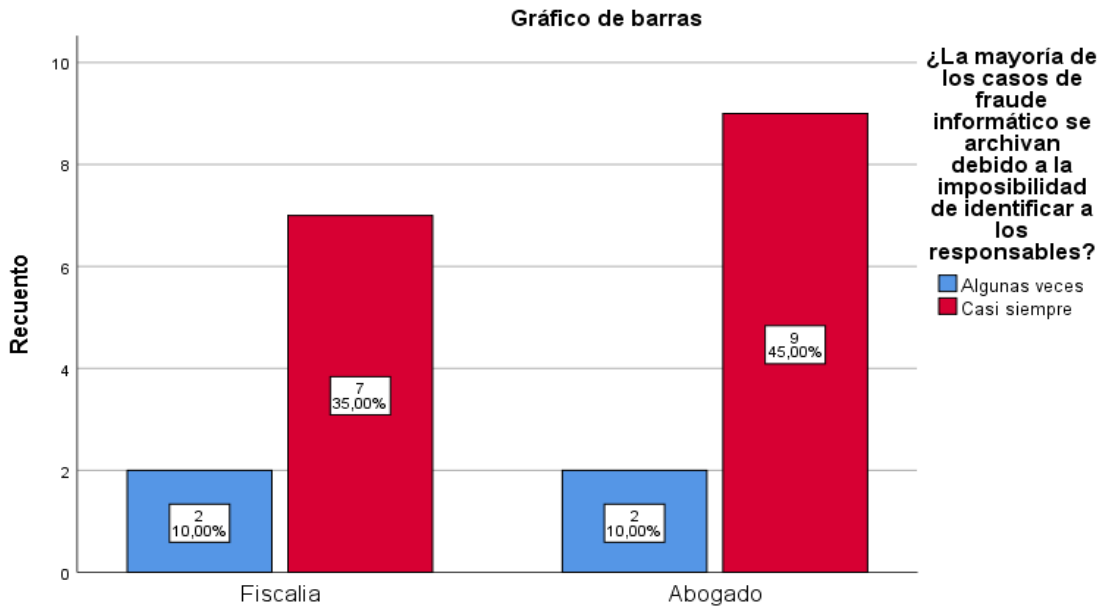

Figura 6: ¿La mayoría de los casos de fraude informático se archivan debido a la imposibilidad de identificar a los responsables?

La **Tabla 9** y la **Figura 6** evalúan si la mayoría de los casos de fraude informático se archivan debido a la imposibilidad de identificar a los responsables. Los resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**. **Casi siempre (16 respuestas, 80%)**: La mayoría de los encuestados, tanto fiscales como abogados, consideran que **casi siempre** los casos de fraude informático se archivan debido a la imposibilidad de identificar a los responsables. Esto refleja una percepción generalizada de que la dificultad para rastrear y atribuir responsabilidades a los ciberdelincuentes es un factor clave en el archivo de estos casos. **Algunas veces (4 respuestas, 20%)**: Un porcentaje menor de los encuestados cree que esta situación ocurre **solo algunas veces**. Esto podría indicar que, en ciertos casos, se logra identificar a los responsables, aunque no de manera consistente o suficiente. Existe una **percepción mayoritaria** de que la mayoría de los casos de fraude informático se archivan debido a la imposibilidad de identificar a los responsables.

Tabla 10: ¿La fiscalía no cuenta con herramientas tecnológicas avanzadas para rastrear transacciones fraudulentas?

Recuento

		¿La fiscalía no cuenta con herramientas tecnológicas avanzadas para rastrear transacciones fraudulentas?		
		Algunas veces	Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	2	7	9
	Abogado	2	9	11
Total		4	16	20

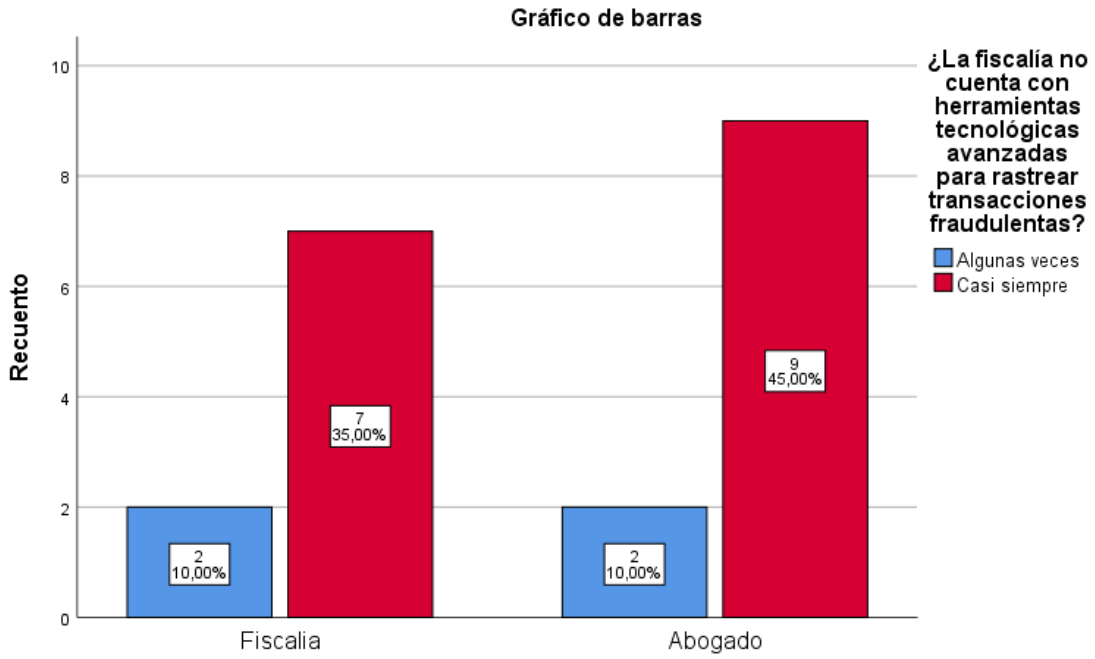

Figura 7: ¿La fiscalía no cuenta con herramientas tecnológicas avanzadas para rastrear transacciones fraudulentas?

La **Tabla 10** y la **Figura 7** analizan si la fiscalía cuenta con herramientas tecnológicas avanzadas para rastrear transacciones fraudulentas. Los resultados se basan

en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**.

Casi siempre (16 respuestas, 80%): La mayoría de los encuestados, tanto fiscales como abogados, consideran que **casi siempre** la fiscalía no cuenta con herramientas tecnológicas avanzadas para rastrear transacciones fraudulentas. Esto indica una percepción generalizada de que la falta de recursos tecnológicos es un obstáculo significativo para la investigación efectiva de estos delitos. **Algunas veces (4 respuestas, 20%)**: Un porcentaje menor de los encuestados cree que esta situación ocurre **solo algunas veces**. Esto podría sugerir que, en ciertos casos, la fiscalía tiene acceso a algunas herramientas, aunque no de manera eficiente. Existe una **percepción mayoritaria** de que la fiscalía no cuenta con herramientas tecnológicas avanzadas para rastrear transacciones fraudulentas.

Tabla 11: ¿El personal de la fiscalía no recibe capacitación constante en técnicas de investigación digital?

Recuento

		¿El personal de la fiscalía no recibe capacitación constante en técnicas de investigación digital?	
		Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	9	9
	Abogado	11	11
Total		20	20

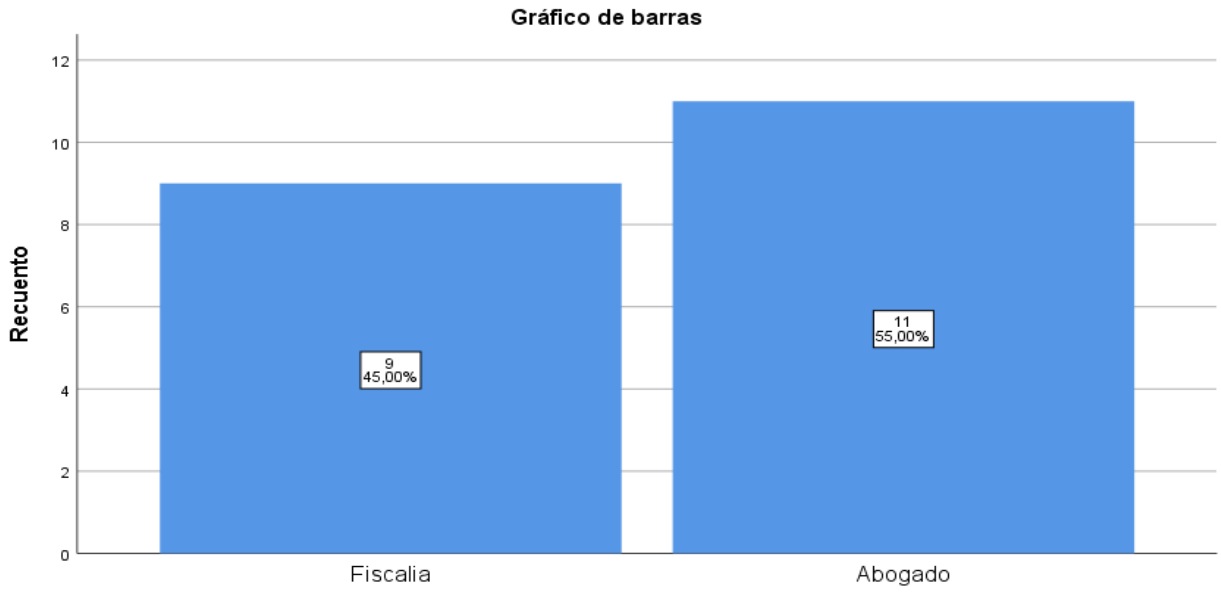

Figura 8: ¿El personal de la fiscalía no recibe capacitación constante en técnicas de investigación digital?

La **Tabla 11** y la **Figura 8** examinan si el personal de la fiscalía recibe capacitación constante en técnicas de investigación digital. Los resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**.

Casi siempre (20 respuestas, 100%): Todos los encuestados, tanto fiscales como abogados, consideran que **casi siempre** el personal de la fiscalía no recibe capacitación constante en técnicas de investigación digital. Esto indica una percepción unánime de que la falta de formación contínua es un problema grave que afecta la capacidad del personal para investigar delitos de fraude informático de manera efectiva. Existe una **percepción unánime** de que el personal de la fiscalía no recibe capacitación constante en técnicas de investigación digital.

Tabla 12: ¿La falta de elementos de convicción (transacciones no rastreables, ausencia de testigos) es la principal razón por la que los casos se archivan?

Recuento

		¿La falta de elementos de convicción (transacciones no rastreables, ausencia de testigos) es la principal razón por la que los casos se archivan?		
		Algunas veces	Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	2	7	9
	Abogado	2	9	11
Total		4	16	20

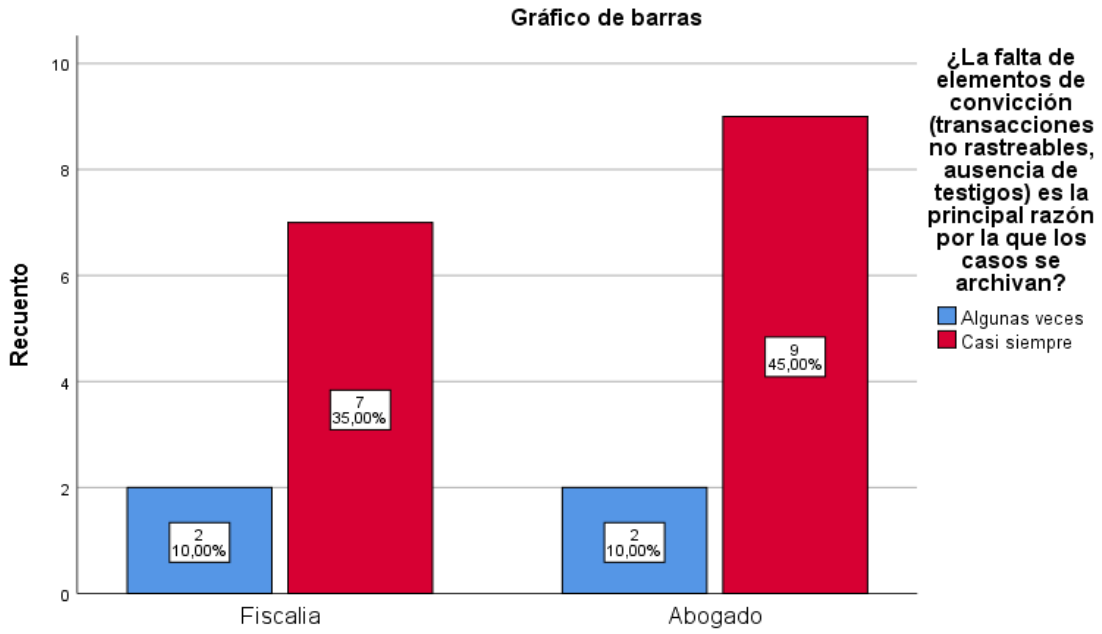

Figura 9: ¿La falta de elementos de convicción (transacciones no rastreables, ausencia de testigos) es la principal razón por la que los casos se archivan?

La **Tabla 12** y la **Figura 9** analizan si la falta de elementos de convicción, como transacciones no rastreables y la ausencia de testigos, es la principal razón por la que los casos de fraude informático se archivan. Los resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**.

Casi siempre (16 respuestas, 80%): La mayoría de los encuestados, tanto fiscales como abogados, consideran que **casi siempre** la falta de elementos de convicción es la principal razón por la que los casos se archivan. Esto refleja una percepción generalizada de que la dificultad para obtener pruebas sólidas, como transacciones rastreables o testimonios, es un obstáculo clave en la resolución de estos casos. **Algunas veces (4 respuestas, 20%)**: Un porcentaje menor de los encuestados cree que esta situación ocurre **solo algunas veces**. Esto podría indicar que, en ciertos casos, se logran reunir suficientes elementos de convicción, aunque no de manera firme. Existe una **percepción mayoritaria** de que la falta de elementos de convicción, como transacciones no rastreables y la ausencia de testigos, es la principal razón por la que los casos de fraude informático se archivan.

Tabla 13: ¿La dificultad para identificar a los responsables (anonimato, uso de tecnologías avanzadas) lleva al archivo de la mayoría de los casos?

Recuento

		¿La dificultad para identificar a los responsables (anonimato, uso de tecnologías avanzadas) lleva al archivo de la mayoría de los casos?		
		Algunas veces	Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	2	7	9
	Abogado	2	9	11
Total		4	16	20

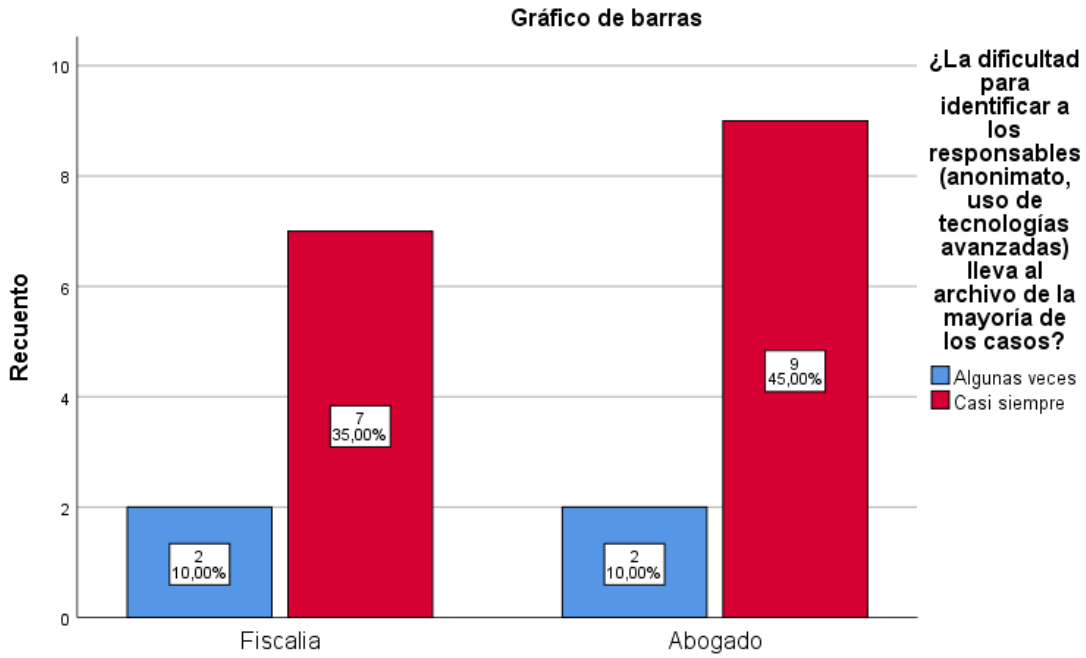

Figura 10: ¿La dificultad para identificar a los responsables (anonimato, uso de tecnologías avanzadas) lleva al archivo de la mayoría de los casos?

La **Tabla 13** y la **Figura 10** analizan si la dificultad para identificar a los responsables, debido al anonimato y el uso de tecnologías avanzadas, lleva al archivo de la mayoría de los casos de fraude informático. Los resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**. **Casi siempre (16 respuestas, 80%)**: La mayoría de los encuestados, tanto fiscales como abogados, consideran que **casi siempre** la dificultad para identificar a los responsables lleva al archivo de la mayoría de los casos. Esto refleja una percepción generalizada de que las técnicas de ocultamiento utilizadas por los ciberdelincuentes, como el anonimato y el uso de tecnologías avanzadas, representan un desafío significativo para las

investigaciones. **Algunas veces (4 respuestas, 20%)**: Un porcentaje menor de los encuestados cree que esta situación ocurre **solo algunas veces**. Esto podría indicar que, en ciertos casos, se logra identificar a los responsables, aunque no de manera estable. Existe una **percepción mayoritaria** de que la dificultad para identificar a los responsables, debido al anonimato y el uso de tecnologías avanzadas, lleva al archivo de la mayoría de los casos de fraude informático.

Tabla 14: ¿El archivo de casos de fraude informático genera impunidad?

		¿El archivo de casos de fraude informático genera impunidad?		
		Algunas veces	Casi siempre	Total
Lugar de trabajo de los encuestados	Fiscalía	1	8	9
	Abogado	1	10	11
Total		2	18	20

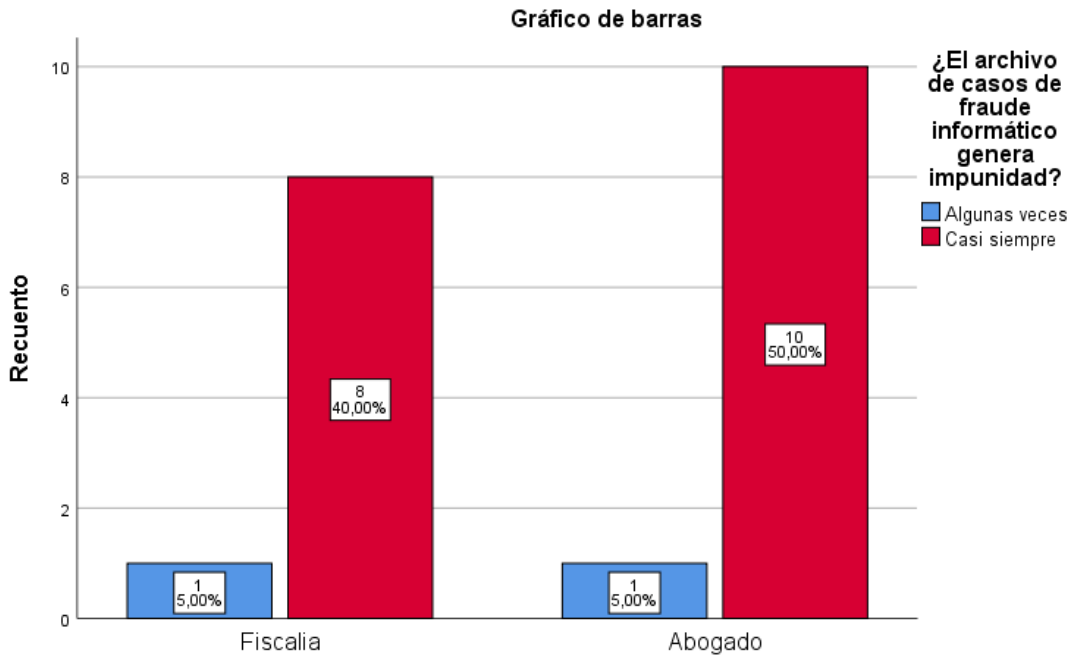

Figura 11: ¿El archivo de casos de fraude informático genera impunidad?

La **Tabla 14** y la **Figura 11** examinan si el archivo de casos de fraude informático genera impunidad. Los resultados se basan en las respuestas de encuestados de dos grupos: fiscales y abogados, con un total de **20 respuestas**. **Casi siempre (18 respuestas, 90%)**: La gran mayoría de los encuestados, tanto fiscales como abogados, consideran que **casi siempre** el archivo de casos de fraude informático genera impunidad. Esto refleja una percepción generalizada de que la falta de resolución de estos casos permite que los delincuentes actúen sin consecuencias, lo que perdura el ciclo de delitos. **Algunas veces (2 respuestas, 10%)**: Un pequeño porcentaje de los encuestados cree que esta situación ocurre **solo algunas veces**. Esto podría indicar que, en ciertos casos, se logra llevar a cabo investigaciones efectivas que evitan la impunidad, aunque no de manera consistente. Existe una **percepción mayoritaria** de que el archivo de casos de fraude informático genera impunidad.

5.2. Discusión de resultados

De esta manera se evidencia que las dificultades en la individualización de los ciberdelincuentes son un factor determinante en el archivo de los casos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023. Los datos muestran que el 80% de los encuestados considera que la falta de herramientas tecnológicas avanzadas, como software de análisis forense y sistemas de rastreo, dificulta la identificación de los responsables. Además, el uso de técnicas de ocultamiento por parte de los delincuentes, como el anonimato, el cifrado y las criptomonedas, hace casi imposible su identificación en la mayoría de los casos (80% de los encuestados). **Esto se refleja en que el 80% de los casos se archivan debido a la imposibilidad de individualizar a los responsables,** lo que a su vez genera impunidad en el 90% de los casos, según la percepción de los encuestados.

Otro aspecto crítico es la **falta de capacitación del personal** de la fiscalía, ya que el 90% de los encuestados señala que no se cuenta con la formación necesaria para investigar estos delitos de manera efectiva. A esto se suma la **falta de cooperación interinstitucional**, que según el 80% de los encuestados, afecta negativamente las investigaciones al limitar el acceso a información y recursos clave. En conjunto, estos factores, que son la falta de herramientas tecnológicas, métodos de ocultamiento, falta de capacitación y cooperación, crean un escenario en el que la individualización de los ciberdelincuentes se vuelve extremadamente difícil, lo que conduce al archivo de la mayoría de los casos y, en última instancia, a la impunidad.

Estos hallazgos resaltan la necesidad urgente de fortalecer las capacidades del Ministerio Público mediante la adquisición de herramientas tecnológicas avanzadas, la implementación de programas de capacitación constante y la promoción de una mayor cooperación interinstitucional. Solo así se podrá superar las barreras actuales y mejorar la efectividad en la investigación y persecución de los delitos de fraude informático.

5.2.1. Contrastación de hipótesis

Hipótesis General:

Las dificultades en la individualización del ciberdelincuente influyen significativamente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023, debido a la falta de herramientas tecnológicas especializadas y la insuficiente capacitación de los fiscales, lo que limita la identificación y persecución de los responsables.

En la **contrastación de la hipótesis**, los resultados obtenidos confirman que las dificultades en la individualización de los ciberdelincuentes influyen significativamente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023.

En primer lugar, según las **Tablas 5 y 10**, el 80% de los encuestados (16 de 20) considera que la falta de herramientas tecnológicas avanzadas, como software de análisis forense y sistemas de rastreo, **casi siempre** dificulta la identificación de los responsables. Además, el 80% señala que la fiscalía **casi siempre** carece de estas herramientas para rastrear transacciones fraudulentas, lo que respalda la hipótesis de que la falta de recursos tecnológicos es un obstáculo clave.

En segundo lugar, las **Tablas 6 y 11** muestran que el 90% de los encuestados (18 de 20) afirma que el personal de la fiscalía **casi siempre** carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva, y el 100% (20 de 20) coincide en que no recibe capacitación constante en técnicas de investigación digital. Esto confirma que la insuficiente capacitación limita la aptitud de los fiscales para identificar y perseguir a los responsables.

Finalmente, las **Tablas 7, 9, 12, 13** revelan que el 80% de los encuestados (16 de 20) considera que los métodos de ocultamiento, como el anonimato y el cifrado, **casi siempre** hacen difícil la identificación de los ciberdelincuentes. Asimismo, el 80% afirma que **casi siempre** los casos se archivan debido a la imposibilidad de identificar a los responsables, y en la **Tabla 14** se pudo identificar que el 90% (18 de 20) coincide en que

esto genera impunidad. Estos resultados confirman que las dificultades en la individualización, derivadas de la falta de herramientas tecnológicas y capacitación, son un factor determinante en el archivo de los casos.

Primera Hipótesis especifica: *La falta de herramientas tecnológicas especializadas dificulta la identificación de los ciberdelincuentes en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023, lo que impide obtener pruebas suficientes y contribuye al archivo de los casos de fraude informático.* En la **contrastación de la hipótesis**, los resultados obtenidos confirman que la **falta de herramientas tecnológicas especializadas dificulta la identificación de los ciberdelincuentes** en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023, lo que impide obtener pruebas suficientes y contribuye al archivo de los casos de fraude informático.

Según las **Tablas 5 y 10**, el 80% de los encuestados (16 de 20) considera que la falta de herramientas tecnológicas avanzadas, como software de análisis forense y sistemas de rastreo, **casi siempre** dificulta la identificación de los responsables. Además, el 80% señala que la fiscalía **casi siempre** carece de estas herramientas para rastrear transacciones fraudulentas. Esta carencia limita la capacidad de los fiscales para recopilar pruebas sólidas, como transacciones rastreables o datos forenses, que son esenciales para individualizar a los ciberdelincuentes.

Del mismo modo, esta falta de herramientas tecnológicas tiene un impacto directo en el archivo de los casos, como se evidencia en las **Tablas 9 y 12**. El 80% de los encuestados (16 de 20) afirma que **casi siempre** los casos se archivan debido a la imposibilidad de identificar a los responsables, y el 80% señala que la falta de elementos de convicción, como transacciones no rastreables, es la principal razón por la que los casos no prosperan. Además, conforme la **Tabla 14**, el 90% de los encuestados (18 de 20) coincide en que el archivo de casos **casi siempre** genera impunidad, lo que refuerza la idea de que la falta de herramientas tecnológicas es un obstáculo crítico.

Segunda Hipótesis especifica: *La insuficiente capacitación de los fiscales afecta negativamente la individualización del ciberdelincuente, lo que limita la efectividad de la investigación y aumenta la probabilidad de que los casos de fraude informático sean archivados en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga.* En la **contrastación de la hipótesis**, los resultados obtenidos confirman que la **insuficiente capacitación de los fiscales afecta negativamente la individualización del ciberdelincuente**, lo que limita la efectividad de las investigaciones y aumenta la probabilidad de que los casos de fraude informático sean archivados en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga, durante el año 2023.

Según las **Tablas 6 y 11**, el 90% de los encuestados (18 de 20) afirma que el personal de la fiscalía **casi siempre** carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva. Además, el 100% de los encuestados (20 de 20) coincide en que el personal **casi siempre** no recibe capacitación constante en técnicas de investigación digital. Esta falta de formación especializada limita la capacidad de los fiscales para utilizar herramientas tecnológicas avanzadas y aplicar métodos de investigación adecuados, lo que dificulta la identificación de los responsables.

Esta insuficiente capacitación tiene un impacto directo en la individualización de los ciberdelincuentes, como se evidencia en las **Tablas 7 y 9**. El 80% de los encuestados (16 de 20) considera que los métodos de ocultamiento, como el anonimato y el cifrado, **casi siempre** hacen casi imposible la identificación de los responsables. Asimismo, el 80% afirma que **casi siempre** los casos se archivan debido a la imposibilidad de identificar a los ciberdelincuentes, y en la **Tabla 14** se evidencia que el 90% (18 de 20) coincide en que esto genera impunidad. Estos resultados demuestran que la falta de capacitación del personal es un factor predominante que contribuye al archivo de los casos.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

PRIMERO: La carencia de herramientas tecnológicas especializadas en las labores de investigación, como software de análisis forense digital y sistemas avanzados de rastreo, no solo constituye una limitación operativa, sino que revela una deficiencia estructural en la capacidad del sistema de justicia para enfrentar de manera eficaz el fenómeno del fraude informático. Esta insuficiencia tecnológica impide una adecuada recolección, análisis y preservación de evidencias digitales, elementos esenciales para sustentar una acusación penal robusta. Como consecuencia directa, se obstaculiza la identificación de los autores del delito y se favorece el archivo de los casos por falta de pruebas contundentes. Este panorama no solo compromete el principio de legalidad y el derecho de las víctimas a obtener justicia, sino que también refuerza la percepción de impunidad en los entornos digitales, debilitando la función disuasiva del derecho penal frente a los ciberdelitos.

SEGUNDO: De la misma manera se evidenció que, la carencia de una capacitación constante y especializada en técnicas de investigación digital constituye una limitación estructural que afecta directamente la eficacia de la Segunda Fiscalía Penal Corporativa de Huamanga en la persecución de delitos de fraude informático. Esta deficiencia formativa no solo restringe el desarrollo de competencias técnicas necesarias para enfrentar la complejidad de los delitos cibernéticos, sino que también obstaculiza la adecuada individualización de los responsables, debilitando así el proceso penal. En un contexto donde las modalidades delictivas digitales evolucionan con rapidez, la falta de actualización profesional no solo compromete la capacidad investigativa de los fiscales, sino que perpetúa la impunidad y mina la confianza ciudadana en el sistema de justicia.

TERCERO: Consecuentemente, con el presente trabajo de investigación se evidencia la creciente sofisticación de las técnicas utilizadas por los ciberdelincuentes, especialmente el uso de mecanismos avanzados de ocultamiento como redes privadas virtuales (VPN) y sistemas de cifrado, representa un desafío crítico para la identificación de

los autores en los casos de fraude informático. Esta realidad evidencia una asimetría preocupante entre las capacidades tecnológicas de los delincuentes y los recursos disponibles para los órganos de persecución penal. La dificultad para rastrear y atribuir con precisión las conductas delictivas en entornos digitales no solo limita la posibilidad de judicializar eficazmente estos casos, sino que también propicia su archivo, alimentando la sensación de impunidad. En este contexto, resulta evidente que la eficacia de la respuesta estatal ante el delito cibernético depende, en gran medida, de la capacidad del sistema fiscal para adaptarse tecnológicamente y fortalecer sus métodos de investigación digital.

CUARTO: Finalmente, en suma, la convergencia de tres factores críticos, como la carencia de herramientas tecnológicas especializadas, la insuficiente capacitación del personal fiscal y el uso cada vez más sofisticado de técnicas de ocultamiento digital por parte de los ciberdelincuentes, ha configurado un escenario adverso para la persecución efectiva de los delitos de fraude informático en la ciudad de Huamanga. Esta combinación de limitaciones estructurales y operativas no solo impide el adecuado desarrollo de las investigaciones, sino que ha derivado en una elevada tasa de archivo de casos, reflejando una preocupante ineficacia del sistema de justicia penal frente a esta modalidad delictiva. La consecuencia directa de esta situación es la consolidación de un clima de impunidad, que no solo vulnera los derechos de las víctimas, sino que además fomenta la repetición del delito al no existir una respuesta disuasiva y efectiva del Estado.

6.2. RECOMENDACIONES

PRIMERO: Se recomienda, con carácter urgente, que la Segunda Fiscalía Penal Corporativa de Huamanga destine recursos específicos a la adquisición e implementación de herramientas tecnológicas especializadas, tales como software de análisis forense digital, sistemas de rastreo de transacciones electrónicas y plataformas de ciberseguridad. Esta inversión no debe entenderse como un gasto aislado, sino como una estrategia fundamental para fortalecer la capacidad institucional frente a los crecientes desafíos del fraude informático. La incorporación de dichas tecnologías permitiría no solo optimizar la recolección y preservación de pruebas digitales con estándares de legalidad y fiabilidad, sino también mejorar sustancialmente los niveles de eficacia en la identificación de responsables y en la sustentación probatoria de los casos ante el sistema judicial. En un contexto donde los ciberdelitos evolucionan con rapidez y sofisticación, el fortalecimiento técnico de los órganos persecutores constituye un elemento clave para romper el ciclo de impunidad y garantizar una respuesta penal efectiva, proporcional y oportuna.

SEGUNDO: De la misma forma, es altamente recomendable que la Segunda Fiscalía Penal Corporativa de Huamanga implemente programas de capacitación continua y especializada dirigidos a fiscales y al personal involucrado en la investigación de delitos de fraude informático, con énfasis en técnicas de investigación digital, ciberseguridad y análisis forense. Esta medida no solo responde a la necesidad de actualizar conocimientos en un entorno tecnológico en constante evolución, sino que también constituye un pilar estratégico para incrementar la eficacia de las investigaciones. La falta de formación especializada limita la comprensión de los métodos delictivos utilizados en entornos digitales, lo que repercute negativamente en la correcta identificación de los responsables, la adecuada recolección de pruebas y la sustentación técnica de los casos. Por tanto, promover la profesionalización permanente del personal fiscal no es una acción complementaria, sino una condición indispensable para enfrentar con éxito la complejidad de los ciberdelitos, reducir la impunidad y garantizar una administración de justicia eficiente y adaptada a los desafíos del siglo XXI.

TERCERO: Asimismo, se recomienda establecer mecanismos de colaboración interinstitucional efectiva entre la Fiscalía, la Policía Nacional, las empresas tecnológicas y

otras entidades relevantes, a fin de facilitar el intercambio oportuno de información, recursos técnicos y herramientas especializadas necesarias para la investigación de delitos de fraude informático. Esta cooperación no solo permitiría superar las limitaciones individuales de cada institución, sino que también fortalecería una respuesta integral y coordinada frente a un fenómeno delictivo que, por su naturaleza transfronteriza y técnica, exige una actuación conjunta y ágil. La falta de articulación entre actores clave retrasa los procesos investigativos, limita el acceso a evidencia digital crítica y dificulta la trazabilidad de los ciberdelincuentes. En este sentido, el establecimiento de canales formales de comunicación, convenios de colaboración y protocolos de actuación conjunta se presenta como una estrategia esencial para mejorar la eficacia del sistema penal frente a los desafíos que plantea el cibercrimen.

CUARTO: Finalmente, se recomienda la creación de unidades especializadas en ciberdelincuencia dentro de la Fiscalía Penal de Huamanga, dotadas de personal altamente capacitado y equipadas con herramientas tecnológicas avanzadas. Esta propuesta responde a la necesidad de abordar de manera más eficiente y técnica los casos de fraude informático, cuya complejidad y especificidad superan las capacidades operativas de las estructuras fiscales tradicionales. La existencia de una unidad especializada permitiría centralizar conocimientos, procedimientos y recursos destinados exclusivamente a la investigación de delitos cibernéticos, lo cual no solo agilizaría los procesos de identificación y sanción de los responsables, sino que también contribuiría significativamente a la reducción de la alta tasa de archivo de casos. Además, estas unidades facilitarían la estandarización de buenas prácticas, el seguimiento especializado de casos complejos y una mayor capacidad de respuesta frente a nuevas formas de criminalidad digital, consolidando así un sistema de justicia penal más eficaz, especializado y adaptado a los retos del entorno tecnológico actual.

REFERENCIAS BIBLIOGRÁFICAS

Arazamendi, A. (2013). *Técnicas e instrumentos de investigación*: Guía práctica para la recolección de datos. Madrid. Editorial Académica.

Ayma, F. C. (2023). *Imputación concreta*. Lima: Zela.

Banco Central de Reserva del Perú. (2022). *Informe sobre transacciones fraudulentas en plataformas digitales*. Lima, Perú.

Barrio Giménez, A. (2017). *Ciberdelitos: Amenazas Criminales del ciberespacio*. Editorial Reus.

Carbajal Camones, M. (2022*). Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen*. https://repositorio.usmp.edu.pe/handle/20.500.12727/11398

Carrasco Diaz, S. (2006). *Metodología de la investigación científica*. Editorial San Marcos E.I.R.L. (primera reimpresión, 2006).

Carriedo Téllez, L. (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México*. MDTIC, Ciudad de México.

Código Procesal Penal. (2024). *Jurisprudencia relevante y actual*. Escuela de Derecho LP.

Convenio sobre la Ciberdelincuencia. *Capitulo III. Cooperación Interinstitucional*. Budapest, 23.XI.2001.

Defensoría del Pueblo (2023). *La Ciberdelincuencia en el Perú. Estrategia y retos del Estado*. Obtenido de: https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Espinoza Calderón, V. (2022). *Delitos informáticos y nuevas modalidades*. Editorial Instituto Pacífico. p. 56.

Espinoza C. V. (2023). *Cibercriminalidad y Delitos Informáticos*. Editorial Instituto Pacífico. 303-304.

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, M. (2014). *Metodología de la investigación*. Sexta edición. Interamericana Editores.

Jiménez Delgado, S. A. (2017). *Manual de derecho penal informático*. Jurista Editores E.I.R.L.

Matos Bernal, E. D. (2022). Tesis de Grado. *Especialización de la investigación preparatoria en los delitos de fraudes informáticos*. Universidad César Vallejo, Lima, Perú. Obtenido de https://hdl.handle.net/20.500.12692/84087

Mayer Lux, L. y Oliver Calderón, G. (2020). *El delito de fraude informático: concepto y delimitación*. Pontificia Universidad Católica del Valparaíso, Chile. Obtenido de: https://www.scielo.cl/pdf/rchdt/v9n1/0719-2584-rchdt-9-1-00151.pdf

Ministerio del Interior del Perú. (2022). *Reporte anual de delitos informáticos en el Perú*. Lima, Perú.

Paguay Calderón, V. & Granizo Castillo, J. (2020). *Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet*. Universidad Nacional de Chimborazo, Riobamba - Ecuador.

Peña, M. (2023). *Delitos informáticos o cibernéticos y los perjuicios hacia el sistema financiero en Colombia*. Trabajo de investigación para optar el título profesional de Magister en Derecho Penal. Bogotá.

Sánchez, H. (2016). *Metodología y diseños en la investigación científica*. Lima: Editorial Universitaria.

Segrera, M., & Cano, R. (2010). *La capacitación de los operadores de justicia en delitos informáticos*. Editorial Jurídica.

Segunda Fiscalía Provincial Penal Corporativa de Huamanga. (2023). *Reporte de casos de fraude informático archivados en el 2023*. Ayacucho, Perú: Autor.

Sotomayor Rodríguez, G. (2023). *La Calificación Fiscal en los Delitos Informáticos en el Distrito Fiscal de Lima Centro, 2019 – 2020*. Universidad César Vallejo, Lima – Perú.

Tejada, F. (2017). *Estrategias para enfrentar la ciberdelincuencia en el siglo XXI*. Revista de Derecho y Tecnología, 12(3), 34-56.

Unión Internacional de Telecomunicaciones. (2022). *Ciberseguridad y delitos informáticos: Tendencias globales*. Ginebra, Suiza: Autor.

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

12° Congreso de las Naciones Unidas sobre *Prevención del Delito y Justicia Penal*. Resolución 65/230 de la Asamblea General.

ANEXOS

Matriz de consistencia

"**Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Provincial Penal Corporativa de Huamanga, 2023**"

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	METODOLOGÍA
Problema General ¿Cómo influyen las dificultades en la individualización del ciberdelincuente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023?	**Objetivo General** Determinar cómo influyen las dificultades en la individualización del ciberdelincuente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023.	**Hipótesis General** Las dificultades en la individualización del ciberdelincuente influyen significativamente en el archivo de los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023, debido a la falta de herramientas tecnológicas especializadas y la insuficiente capacitación de los fiscales, lo que limita la identificación y persecución de los responsables.	**Variable Independiente (V1)** Dificultades en la individualización del ciberdelincuente Dimensiones: ▪ Recursos tecnológicos ▪ Capacitación del personal ▪ Métodos de los ciberdelincuentes ▪ Cooperación interinstitucional	**Tipo de investigación:** El presente trabajo investigativo es Aplicada. **Nivel de investigación:** Descriptivo – Explicativo. **Método de investigación:** Deductivo. **Enfoque de investigación:** Mixto. **Diseño de la investigación:** No experimental. **Universo:** Conformado por los casos de fraude informático registrados en el Distrito Fiscal de Ayacucho durante el 2023. **Población:** Conformado por los 37 casos reportados de fraude informático en la Segunda Fiscalía Penal Corporativa de Huamanga durante del año 2023.

PROBLEMAS ESPECÍFICOS	OBJETIVOS ESPECÍFICOS	HIPÓTESIS ESPECÍFICAS	Variable dependiente (V2):	Muestra: Conformada por 20 Carpetas Fiscales de fraude informático en la Segunda Fiscalía Penal Corporativa de Huamanga durante del año 2023.
Primer problema específico ¿De qué manera la falta de herramientas tecnológicas especializadas afecta la identificación de los ciberdelincuentes en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023?	**Primer objetivo específico** Determinar de qué manera la falta de herramientas tecnológicas especializadas afecta la identificación de los ciberdelincuentes en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023.	**Primera Hipótesis especifica** La falta de herramientas tecnológicas especializadas dificulta la identificación de los ciberdelincuentes en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023, lo que impide obtener pruebas suficientes y contribuye al archivo de los casos de fraude informático.	Archivo de los delitos de fraude informático. Dimensiones: ▪ Tasa de Archivo de casos. ▪ Causas de Archivo. ▪ Impacto de Archivo.	**Técnicas** ▪ Análisis documental. ▪ Encuesta. ▪ Procesamientos de datos. ▪ Empleo de software Excel. **Instrumentos** ▪ Fichas de análisis de documentos. ▪ Cuestionarios. ▪ Tablas de procesamientos. ▪ Sistema de Gestión Fiscal. **Fuentes** ▪ Literatura especializada en materia penal, procesal penal, delitos informáticos, fraude informático.

Segundo problema específico ¿De qué manera la falta de capacitación de los fiscales influye en la individualización del ciberdelincuente y en la decisión de archivar los delitos de fraude informático?	**Segundo objetivo específico** Determinar de qué manera la falta de capacitación de los fiscales influye en la individualización del ciberdelincuente y en la decisión de archivar los delitos de fraude informático en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023.	**Segunda Hipótesis especifica** La insuficiente capacitación de los fiscales afecta negativamente la individualización del ciberdelincuente, lo que limita la efectividad de la investigación y aumenta la probabilidad de que los casos de fraude informático sean archivados en la Segunda Fiscalía Provincial Penal Corporativa de Huamanga durante el año 2023.		▪ Fiscales de la Segunda Fiscalía Penal Corporativa de Huamanga y abogados con experiencia en delitos de fraude informático.

Ayacucho, 29 de noviembre de 2024

CARTA N° 048-2024-MP-FN- INDICADORES-ADMDFAYAC

Señor

CARLOS FRANCISCO GÓMEZ VILCATOMA
Jr. Chavín N° 125 - San Juan Bautista
Email: karlozvilctoma@gmail.com
Telf. 998892888

Presente. -

Asunto **:** Remite reporte de denuncias por delitos informáticos 2022 - 2023

Referencia **:** OFICIO N° 4005-2024-MP-FN-PJFSAYACUCHO
Solicitud: Carlos Francisco Gómez Vilcatoma

Expediente **:** MUPDFA20240008445

Tengo el agrado de dirigirme a Usted, por encargo de la Presidencia de la Junta de Fiscales Superiores del Distrito Fiscal de Ayacucho, en relación a los documentos de la referencia; se remite, adjunto al presente, el reporte de denuncias y el listado de casos ingresadas a las 6 Fiscalías Provinciales Penales Corporativa de Huamanga por delitos informáticos, correspondiente al periodo 2022 - 2023.

Sin otro particular, hago propicia la ocasión para expresarle mi mayor consideración.

Atentamente,

Firma Digital
Firmado digitalmente por CURI MENDOZA Alex Josseph FAU 20131370301 soft
Motivo: Soy el autor del documento
Fecha: 29.11.2024 12:19:30 -05:00

ALEX JOSSEPH CURI MENDOZA
ANALISTA DEL AREA DE GESTION DE INDICADORES
DISTRITO FISCAL AYACUCHO

cc:
ACM

DISTRITO FISCAL DE AYACUCHO
FISCALIAS PROVINCIALES PENALES CORPORATIVAS DE HUAMANGA
DENUNCIAS INGRESADAS POR DELITOS INFORMÁTICOS
PERIODO: 2022 - 2023

FISCALIA	AÑO		Total general
	2022	2023	
1° FPPC HUAMANGA	1	28	29
2° FPPC HUAMANGA	19	37	56
3° FPPC HUAMANGA	33	39	72
4° FPPC HUAMANGA	23	20	43
5° FPPC HUAMANGA	34	35	69
6° FPPC HUAMANGA	17	39	56
Total general	**127**	**198**	**325**

FUENTE: Sistema de Gestión Fiscal - SGF

DISTRITO FISCAL DE AYACUCHO
FISCALIAS PROVINCIALES PENALES CORPORATIVAS DE HUAMANGA
DENUNCIAS INGRESADAS POR DELITOS INFORMÁTICOS
PERIODO: 2022 - 2023

N°	Fiscalia	Fiscal	Caso	fe_ing_caso	Estado	Delito
1	1° FPPC HUAMANGA	ALARCON GUTIERREZ ROBINSON MARIANO	1606014501-2023-000684-0000	24/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
2	1° FPPC HUAMANGA	ALARCON GUTIERREZ ROBINSON MARIANO	1606014501-2023-000709-0000	03/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
3	1° FPPC HUAMANGA	ALARCON GUTIERREZ ROBINSON MARIANO	1606014501-2023-000753-0000	25/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
4	1° FPPC HUAMANGA	ALARCON GUTIERREZ ROBINSON MARIANO	1606014501-2023-001219-0000	20/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
5	1° FPPC HUAMANGA	ALARCON GUTIERREZ ROBINSON MARIANO	1606014501-2023-000367-0000	15/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
6	1° FPPC HUAMANGA	FARFAN WILSON ITALA	1606014501-2023-001656-0000	12/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
7	1° FPPC HUAMANGA	FARFAN WILSON ITALA	1606014501-2023-001787-0000	10/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
8	1° FPPC HUAMANGA	FARFAN WILSON ITALA	1606014501-2023-001961-0000	21/11/2023	CON ARCHIVO (CALIFICA)	FRAUDE INFORMATICO
9	1° FPPC HUAMANGA	FARFAN WILSON ITALA	1606014501-2023-002037-0000	22/11/2023	CON ARCHIVO (CALIFICA)	FRAUDE INFORMATICO
10	1° FPPC HUAMANGA	FLORES POZO WILMA	1606014501-2023-000735-0000	16/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
11	1° FPPC HUAMANGA	FLORES POZO WILMA	1606014501-2023-001210-0000	20/07/2023	ARCHIVO CONSENTIDO	FORMAS AGRAVADAS (SOBRE EQUIPOS DE INFORMATICA, TELECOMUNICACION, SUS COMPONENTES Y PERIFERICOS)
12	1° FPPC HUAMANGA	GALVEZ LAURA KAREN	1606014501-2023-000179-0000	02/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
13	1° FPPC HUAMANGA	GALVEZ LAURA KAREN	1606014501-2023-001584-0000	06/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
14	1° FPPC HUAMANGA	HUAMACCTO TANTA JULIO CESAR	1606014501-2022-001979-0000	17/10/2022	ARCHIVO CONSENTIDO	FORMAS AGRAVADAS (SOBRE EQUIPOS DE INFORMATICA, TELECOMUNICACION, SUS COMPONENTES Y PERIFERICOS)
15	1° FPPC HUAMANGA	HUAMACCTO TANTA JULIO CESAR	1606014501-2023-001209-0000	20/07/2023	ARCHIVO CONSENTIDO	FORMAS AGRAVADAS (SOBRE EQUIPOS DE INFORMATICA, TELECOMUNICACION, SUS COMPONENTES Y PERIFERICOS)
16	1° FPPC HUAMANGA	HUAMACCTO TANTA JULIO CESAR	1606014501-2023-001821-0000	06/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
17	1° FPPC HUAMANGA	INFANZON CASTRO FRANCISCO	1606014501-2023-002258-0000	01/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
18	1° FPPC HUAMANGA	INFANZON CASTRO FRANCISCO	1606014501-2023-001706-0000	18/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
19	1° FPPC HUAMANGA	LUDEÑA SOLIS ROSA MAGALI	1606014501-2023-001820-0000	02/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
20	1° FPPC HUAMANGA	LUDEÑA SOLIS ROSA MAGALI	1606014501-2023-001897-0000	16/11/2023	ARCHIVO CONSENTIDO	FORMAS AGRAVADAS (SOBRE EQUIPOS DE INFORMATICA, TELECOMUNICACION, SUS COMPONENTES Y PERIFERICOS)
21	1° FPPC HUAMANGA	MENDOZA TINEO LUIS ALBERTO	1606014501-2023-000487-0000	18/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
22	1° FPPC HUAMANGA	MENDOZA TINEO LUIS ALBERTO	1606014501-2023-001398-0000	29/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
23	1° FPPC HUAMANGA	RAMIREZ SALAZAR REYDER HENRY	1606014501-2023-001216-0000	20/07/2023	ARCHIVO CONSENTIDO	FORMAS AGRAVADAS (SOBRE EQUIPOS DE INFORMATICA, TELECOMUNICACION, SUS COMPONENTES Y PERIFERICOS)
24	1° FPPC HUAMANGA	SARMIENTO CHIPANA MARY CERLY	1606014501-2023-001046-0000	14/06/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
25	1° FPPC HUAMANGA	SARMIENTO CHIPANA MARY CERLY	1606014501-2023-002234-0000	30/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
26	1° FPPC HUAMANGA	SARMIENTO CHIPANA MARY CERLY	1606014501-2023-001896-0000	16/11/2023	CON ARCHIVO (CALIFICA)	FORMAS AGRAVADAS (SOBRE EQUIPOS DE INFORMATICA, TELECOMUNICACION, SUS COMPONENTES Y PERIFERICOS)
27	1° FPPC HUAMANGA	SOSA PARIONA JESSICA KARLA	1606014501-2023-001587-0000	06/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
28	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2022-000398-0000	15/03/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
29	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2022-001439-0000	23/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
30	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2022-001834-0000	21/10/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
31	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2022-001951-0000	10/11/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
32	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2022-002039-0000	27/12/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
33	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2023-000130-0000	12/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
34	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2023-000443-0000	17/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
35	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2023-000494-0000	21/03/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
36	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2023-001667-0000	11/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
37	2° FPPC HUAMANGA	ABAD CONTRERAS JORGE GUSTAVO	1606014502-2023-002464-0000	14/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
38	2° FPPC HUAMANGA	AMES BLAS JUAN CARLOS	1606014502-2022-001934-0000	10/11/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
39	2° FPPC HUAMANGA	AMES BLAS JUAN CARLOS	1606014502-2023-001491-0000	24/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
40	2° FPPC HUAMANGA	AMES BLAS JUAN CARLOS	1606014502-2023-002051-0000	10/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
41	2° FPPC HUAMANGA	ARANGO SULCA EDWARD	1606014502-2023-001417-0000	18/07/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
42	2° FPPC HUAMANGA	ARANGO SULCA EDWARD	1606014502-2023-002003-0000	05/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
43	2° FPPC HUAMANGA	ARANGO SULCA EDWARD	1606014502-2023-000407-0000	10/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
44	2° FPPC HUAMANGA	ARANGO SULCA EDWARD	1606014502-2023-001371-0000	10/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
45	2° FPPC HUAMANGA	AVILA FERNANDEZ MAURICIO	1606014502-2023-002600-0000	28/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
46	2° FPPC HUAMANGA	AVILA FERNANDEZ MAURICIO	1606014502-2023-001124-0000	20/06/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
47	2° FPPC HUAMANGA	CALLE VALER JOEL	1606014502-2022-001288-0000	04/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
48	2° FPPC HUAMANGA	CALLE VALER JOEL	1606014502-2022-002010-0000	23/11/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
49	2° FPPC HUAMANGA	CHUCHON PALOMINO NAYLEA LUY	1606014502-2023-000328-0000	30/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
50	2° FPPC HUAMANGA	CHUCHON PALOMINO NAYLEA LUY	1606014502-2023-000442-0000	17/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
51	2° FPPC HUAMANGA	CHUCHON PALOMINO NAYLEA LUY	1606014502-2022-000847-0000	26/05/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO

N°	Fiscalia	Fiscal	Caso	fe_ing_caso	Estado	Delito
52	2° FPPC HUAMANGA	DE LA TORRE HUAMANI OMAR PAVEL	1606014502-2023-001163-0000	23/06/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
53	2° FPPC HUAMANGA	DE LA TORRE HUAMANI OMAR PAVEL	1606014502-2023-002531-0000	27/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
54	2° FPPC HUAMANGA	DE LA TORRE HUAMANI OMAR PAVEL	1606014502-2022-000397-0000	15/03/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
55	2° FPPC HUAMANGA	DE LA TORRE HUAMANI OMAR PAVEL	1606014502-2023-000538-0000	23/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
56	2° FPPC HUAMANGA	DE LA TORRE HUAMANI OMAR PAVEL	1606014502-2023-001526-0000	16/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
57	2° FPPC HUAMANGA	HUAMAN CUBA IRMA YENISER	1606014502-2023-000465-0000	27/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
58	2° FPPC HUAMANGA	HUAMAN CUBA IRMA YENISER	1606014502-2023-001554-0000	25/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
59	2° FPPC HUAMANGA	HUAMAN CUBA IRMA YENISER	1606014502-2023-001627-0000	08/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
60	2° FPPC HUAMANGA	SIERRA ORIUNDO JOSE NORMAN	1606014502-2022-000022-0000	11/01/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
61	2° FPPC HUAMANGA	SIERRA ORIUNDO JOSE NORMAN	1606014502-2022-001432-0000	23/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
62	2° FPPC HUAMANGA	SIERRA ORIUNDO JOSE NORMAN	1606014502-2023-000150-0000	13/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
63	2° FPPC HUAMANGA	SIERRA ORIUNDO JOSE NORMAN	1606014502-2023-000340-0000	30/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
64	2° FPPC HUAMANGA	SIERRA ORIUNDO JOSE NORMAN	1606014502-2023-000341-0000	30/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
65	2° FPPC HUAMANGA	SIERRA ORIUNDO JOSE NORMAN	1606014502-2023-000444-0000	17/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
66	2° FPPC HUAMANGA	SULCA ALBITES MARIA DEL PILAR	1606014502-2023-000967-0000	11/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
67	2° FPPC HUAMANGA	SULCA ALBITES MARIA DEL PILAR	1606014502-2023-000979-0000	16/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
68	2° FPPC HUAMANGA	SULCA TUDELA ROSA ESTEPHANIA	1606014502-2023-001565-0000	29/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
69	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2022-001967-0000	23/11/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
70	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2022-001987-0000	23/11/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
71	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2023-000350-0000	30/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
72	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2023-000560-0000	24/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
73	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2023-002024-0000	09/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
74	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2023-002068-0000	19/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
75	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2023-002093-0000	13/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
76	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2022-000001-0000	10/01/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
77	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2022-000514-0000	25/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
78	2° FPPC HUAMANGA	VELARDE ALVAREZ PINTO MARIANO RICARDO	1606014502-2022-001437-0000	23/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
79	3° FPPC HUAMANGA	ALCA QUISPE GUIDO MANRIQUE	1606014503-2022-001642-0000	14/10/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
80	3° FPPC HUAMANGA	ALCA QUISPE GUIDO MANRIQUE	1606014503-2022-000536-0000	13/04/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
81	3° FPPC HUAMANGA	ALCA QUISPE GUIDO MANRIQUE	1606014503-2022-001975-0000	09/11/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
82	3° FPPC HUAMANGA	ALCA QUISPE GUIDO MANRIQUE	1606014503-2023-000358-0000	26/01/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
83	3° FPPC HUAMANGA	ALCA QUISPE GUIDO MANRIQUE	1606014503-2023-000459-0000	17/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
84	3° FPPC HUAMANGA	ALCA QUISPE GUIDO MANRIQUE	1606014503-2023-000513-0000	20/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
85	3° FPPC HUAMANGA	ALCA QUISPE GUIDO MANRIQUE	1606014503-2023-002354-0000	20/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
86	3° FPPC HUAMANGA	ALCA TOMAIRO JAIME	1606014503-2022-000076-0000	26/01/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
87	3° FPPC HUAMANGA	ALCA TOMAIRO JAIME	1606014503-2023-000531-0000	04/04/2023	ARCHIVO CONSENTIDO	FORMAS AGRAVADAS (SOBRE EQUIPOS DE INFORMATICA, TELECOMUNICACION, SUS COMPONENTES Y PERIFERICOS)
88	3° FPPC HUAMANGA	ALCA TOMAIRO JAIME	1606014503-2023-001583-0000	17/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
89	3° FPPC HUAMANGA	ALCA TOMAIRO JAIME	1606014503-2023-002427-0000	27/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
90	3° FPPC HUAMANGA	ALCA TOMAIRO JAIME	1606014503-2023-001599-0000	20/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
91	3° FPPC HUAMANGA	CASAFRANCA LUZA KEY MAXIMO.	1606014503-2022-001561-0000	01/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
92	3° FPPC HUAMANGA	CASAFRANCA LUZA KEY MAXIMO.	1606014503-2023-000524-0000	30/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
93	3° FPPC HUAMANGA	CASAFRANCA LUZA KEY MAXIMO.	1606014503-2023-000866-0000	21/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
94	3° FPPC HUAMANGA	CASAFRANCA LUZA KEY MAXIMO.	1606014503-2023-000867-0000	21/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
95	3° FPPC HUAMANGA	CASAFRANCA LUZA KEY MAXIMO.	1606014503-2023-001081-0000	16/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
96	3° FPPC HUAMANGA	CASAFRANCA LUZA KEY MAXIMO.	1606014503-2023-002356-0000	20/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
97	3° FPPC HUAMANGA	CASAFRANCA LUZA KEY MAXIMO.	1606014503-2023-002774-0000	29/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
98	3° FPPC HUAMANGA	CASAFRANCA LUZA KEY MAXIMO.	1606014503-2023-001631-0000	02/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
99	3° FPPC HUAMANGA	ENCISO MENESES NIEVES	1606014503-2023-002149-0000	03/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
100	3° FPPC HUAMANGA	ENCISO MENESES NIEVES	1606014503-2022-000256-0000	22/02/2022	ARCHIVO CONSENTIDO	INTERCEPTACION DE DATOS INFORMATICOS
101	3° FPPC HUAMANGA	ENCISO MENESES NIEVES	1606014503-2022-001503-0000	19/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
102	3° FPPC HUAMANGA	ENCISO MENESES NIEVES	1606014503-2023-000254-0000	25/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
103	3° FPPC HUAMANGA	JAICO MORALES YENY	1606014503-2023-002740-0000	28/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
104	3° FPPC HUAMANGA	JAICO MORALES YENY	1606014503-2023-002741-0000	28/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
105	3° FPPC HUAMANGA	JAICO MORALES YENY	1606014503-2022-000159-0000	16/02/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
106	3° FPPC HUAMANGA	JAICO MORALES YENY	1606014503-2022-000533-0000	13/04/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
107	3° FPPC HUAMANGA	MARMOLEJO CUADROS DANITZA	1606014503-2022-000259-0000	22/02/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
108	3° FPPC HUAMANGA	MARMOLEJO CUADROS DANITZA	1606014503-2022-001609-0000	29/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
109	3° FPPC HUAMANGA	MARMOLEJO CUADROS DANITZA	1606014503-2023-001105-0000	18/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
110	3° FPPC HUAMANGA	MAYORGA AMADO JUAN LUIS	1606014503-2022-001517-0000	24/08/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS

N°	Fiscalia	Fiscal	Caso	fe_ing_caso	Estado	Delito
111	3° FPPC HUAMANGA	MAYORGA AMADO JUAN LUIS	1606014503-2022-002015-0000	25/11/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
112	3° FPPC HUAMANGA	MAYORGA AMADO JUAN LUIS	1606014503-2022-001933-0000	08/11/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
113	3° FPPC HUAMANGA	MAYORGA AMADO JUAN LUIS	1606014503-2023-000512-0000	20/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
114	3° FPPC HUAMANGA	MAYORGA AMADO JUAN LUIS	1606014503-2023-001764-0000	18/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
115	3° FPPC HUAMANGA	MAYORGA AMADO JUAN LUIS	1606014503-2022-000275-0000	23/02/2022	CON ARCHIVO (PRELIMINAR)	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
116	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2022-001655-0000	18/10/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
117	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2023-000751-0000	18/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
118	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2023-001075-0000	16/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
119	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2023-002170-0000	04/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
120	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2023-002208-0000	04/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
121	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2022-000154-0000	16/02/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
122	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2022-000522-0000	12/04/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
123	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2022-000567-0000	22/04/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
124	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2022-000601-0000	05/05/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
125	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2023-000816-0000	20/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
126	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2023-000954-0000	24/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
127	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2023-001441-0000	12/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
128	3° FPPC HUAMANGA	MUNAREZ CAMPOS ESTEFANY MELISSA	1606014503-2023-002373-0000	24/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
129	3° FPPC HUAMANGA	ORE SICHA GISSELA ANAI	1606014503-2022-000475-0000	16/03/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
130	3° FPPC HUAMANGA	ORE SICHA GISSELA ANAI	1606014503-2022-000538-0000	13/04/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
131	3° FPPC HUAMANGA	ORE SICHA GISSELA ANAI	1606014503-2022-000539-0000	13/04/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
132	3° FPPC HUAMANGA	ORE SICHA GISSELA ANAI	1606014503-2022-001538-0000	25/08/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
133	3° FPPC HUAMANGA	ORE SICHA GISSELA ANAI	1606014503-2023-001660-0000	03/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
134	3° FPPC HUAMANGA	ORE SICHA GISSELA ANAI	1606014503-2023-002399-0000	02/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
135	3° FPPC HUAMANGA	REVOLLAR OCHATOMA EDITH	1606014503-2022-000038-0000	07/01/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
136	3° FPPC HUAMANGA	REVOLLAR OCHATOMA EDITH	1606014503-2022-000065-0000	14/01/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
137	3° FPPC HUAMANGA	REVOLLAR OCHATOMA EDITH	1606014503-2023-002378-0000	24/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
138	3° FPPC HUAMANGA	VALLEJOS REVOLLAR ERICK JONATTAN	1606014503-2022-001621-0000	29/09/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
139	3° FPPC HUAMANGA	VALLEJOS REVOLLAR ERICK JONATTAN	1606014503-2023-000475-0000	02/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
140	3° FPPC HUAMANGA	VALLEJOS REVOLLAR ERICK JONATTAN	1606014503-2023-000817-0000	20/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
141	3° FPPC HUAMANGA	VALLEJOS REVOLLAR ERICK JONATTAN	1606014503-2022-000518-0000	12/04/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
142	3° FPPC HUAMANGA	ZEGARRA HUAMAN ROMEL	1606014503-2022-001492-0000	17/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
143	3° FPPC HUAMANGA	ZEGARRA HUAMAN ROMEL	1606014503-2023-000450-0000	16/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
144	3° FPPC HUAMANGA	ZEGARRA HUAMAN ROMEL	1606014503-2023-000865-0000	21/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
145	3° FPPC HUAMANGA	ZEGARRA HUAMAN ROMEL	1606014503-2023-001338-0000	06/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
146	3° FPPC HUAMANGA	ZEGARRA HUAMAN ROMEL	1606014503-2023-001606-0000	20/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
147	3° FPPC HUAMANGA	ZEGARRA HUAMAN ROMEL	1606014503-2022-000268-0000	22/02/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
148	4° FPPC HUAMANGA	CABRERA CONDORPUSA GUIDO	1606014504-2022-001951-0000	23/11/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
149	4° FPPC HUAMANGA	CABRERA CONDORPUSA GUIDO	1606014504-2023-001671-0000	05/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
150	4° FPPC HUAMANGA	CABRERA CONDORPUSA GUIDO	1606014504-2023-002111-0000	31/10/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
151	4° FPPC HUAMANGA	CHAVEZ MALLMA ZINA PAMELA	1606014504-2022-000027-0000	06/01/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
152	4° FPPC HUAMANGA	CHAVEZ MALLMA ZINA PAMELA	1606014504-2023-001703-0000	03/10/2023	ARCHIVO CONSENTIDO	ACCESO ILICITO (ACCEDER SIN AUTORIZACION A SISTEMA INFORMATICO, CON VULNERACION DE MEDIDAS DE SEG...
153	4° FPPC HUAMANGA	CHAVEZ MALLMA ZINA PAMELA	1606014504-2023-000862-0000	03/05/2023	CON ARCHIVO (PRELIMINAR)	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
154	4° FPPC HUAMANGA	DAVILA CONTRERAS PATRICIA GUADALUPE	1606014504-2022-000398-0000	17/03/2022	ARCHIVO CONSENTIDO	ACCESO ILICITO (ACCEDER SIN AUTORIZACION A SISTEMA INFORMATICO, CON VULNERACION DE MEDIDAS DE SEG...
155	4° FPPC HUAMANGA	DAVILA CONTRERAS PATRICIA GUADALUPE	1606014504-2022-001230-0000	11/08/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
156	4° FPPC HUAMANGA	DAVILA CONTRERAS PATRICIA GUADALUPE	1606014504-2022-001554-0000	09/09/2022	ARCHIVO CONSENTIDO	INTERCEPTACION DE DATOS INFORMATICOS
157	4° FPPC HUAMANGA	DAVILA CONTRERAS PATRICIA GUADALUPE	1606014504-2023-000091-0000	24/01/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
158	4° FPPC HUAMANGA	DAVILA CONTRERAS PATRICIA GUADALUPE	1606014504-2023-000609-0000	30/03/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
159	4° FPPC HUAMANGA	DAVILA CONTRERAS PATRICIA GUADALUPE	1606014504-2023-000610-0000	30/03/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
160	4° FPPC HUAMANGA	DAVILA CONTRERAS PATRICIA GUADALUPE	1606014504-2023-002269-0000	24/11/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
161	4° FPPC HUAMANGA	GALVEZ HUAMAN REYNA ELIZABETH	1606014504-2023-001455-0000	04/08/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
162	4° FPPC HUAMANGA	GALVEZ HUAMAN REYNA ELIZABETH	1606014504-2023-001549-0000	10/08/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
163	4° FPPC HUAMANGA	GALVEZ HUAMAN REYNA ELIZABETH	1606014504-2023-002148-0000	02/11/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
164	4° FPPC HUAMANGA	GALVEZ HUAMAN REYNA ELIZABETH	1606014504-2023-001135-0000	03/07/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
165	4° FPPC HUAMANGA	GIRALDEZ SOLANO DEYSY DORIS	1606014504-2022-000063-0000	12/01/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
166	4° FPPC HUAMANGA	GIRALDEZ SOLANO DEYSY DORIS	1606014504-2023-002279-0000	27/11/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
167	4° FPPC HUAMANGA	GIRALDEZ SOLANO DEYSY DORIS	1606014504-2022-000566-0000	13/04/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
168	4° FPPC HUAMANGA	GIRALDEZ SOLANO DEYSY DORIS	1606014504-2022-001275-0000	15/08/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
169	4° FPPC HUAMANGA	GIRALDEZ SOLANO DEYSY DORIS	1606014504-2023-001128-0000	03/07/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS

N°	Fiscalia	Fiscal	Caso	fe_ing_caso	Estado	Delito
170	4° FPPC HUAMANGA	GIRALDEZ SOLANO DEYSY DORIS	1606014504-2022-000567-0000	13/04/2022	CON ARCHIVO (PRELIMINAR)	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
171	4° FPPC HUAMANGA	MANTARI INTIMAYTA HEIDE JHONALISA	1606014504-2022-001422-0000	22/08/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
172	4° FPPC HUAMANGA	MANTARI INTIMAYTA HEIDE JHONALISA	1606014504-2022-001261-0000	12/08/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
173	4° FPPC HUAMANGA	MANTARI INTIMAYTA HEIDE JHONALISA	1606014504-2023-002195-0000	02/11/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
174	4° FPPC HUAMANGA	PERALES ARGANDOÑA REYNALDO	1606014504-2022-001392-0000	19/08/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
175	4° FPPC HUAMANGA	PERALES ARGANDOÑA REYNALDO	1606014504-2022-002014-0000	12/12/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
176	4° FPPC HUAMANGA	PERALES ARGANDOÑA REYNALDO	1606014504-2023-001340-0000	25/07/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
177	4° FPPC HUAMANGA	PERALES ARGANDOÑA REYNALDO	1606014504-2022-000556-0000	12/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
178	4° FPPC HUAMANGA	PERALES ARGANDOÑA REYNALDO	1606014504-2022-001552-0000	08/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
179	4° FPPC HUAMANGA	ROJAS CASTILLO REYNALDA	1606014504-2022-001658-0000	03/11/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
180	4° FPPC HUAMANGA	ROJAS CASTILLO REYNALDA	1606014504-2022-000016-0000	05/01/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
181	4° FPPC HUAMANGA	ROJAS CASTILLO REYNALDA	1606014504-2022-001608-0000	29/09/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
182	4° FPPC HUAMANGA	TELLO JURADO JULIO CESAR	1606014504-2022-001190-0000	02/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
183	4° FPPC HUAMANGA	TELLO JURADO JULIO CESAR	1606014504-2023-000740-0000	27/04/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
184	4° FPPC HUAMANGA	TELLO JURADO JULIO CESAR	1606014504-2022-001161-0000	22/07/2022	ARCHIVO CONSENTIDO	ACCESO ILICITO (ACCEDER A UN SISTEMA INFORMATICO, EXCEDIENDO LO AUTORIZADO)
185	4° FPPC HUAMANGA	VILA CALLE MARICRUZ	1606014504-2023-002218-0000	03/11/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
186	4° FPPC HUAMANGA	VILA CALLE MARICRUZ	1606014504-2023-002295-0000	05/12/2023	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
187	4° FPPC HUAMANGA	ZUÑIGA VARGAS LUIS ENRIQUE	1606014504-2022-000782-0000	30/05/2022	CON ARCHIVO (PRELIMINAR)	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
188	4° FPPC HUAMANGA	ZUÑIGA VARGAS LUIS ENRIQUE	1606014504-2022-001062-0000	20/06/2022	CON ARCHIVO (PRELIMINAR)	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
189	4° FPPC HUAMANGA	ZUÑIGA VARGAS LUIS ENRIQUE	1606014504-2022-001887-0000	17/11/2022	CON ARCHIVO (PRELIMINAR)	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
190	5° FPPC HUAMANGA	AROTOMA ORE RAUL	1606014505-2022-000513-0000	29/03/2022	ARCHIVO CONSENTIDO	ACCESO ILICITO (ACCEDER A UN SISTEMA INFORMATICO, EXCEDIENDO LO AUTORIZADO)
191	5° FPPC HUAMANGA	AROTOMA ORE RAUL	1606014505-2022-000655-0000	20/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
192	5° FPPC HUAMANGA	AROTOMA ORE RAUL	1606014505-2022-001467-0000	02/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
193	5° FPPC HUAMANGA	AROTOMA ORE RAUL	1606014505-2022-001657-0000	20/09/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
194	5° FPPC HUAMANGA	AROTOMA ORE RAUL	1606014505-2022-001252-0000	01/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
195	5° FPPC HUAMANGA	ASCARZA MOISES. EDGAR RUBEN	1606014505-2022-000631-0000	18/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
196	5° FPPC HUAMANGA	ASCARZA MOISES. EDGAR RUBEN	1606014505-2022-001199-0000	14/07/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
197	5° FPPC HUAMANGA	ASCARZA MOISES. EDGAR RUBEN	1606014505-2022-001465-0000	02/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
198	5° FPPC HUAMANGA	ASCARZA MOISES. EDGAR RUBEN	1606014505-2022-001636-0000	15/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
199	5° FPPC HUAMANGA	ASCARZA MOISES. EDGAR RUBEN	1606014505-2023-000104-0000	26/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
200	5° FPPC HUAMANGA	ASCARZA MOISES. EDGAR RUBEN	1606014505-2023-002114-0000	27/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
201	5° FPPC HUAMANGA	ASCARZA MOISES. EDGAR RUBEN	1606014505-2023-002333-0000	13/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
202	5° FPPC HUAMANGA	CCASANI LAUREANO ROSA VERONICA JACQUELINE	1606014505-2023-001805-0000	05/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
203	5° FPPC HUAMANGA	CCASANI LAUREANO ROSA VERONICA JACQUELINE	1606014505-2022-000658-0000	20/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
204	5° FPPC HUAMANGA	CCASANI LAUREANO ROSA VERONICA JACQUELINE	1606014505-2022-001070-0000	16/06/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
205	5° FPPC HUAMANGA	CCASANI LAUREANO ROSA VERONICA JACQUELINE	1606014505-2022-001770-0000	14/11/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
206	5° FPPC HUAMANGA	CCASANI LAUREANO ROSA VERONICA JACQUELINE	1606014505-2022-001974-0000	02/12/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
207	5° FPPC HUAMANGA	CHIRINOS ARREDONDO MARCIAL NICOLAS	1606014505-2022-001287-0000	05/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
208	5° FPPC HUAMANGA	CHIRINOS ARREDONDO MARCIAL NICOLAS	1606014505-2023-000674-0000	13/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
209	5° FPPC HUAMANGA	CHIRINOS ARREDONDO MARCIAL NICOLAS	1606014505-2023-001460-0000	07/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
210	5° FPPC HUAMANGA	CHIRINOS ARREDONDO MARCIAL NICOLAS	1606014505-2023-002475-0000	28/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
211	5° FPPC HUAMANGA	CHIRINOS ARREDONDO MARCIAL NICOLAS	1606014505-2022-000348-0000	14/03/2022	ARCHIVO CONSENTIDO	ACCESO ILICITO (ACCEDER A UN SISTEMA INFORMATICO, EXCEDIENDO LO AUTORIZADO)
212	5° FPPC HUAMANGA	HUALLANCA GUTIERREZ SANDRA BETZABETH	1606014505-2022-000846-0000	07/06/2022	ARCHIVO CONSENTIDO	ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMATICOS
213	5° FPPC HUAMANGA	HUALLANCA GUTIERREZ SANDRA BETZABETH	1606014505-2022-001972-0000	02/12/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
214	5° FPPC HUAMANGA	HUALLANCA GUTIERREZ SANDRA BETZABETH	1606014505-2022-002093-0000	28/12/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
215	5° FPPC HUAMANGA	HUAMANI PILLACA NOEMI	1606014505-2023-000465-0000	02/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
216	5° FPPC HUAMANGA	HUAMANI PILLACA NOEMI	1606014505-2023-001717-0000	05/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
217	5° FPPC HUAMANGA	HUAMANI PILLACA NOEMI	1606014505-2023-002445-0000	12/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
218	5° FPPC HUAMANGA	HUAMANI PILLACA NOEMI	1606014505-2022-000708-0000	03/05/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
219	5° FPPC HUAMANGA	HUAMANI PILLACA NOEMI	1606014505-2023-000975-0000	19/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
220	5° FPPC HUAMANGA	HUAMANI PILLACA NOEMI	1606014505-2023-001807-0000	06/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
221	5° FPPC HUAMANGA	HUAMANI PILLACA NOEMI	1606014505-2022-001969-0000	24/05/2023	CON ARCHIVO (PRELIMINAR)	ATENTADO CONTRA LA INTEGRIDAD DE SISTEMAS INFORMATICOS (INUTILIZAR UN SISTEMA INFORMATICO, IMPIDI...
222	5° FPPC HUAMANGA	LEON CONGA NILDA	1606014505-2023-002478-0000	28/12/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
223	5° FPPC HUAMANGA	LEON CONGA NILDA	1606014505-2022-000651-0000	20/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
224	5° FPPC HUAMANGA	LEON CONGA NILDA	1606014505-2022-001204-0000	14/07/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
225	5° FPPC HUAMANGA	LEON CONGA NILDA	1606014505-2022-001646-0000	15/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
226	5° FPPC HUAMANGA	LEON CONGA NILDA	1606014505-2023-000116-0000	26/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
227	5° FPPC HUAMANGA	LEON CONGA NILDA	1606014505-2023-002292-0000	09/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
228	5° FPPC HUAMANGA	LEON CONGA NILDA	1606014505-2023-002331-0000	13/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO

N°	Fiscalia	Fiscal	Caso	fe_ing_caso	Estado	Delito
229	5° FPPC HUAMANGA	LEON CUBA DORA	1606014505-2022-000672-0000	25/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
230	5° FPPC HUAMANGA	LEON CUBA DORA	1606014505-2022-001463-0000	02/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
231	5° FPPC HUAMANGA	LEON CUBA DORA	1606014505-2023-000150-0000	06/02/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
232	5° FPPC HUAMANGA	LEON CUBA DORA	1606014505-2023-000468-0000	02/03/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
233	5° FPPC HUAMANGA	LEON CUBA DORA	1606014505-2023-001735-0000	29/12/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
234	5° FPPC HUAMANGA	LEON CUBA DORA	1606014505-2023-002334-0000	13/11/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
235	5° FPPC HUAMANGA	MELGAR SANTANDER EBERT AUGURIO	1606014505-2023-001808-0000	06/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
236	5° FPPC HUAMANGA	MELGAR SANTANDER EBERT AUGURIO	1606014505-2023-002336-0000	13/11/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
237	5° FPPC HUAMANGA	MERCADO QUISPE KEVIN	1606014505-2023-002394-0000	15/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
238	5° FPPC HUAMANGA	MERCADO QUISPE KEVIN	1606014505-2023-001804-0000	04/10/2023	CON ARCHIVO (CALIFICA)	FRAUDE INFORMATICO
239	5° FPPC HUAMANGA	MERCADO QUISPE KEVIN	1606014505-2022-001464-0000	02/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
240	5° FPPC HUAMANGA	MERCADO QUISPE KEVIN	1606014505-2023-001432-0000	05/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
241	5° FPPC HUAMANGA	MUÑOZ LAPA BRECHMAN FELIX	1606014505-2022-001255-0000	01/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
242	5° FPPC HUAMANGA	MUÑOZ LAPA BRECHMAN FELIX	1606014505-2022-001319-0000	22/08/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
243	5° FPPC HUAMANGA	MUÑOZ LAPA BRECHMAN FELIX	1606014505-2023-001678-0000	29/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
244	5° FPPC HUAMANGA	MUÑOZ LAPA BRECHMAN FELIX	1606014505-2022-000510-0000	24/03/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
245	5° FPPC HUAMANGA	MUÑOZ LAPA BRECHMAN FELIX	1606014505-2022-001975-0000	02/12/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
246	5° FPPC HUAMANGA	MUÑOZ LAPA BRECHMAN FELIX	1606014505-2023-002231-0000	06/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
247	5° FPPC HUAMANGA	PILLACA HUACCACHI JORGE	1606014505-2022-001205-0000	14/07/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
248	5° FPPC HUAMANGA	PILLACA HUACCACHI JORGE	1606014505-2023-001205-0000	13/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
249	5° FPPC HUAMANGA	PILLACA HUACCACHI JORGE	1606014505-2023-002453-0000	13/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
250	5° FPPC HUAMANGA	ROJAS FUENTES YANETT MAGALY	1606014505-2022-000630-0000	18/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
251	5° FPPC HUAMANGA	ROJAS FUENTES YANETT MAGALY	1606014505-2022-001987-0000	06/12/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
252	5° FPPC HUAMANGA	ROJAS FUENTES YANETT MAGALY	1606014505-2023-001108-0000	05/06/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
253	5° FPPC HUAMANGA	ROJAS FUENTES YANETT MAGALY	1606014505-2023-001537-0000	16/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
254	5° FPPC HUAMANGA	ROJAS FUENTES YANETT MAGALY	1606014505-2023-002443-0000	12/12/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
255	6° FPPC HUAMANGA	CHAVEZ GOMEZ TANIA FLOR	1606014506-2022-001339-0000	26/07/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
256	6° FPPC HUAMANGA	CHAVEZ GOMEZ TANIA FLOR	1606014506-2023-001280-0000	24/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
257	6° FPPC HUAMANGA	CHAVEZ GOMEZ TANIA FLOR	1606014506-2022-000140-0000	11/01/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
258	6° FPPC HUAMANGA	CHAVEZ GOMEZ TANIA FLOR	1606014506-2022-000385-0000	09/03/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
259	6° FPPC HUAMANGA	CHAVEZ GOMEZ TANIA FLOR	1606014506-2022-001811-0000	04/10/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
260	6° FPPC HUAMANGA	CHAVEZ GOMEZ TANIA FLOR	1606014506-2023-002393-0000	28/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
261	6° FPPC HUAMANGA	COLOS MORALES CLYDE URIEL	1606014506-2022-001853-0000	14/10/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
262	6° FPPC HUAMANGA	COLOS MORALES CLYDE URIEL	1606014506-2023-001105-0000	06/06/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
263	6° FPPC HUAMANGA	COLOS MORALES CLYDE URIEL	1606014506-2023-001754-0000	11/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
264	6° FPPC HUAMANGA	COLOS MORALES CLYDE URIEL	1606014506-2023-000051-0000	17/01/2023	CON ARCHIVO (CALIFICA)	FRAUDE INFORMATICO
265	6° FPPC HUAMANGA	COLOS MORALES CLYDE URIEL	1606014506-2023-001113-0000	08/06/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
266	6° FPPC HUAMANGA	COLOS MORALES CLYDE URIEL	1606014506-2023-001785-0000	13/09/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
267	6° FPPC HUAMANGA	GARCIA QUILCA OLIVERIO	1606014506-2023-000580-0000	17/03/2023	ARCHIVO CONSENTIDO	ACCESO ILICITO (ACCEDER SIN AUTORIZACION A SISTEMA INFORMATICO, CON VULNERACION DE MEDIDAS DE SEG...
268	6° FPPC HUAMANGA	GARCIA QUILCA OLIVERIO	1606014506-2023-000169-0000	07/02/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
269	6° FPPC HUAMANGA	GARCIA QUILCA OLIVERIO	1606014506-2023-001071-0000	02/06/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
270	6° FPPC HUAMANGA	GARCIA QUILCA OLIVERIO	1606014506-2023-001294-0000	01/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
271	6° FPPC HUAMANGA	GARCIA QUILCA OLIVERIO	1606014506-2023-001906-0000	13/10/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
272	6° FPPC HUAMANGA	GARCIA QUILCA OLIVERIO	1606014506-2023-002365-0000	27/11/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
273	6° FPPC HUAMANGA	JAIME MORALES RAUL GIANCARLO	1606014506-2023-000442-0000	07/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
274	6° FPPC HUAMANGA	JAIME MORALES RAUL GIANCARLO	1606014506-2023-001369-0000	11/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
275	6° FPPC HUAMANGA	JAIME MORALES RAUL GIANCARLO	1606014506-2023-002109-0000	13/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
276	6° FPPC HUAMANGA	JAIME MORALES RAUL GIANCARLO	1606014506-2023-001287-0000	25/07/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
277	6° FPPC HUAMANGA	JAIME MORALES RAUL GIANCARLO	1606014506-2023-001627-0000	31/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
278	6° FPPC HUAMANGA	MARTINEZ FLORES JUAN MARINO	1606014506-2023-002231-0000	22/11/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
279	6° FPPC HUAMANGA	MUÑOZ QUISPE NELSA JENET	1606014506-2022-001312-0000	03/10/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
280	6° FPPC HUAMANGA	MUÑOZ QUISPE NELSA JENET	1606014506-2023-000611-0000	21/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
281	6° FPPC HUAMANGA	MUÑOZ QUISPE NELSA JENET	1606014506-2023-001198-0000	16/06/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
282	6° FPPC HUAMANGA	MUÑOZ QUISPE NELSA JENET	1606014506-2023-001337-0000	09/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
283	6° FPPC HUAMANGA	MUÑOZ QUISPE NELSA JENET	1606014506-2023-001784-0000	13/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
284	6° FPPC HUAMANGA	MUÑOZ QUISPE NELSA JENET	1606014506-2023-001795-0000	13/09/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
285	6° FPPC HUAMANGA	PAITAN BUENDIA NELLY	1606014506-2022-001301-0000	19/07/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
286	6° FPPC HUAMANGA	PAITAN BUENDIA NELLY	1606014506-2022-001869-0000	19/10/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
287	6° FPPC HUAMANGA	PALOMINO CARHUAS JULIO EDGAR	1606014506-2022-001674-0000	22/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO

N°	Fiscalia	Fiscal	Caso	fe_ing_caso	Estado	Delito
288	6° FPPC HUAMANGA	PALOMINO CARHUAS JULIO EDGAR	1606014506-2022-001790-0000	03/10/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
289	6° FPPC HUAMANGA	POMA HUAMAN ENA FLORABEL	1606014506-2022-001356-0000	27/07/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
290	6° FPPC HUAMANGA	POMA HUAMAN ENA FLORABEL	1606014506-2023-000075-0000	18/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
291	6° FPPC HUAMANGA	POMA HUAMAN ENA FLORABEL	1606014506-2023-000471-0000	10/03/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
292	6° FPPC HUAMANGA	POMA HUAMAN ENA FLORABEL	1606014506-2023-001547-0000	21/08/2023	ARCHIVO CONSENTIDO	ATENTADO CONTRA LA INTEGRIDAD DE SISTEMAS INFORMATICOS (INUTILIZAR UN SISTEMA INFORMATICO, IMPIDI...
293	6° FPPC HUAMANGA	RIVEROS LANDEO JAZMINY	1606014506-2023-000233-0000	23/02/2023	ARCHIVO CONSENTIDO	INTERCEPTACION DE DATOS INFORMATICOS
294	6° FPPC HUAMANGA	RIVEROS LANDEO JAZMINY	1606014506-2022-002153-0000	28/12/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
295	6° FPPC HUAMANGA	RONDINEL AGREDA DIANA DEL PILAR	1606014506-2022-001277-0000	11/07/2022	CON ARCHIVO (CALIFICA)	FRAUDE INFORMATICO
296	6° FPPC HUAMANGA	RONDINEL AGREDA DIANA DEL PILAR	1606014506-2022-000829-0000	27/04/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
297	6° FPPC HUAMANGA	RONDINEL AGREDA DIANA DEL PILAR	1606014506-2022-001547-0000	13/09/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
298	6° FPPC HUAMANGA	RONDINEL AGREDA DIANA DEL PILAR	1606014506-2023-000005-0000	09/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
299	6° FPPC HUAMANGA	RONDINEL AGREDA DIANA DEL PILAR	1606014506-2023-000006-0000	09/01/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
300	6° FPPC HUAMANGA	RONDINEL AGREDA DIANA DEL PILAR	1606014506-2022-001580-0000	16/09/2022	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
301	6° FPPC HUAMANGA	RONDINEL AGREDA DIANA DEL PILAR	1606014506-2023-000195-0000	20/02/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO
302	6° FPPC HUAMANGA	ZAMBRANO CAVALCANTI GALILA GANDHI	1606014506-2023-000183-0000	20/04/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
303	6° FPPC HUAMANGA	ZAMBRANO CAVALCANTI GALILA GANDHI	1606014506-2022-002094-0000	22/12/2022	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
304	6° FPPC HUAMANGA	ZAMBRANO CAVALCANTI GALILA GANDHI	1606014506-2023-000871-0000	22/05/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
305	6° FPPC HUAMANGA	ZAMBRANO CAVALCANTI GALILA GANDHI	1606014506-2023-001604-0000	24/08/2023	ARCHIVO CONSENTIDO	FRAUDE INFORMATICO
306	6° FPPC HUAMANGA	ZAMBRANO CAVALCANTI GALILA GANDHI	1606014506-2023-002366-0000	27/11/2023	CON ARCHIVO (PRELIMINAR)	FRAUDE INFORMATICO

FUENTE: SGF

FICHA DE ANÁLISIS DOCUMENTAL

DELITO DE FRAUDE INFORMÁTICO, SEGUNDA FISCALÍA PROVINCIAL PENAL CORPORATIVA DE HUAMANGA, 2023

N°	Carpeta Fiscal	Denuncia	Investigado	Resultado
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA
FACULTAD DE DERECHO Y CIENCIAS POLITICAS
ESCUELA DE FORMACION PROFESIONAL DE DERECHO

CUESTIONARIO

Estimado(a) Dr.(a) el presente cuestionario parte del estudio sobre: ***"Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Penal Corporativa de Huamanga, 2023"***. A continuación, se le presentará una serie de preguntas.

Marque con una **x** su respuesta
Escala de Liker para la calificación:

1	**Nunca**
2	**Casi nunca**
3	**Algunas veces**
4	**Casi siempre**
5	**Siempre**

ITEMS	1	2	3	4	5
1. ¿La falta de recursos tecnológicos (software de análisis forense, herramientas de rastreo) dificulta la individualización de los ciberdelincuentes?					
2. ¿El personal de la fiscalía carece de la capacitación necesaria para investigar delitos de fraude informático de manera efectiva?					
3. ¿Los métodos utilizados por los ciberdelincuentes (anonimato, cifrado, criptomonedas) hacen casi imposible su identificación?					
4. ¿La falta de cooperación interinstitucional (con policía, empresas tecnológicas, etc.) afecta negativamente la investigación de estos delitos?					
5. ¿La mayoría de los casos de fraude informático se archivan debido a la imposibilidad de identificar a los responsables?					
6. ¿La fiscalía no cuenta con herramientas tecnológicas avanzadas para rastrear transacciones fraudulentas?					
7. ¿El personal de la fiscalía no recibe capacitación constante en técnicas de investigación digital?					
8. ¿La falta de elementos de convicción (transacciones no rastreables, ausencia de testigos) es la principal razón por la que los casos se archivan?					
9. ¿La dificultad para identificar a los responsables (anonimato, uso de tecnologías avanzadas) lleva al archivo de la mayoría de los casos?					
10. ¿El archivo de casos de fraude informático genera impunidad?					

¡Muchas gracias ¡

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

Titulo de la tesis: "Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Penal Corporativa de Huamanga, 2023"

Nombre del estudiante: Bach. Carlos Francisco Gómez Vilcatoma

Experto: ROSA ESTEPHANIA SULCA TUDELA (Fiscal Adjunta Provincial)

Instrucciones: Determinar si el instrumento de medición reúne los indicadores mencionados y evaluar si ha sido muy bueno, bueno, regular, malo o muy malo; colocando con un aspa (X) en el casillero correspondiente.

1	**Muy bueno**
2	**Bueno**
3	**Regular**
4	**Malo**
5	**Muy malo**

Indicadores	Definición	1	2	3	4	5
Claridad y precisión	El instrumento de recolección de datos, encuesta a expertos está orientado al problema de investigación.		X			
Coherencia	El instrumento de recolección de datos, guarda relación con los objetivos, la hipótesis y las variables de la investigación.		X			
Validez	Las preguntas han sido formuladas tomando en consideración la validez del contenido del trabajo de investigación.		X			
Organización	La formulación de la encuesta a experto resulta estructuralmente adecuada.		X			
Confiabilidad	El instrumento es confiable porque se aplica la escala de Likert.		X			
Control de sesgo	Presenta preguntas distractoras para controlar la contaminación de las preguntas.		X			
Orden	Las preguntas formuladas presentan un orden especifico, de lo general a lo concreto.		X			
Marco referencial	Las preguntas han sido efectuadas conforme al grado de experiencia de los expertos encuestados.		X			
Extensión	El número de preguntas no resulta excesivo.		X			
Inocuidad	Las preguntas no constituyen un riesgo para el encuestado.		X			

Observaciones: Ninguna

En consecuencia, el instrumento puede ser aplicado.

Ayacucho, 10 de enero de 2025

Abg. Rosa Estephania Sulca Tudela
FISCAL ADJUNTA PROVINCIAL
Segunda Fiscalía Provincial Penal
Corporativa de Huamanga

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

Titulo de la tesis: "Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Penal Corporativa de Huamanga, 2023"

Nombre del estudiante: Bach. Carlos Francisco Gómez Vilcatoma

Experto: WALTER ALEX PRADO CHUCHÓN (Abogado Litigante)

Instrucciones: Determinar si el instrumento de medición reúne los indicadores mencionados y evaluar si ha sido muy bueno, bueno, regular, malo o muy malo; colocando con un aspa (X) en el casillero correspondiente.

1	**Muy bueno**
2	**Bueno**
3	**Regular**
4	**Malo**
5	**Muy malo**

Indicadores	Definición	1	2	3	4	5
Claridad y precisión	El instrumento de recolección de datos, encuesta a expertos está orientado al problema de investigación.		X			
Coherencia	El instrumento de recolección de datos, guarda relación con los objetivos, la hipótesis y las variables de la investigación.		X			
Validez	Las preguntas han sido formuladas tomando en consideración la validez del contenido del trabajo de investigación.		X			
Organización	La formulación de la encuesta a experto resulta estructuralmente adecuada.		X			
Confiabilidad	El instrumento es confiable porque se aplica la escala de Likert.		X			
Control de sesgo	Presenta preguntas distractoras para controlar la contaminación de las preguntas.		X			
Orden	Las preguntas formuladas presentan un orden especifico, de lo general a lo concreto.		X			
Marco referencial	Las preguntas han sido efectuadas conforme al grado de experiencia de los expertos encuestados.		X			
Extensión	El número de preguntas no resulta excesivo.		X			
Inocuidad	Las preguntas no constituyen un riesgo para el encuestado.		X			

Observaciones: Ninguna

En consecuencia, el instrumento puede ser aplicado.

Ayacucho, 10 de enero de 2025

Walter Alex Prado Chuchón
ABOGADO
Reg. C.A.A. N° 2018

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA DE FORMACIÓN PROFESIONAL DE DERECHO

ACTA DE SUSTENTACIÓN DE TESIS PARA LA TITULACIÓN DEL ASPIRANTE

CARLOS FRANCISCO GOMEZ VILCATOMA

En la ciudad de Ayacucho, siendo las 16:00 p.m. del día 06 de mayo del 2025, se reunieron en el Auditorio de la Facultad de Derecho y Ciencias Políticas de la Universidad Nacional de San Cristóbal de Huamanga. Los docentes Richard Almonacid Zamudio, Luz Diana Gamboa Castro, Iván Chumbe Carrera, Marlene León Palacios y Víctor Cabrera Medrano, el primero como Presidente y el último como Secretario, todos integrantes del jurado calificador para la sustentación de la tesis del Bach. Carlos Francisco Gomez Vilcatoma.

El Presidente da inicio al Acto Académico preguntando al aspirante si tiene alguna objeción contra los miembros del jurado, respondiendo que no, luego dispuso la lectura de la Resolución Decanal N° 178-2025-UNSCH-FDCP-D de fecha 24 de abril de 2025 y el Reglamento, invitando al Bachiller a que inicie con su exposición de la tesis denominada: Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Provincial Penal Corporativa de Huamanga, 2023. Concluida la exposición el Presidente invitó a los miembros del jurado a realizar sus preguntas y/o objeciones de mayor a menor antigüedad, al final el Presidente realizó las suyas.

Concluidas la absolución de preguntas y/o objeciones, el Presidente invitó al aspirante a retirarse del Auditorio, igual al público para que el jurado pueda deliberar. Al concluir la deliberación, el Presidente dispuso la reapertura del Acto Académico para comunicar el resultado de la deliberación. El jurado decidió por unanimidad aprobarlo con la nota de quince (15). Reabierto el Acto Académico, el Presidente comunicó el resultado, dando las recomendaciones del caso, con lo que concluyó el Acto Académico a las 18:00 p.m. del mismo día. Firmando en señal de conformidad.

Richard Almonacid Zamudio

(Presidente)

Luz Diana Gamboa Castro

Iván Chumbe Carrera

Marlene León Palacios

Víctor Cabrera Medrano

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

CONSTANCIA DE ORIGINALIDAD N° 06 -2025-UNSCH-FDCP

El que suscribe responsable verificador de originalidad de trabajo de tesis de la Facultad de Derecho y Ciencias Políticas de la UNSCH, en cumplimiento a la Resolución de Consejo Universitario N.° 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. Carlos Francisco Gomez Vilcatoma**
Para	**Titulo profesional**
Denominación de la tesis	**Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Provincial Penal Corporativa de Huamanga, 2023.**
Evaluación de Originalidad	**18%**
Numero de trabajo	**2655552630**
Fecha	**08 de mayo de 2025**

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

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

Ayacucho, 08 de mayo de 2025

Dr. Richard Almonacid Zamudio

Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Provincial Penal Corporativa de Huamanga, 2023.

por Carlos Francisco GOMEZ VILCATOMA

Fecha de entrega: 08-may-2025 08:44a.m. (UTC-0500)
Identificador de la entrega: 2655552630
Nombre del archivo: TESIS_FINAL_CARLOS-GOMEZ-fraude_informatico-2FPCH.docx (677.02K)
Total de palabras: 23236
Total de caracteres: 133717

Dificultades en la individualización del ciberdelincuente y su influencia en el archivo de los delitos de fraude informático, Segunda Fiscalía Provincial Penal Corporativa de Huamanga, 2023.

INFORME DE ORIGINALIDAD

18%	16%	6%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unsch.edu.pe Fuente de Internet	3%
2	hdl.handle.net Fuente de Internet	2%
3	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	2%
4	lpderecho.pe Fuente de Internet	2%
5	ebiz.pe Fuente de Internet	1%
6	Submitted to Universidad Privada del Norte Trabajo del estudiante	1%
7	revistas.pj.gob.pe Fuente de Internet	1%
8	repositorio.upla.edu.pe Fuente de Internet	<1%
9	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 17 (2001)", Brill, 2005 Publicación	<1%
10	www.transparencia.org.es Fuente de Internet	<1%

11	cdn.www.gob.pe Fuente de Internet	<1 %
12	doku.pub Fuente de Internet	<1 %
13	www.sbs.gob.pe Fuente de Internet	<1 %
14	repositorio.upse.edu.ec Fuente de Internet	<1 %
15	xdocs.net Fuente de Internet	<1 %
16	es.slideshare.net Fuente de Internet	<1 %
17	repositorio.ucv.edu.pe Fuente de Internet	<1 %
18	Submitted to Universidad Anahuac México Sur Trabajo del estudiante	<1 %
19	portalrevistas.aulavirtualusmp.pe Fuente de Internet	<1 %
20	repositorio.usanpedro.edu.pe Fuente de Internet	<1 %
21	www.iksadamerica.org Fuente de Internet	<1 %
22	repositorio.uss.edu.pe Fuente de Internet	<1 %
23	repositorio.ulasamericas.edu.pe Fuente de Internet	<1 %
24	repositorio.une.edu.pe Fuente de Internet	<1 %
25	repositorio.uandina.edu.pe Fuente de Internet	<1 %

26	www.coursehero.com Fuente de Internet	<1 %
27	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	<1 %
28	Submitted to Universidad Argentina John F. Kennedy Trabajo del estudiante	<1 %
29	(Carlinda Leite and Miguel Zabalza). "Ensino superior: inovação e qualidade na docência", Repositório Aberto da Universidade do Porto, 2012. Publicación	<1 %
30	dspace.unach.edu.ec Fuente de Internet	<1 %
31	Submitted to Universidad Carlos III de Madrid - EUR Trabajo del estudiante	<1 %
32	Jiménez, Carlos Arturo Flores. "La Responsabilidad de las Entidades Financieras Ante la Comisión de Delitos Informáticos", Pontificia Universidad Catolica del Peru (Peru), 2024 Publicación	<1 %

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		