UNIVERSIDAD AUTÓNOMA DE ICA

FACULTAD DE INGENIERÍA, CIENCIAS Y ADMINISTRACIÓN

PROGRAMA ACADÉMICO DE DERECHO

TESIS

INVESTIGACIÓN DEL DELITO DE FRAUDE INFORMÁTICO EN LA FISCALÍA DE LA PROVINCIA DE SAN ROMÁN – JULIACA, 2024

LÍNEA DE INVESTIGACIÓN:

GESTIÓN PÚBLICA

PRESENTADO POR:

JOSELYN KAREN CHURATA CHUQUIPALLA

Código de ORCID N° 0009-0007-4504-3839

DIANETH ADELAYDA QUISPE MACHACA

Código de ORCID N° 0009-0002-8286-4082

TESIS DESARROLLADA PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADA

DOCENTE ASESOR:

Dr. MIGUEL GERARDO MENDOZA VARGAS

CÓDIGO ORCID N° 0000-0002-9812-6714

CHINCHA, 2024

Constancia de aprobación de investigación

UNIVERSIDAD AUTÓNOMA DE ICA

CONSTANCIA DE APROBACIÓN DE TESIS

Chincha, 24 de febrero de 2024

Dra. Mariana Alejandra Campos Sobrino
DECANA DE LA FACULTAD DE INGENIERÍA, CIENCIAS Y ADMINISTRACIÓN
Presente. -

De mi especial consideración:

Sirva la presente para saludarla e informar que las bachilleres **CHURATA CHUQUIPALLA JOSELYN KAREN,** con DNI Nro. **77133616, y QUISPE MACHACA DIANETH ADELAYDA,** con DNI Nro. **77022060;** de la Facultad Ingeniería, Ciencias y Administración del Programa Académico de **DERECHO,** han cumplido con presentar su TESIS titulada: **"INVESTIGACIÓN DEL DELITO DE FRAUDE INFORMÁTICO EN LA FISCALÍA DE LA PROVINCIA DE SAN ROMÁN – JULIACA, 2024"** con mención:

APROBADO(A)

Por lo tanto, queda expedita para la revisión por parte de los Jurados para su sustentación.

Agradezco por anticipado la atención a la presente, aprovecho la ocasión para expresar los sentimientos de mi especial consideración y deferencia personal.

Atentamente,

Dr. Miguel G. Mendoza Vargas
CODIGO ORCID: 0000-0002-9812-6714

Declaratoria de autenticidad de la investigación

Declaratoria de autenticidad de la investigación

Yo, **Joselyn Karen CHURATA CHUQUIPALLA**, identificada con DNI N° 77133616, y **Dianeth Adelayda QUISPE MACHACA** identificada con DNI N° 77022060, en nuestra condición de estudiantes del programa de estudios **Derecho**, de la **Facultad de Ingeniería, Ciencias y Administración**, en la Universidad Autónoma de Ica y que habiendo desarrollado la Tesis titulada: **"INVESTIGACIÓN DEL DELITO DE FRAUDE INFORMÁTICO EN LA FISCALÍA DE LA PROVINCIA DE SAN ROMÁN – JULIACA, 2024"**, declaramos bajo juramento que:

a. La investigación realizada es de nuestra autoría.

b. La tesis no ha cometido falta alguna a las conductas responsables de investigación, por lo que, no se ha cometido plagio, ni autoplagio en su elaboración.

c. La información presentada en la tesis se ha elaborado respetando las normas de redacción para la citación y referenciación de las fuentes de información consultadas.

d. Así mismo, el estudio no ha sido publicado anteriormente, ni parcial, ni totalmente con fines de obtención de algún grado académico o título profesional.

e. Los resultados presentados en el estudio, producto de la recopilación de datos, son reales, por lo que, el (la) investigador(a), no han incurrido ni en falsedad, duplicidad, copia o adulteración de estos, ni parcial, ni totalmente.

f. La investigación cumple con el porcentaje de similitud establecido según la normatividad

7 % similitud

Autorizo a la Universidad Autónoma de Ica, de identificar plagio, autoplagio, falsedad de información o adulteración de estos, se proceda según lo indicado por la normatividad vigente de la universidad, asumiendo las consecuencias o sanciones que se deriven de alguna de estas malas conductas.

Juliaca, 28 de marzo de 2025.

Joselyn Karen Churata Chuquipalla
DNI N° 77133616

Dianeth Adelayda Quispe Machaca
DNI N° 77022060

CERTIFICACIÓN A LA VUELTA

CERTIFICO: Que las firmas y las huellas digitales que anteceden corresponden a: **JOSELYN KAREN CHURATA CHUQUIPALLA,** identificado(a) con DNI N° **77133616, y a: DIANETH ADELAYDA QUISPE MACHACA,** identificado(a) con DNI N° **77022060.-** EL Notario que suscribe no asume responsabilidad sobre el contenido del documento D. leg. 1049, de todo lo que Doy Fe.- Juliaca, 28 de marzo del 2025.-==========

0112602656

NOTARIA
SUNI HUANCA JESUS
SERVICIO DE AUTENTICACIÓN E IDENTIFICACIÓN BIOMÉTRICA

INFORMACIÓN PERSONAL

DNI	77133616
Primer Apellido	CHURATA
Segundo Apellido	CHUQUIPALLA
Nombres	JOSELYN KAREN

CORRESPONDE

La primera impresión dactilar capturada corresponde al DNI consultado. La segunda impresión dactilar capturada corresponde al DNI consultado.

CHURATA CHUQUIPALLA, JOSELYN KAREN
DNI 77133616

INFORMACIÓN DE CONSULTA DACTILAR

Operador: 73359724 - Tobet Tomas Livisi Vilcapaza

Fecha de Transacción: 28-03-2025 15:01:46

Entidad: 10023887156 - SUNI HUANCA JESUS

VERIFICACIÓN DE CONSULTA

Puede verificar la información en línea en:
https://serviciosbiometricos.reniec.gob.pe/identifica3/verification.do

Número de Consulta: 0112602656

0112602685

NOTARIA
SUNI HUANCA JESUS
SERVICIO DE AUTENTICACIÓN E IDENTIFICACIÓN BIOMÉTRICA

INFORMACIÓN PERSONAL

DNI	77022060
Primer Apellido	QUISPE
Segundo Apellido	MACHACA
Nombres	DIANETH ADELAYDA

CORRESPONDE

La primera impresión dactilar capturada corresponde al DNI consultado. La segunda impresión dactilar capturada corresponde al DNI consultado.

QUISPE MACHACA, DIANETH ADELAYDA
DNI 77022060

INFORMACIÓN DE CONSULTA DACTILAR

Operador: 73359724 - Tobet Tomas Livisi Vilcapaza

Fecha de Transacción: 28-03-2025 15:02:12

Entidad: 10023887156 - SUNI HUANCA JESUS

VERIFICACIÓN DE CONSULTA

Puede verificar la información en línea en: https://serviciosbiometricos.reniec.gob.pe/identifica3/verification.do

Número de Consulta: 0112602685

Dedicatoria

A mis seres queridos, que me han apoyado en este camino, con mucho amor y dedicación. Asimismo, a mi madre, quien me ha enseñado la importancia de la perseverancia y por ser mi mayor inspiración. A mis queridas amistades por estar siempre ahí para animarme.

Dianeth Adelayda Quispe Machaca.

A mis padres, por inculcarme los valores de la perseverancia y el amor al conocimiento; a mis hermanos, por su apoyo constante y confianza en mis capacidades. A mis amigos, por su compañía. No podría haber logrado esto sin el apoyo de todos ustedes, siempre serán mi mayor motivación.

Joselyn Karen Churata Chuquipalla

Agradecimiento

Agradecemos a nuestro asesor, por su orientación y apoyo constante, así como a la Universidad Autónoma de Ica, por la oportunidad de brindarnos continuar con nuestra educación. A nuestros amigos por su motivación y nuestra familia por su apoyo incondicional. También agradecer a todas las personas y la entidad que participó en nuestra investigación.

Joselyn Karen Churata Chuquipalla
Dianeth Adelayda Quispe Machaca.

Resumen

Objetivo general: Determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

Metodología: La metodología es cualitativa, tipo de estudio básico, nivel de investigación descriptivo e interpretativa, diseño de investigación fenomenológico. Para el procedimiento de muestreo se utilizó el no probabilístico por conveniencia, incluyendo dos fiscales provinciales y cinco fiscales adjuntos provinciales, en la Fiscalía de la Provincia de San Román – Juliaca; para la recolección de datos se utilizó la técnica de entrevista y el instrumento de investigación fue la guía de entrevista, constando 10 ítems.

Resultados descriptivos: Como resultado, se pudo determinar que, como consecuencia de la pandemia el delito de fraude informático presentó un aumento de forma exponencial, siendo la mayoría de casos archivados debido a la falta de individualización del imputado lo cual demuestra la falta de eficacia en las investigaciones por parte del Ministerio Público pese a realizar las diligencias correspondientes para recaudar los suficientes medios probatorios, la falta de instrumentos tecnológicos, capacitación especializada, peritos calificados, cooperación institucional, normativa y logística, entre otros factores que causan el archivo de los casos en un alto porcentaje.

Conclusiones: Se concluye que las técnicas de investigación utilizadas por la fiscalía en la persecución del delito de fraude informático resultan ser ineficaces al no lograr la persecución del delito individualizando a los ciberdelincuentes.

Palabras claves: Fraude Informático, Cooperación Institucional, investigación, delito Informático, Ciberdelincuencia.

Abstract

General objective: Determine whether the investigation into the crime of computer fraud is being conducted effectively by the San Román Provincial Prosecutor's Office - Juliaca, 2024.

Methodology: The methodology is qualitative, with a basic study type, descriptive and interpretive research level, and a phenomenological research design. A non-probability convenience sampling procedure was used, including two Provincial Prosecutors and five Deputy Provincial Prosecutors at the San Román Provincial Prosecutor's Office in Juliaca. Data collection was conducted using an interview technique, and the research instrument was a 10-item interview guide.

Descriptive results: As a result, it was determined that, as a consequence of the pandemic, the crime of computer fraud presented an exponential increase, with the majority of cases being archived due to the lack of individualization of the accused, which demonstrates the lack of effectiveness in the investigations by the Public Ministry despite carrying out the corresponding procedures to collect sufficient evidence, the lack of technological instruments, specialized training, qualified experts, institutional cooperation, regulations and logistics, among other factors that cause the archiving of cases in a high percentage.

Conclusions: It is concluded that the investigative techniques used by the prosecutor's office in the prosecution of computer fraud are ineffective, as they fail to identify the cybercriminals.

Keywords: Computer fraud, crime investigation, cybercriminals.

Índice general

Índice Tabla

Índice Figura

I. INTRODUCCIÓN

En nuestro país, el delito de fraude Informático estos últimos años ha experimentado un aumento creciente, debido al mayor acceso a internet y la proliferación de dispositivos móviles de última generación, por lo que existen diversas modalidades de fraude informático y estas van evolucionando, desde el phishing, el skimming, suplantación de identidad y más.

Ante esta situación, la presente investigación se enfoca en analizar la eficacia de la investigación del delito de fraude Informático. Esta Fiscalía presenta muchas limitaciones, lo que ha generado el archivamiento del 90% de los casos y dificultades en su resolución.

El objetivo principal de esta investigación fue determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024. En donde se realizó un análisis cualitativo de la eficacia de la Investigación en esta Fiscalía y la creación de una Fiscalía Especializada con competencia Regional, como herramienta de resolución de conflictos.

De esta forma, la presente investigación se encuentra estructurada en seis capítulos:

En el capítulo I: Se abordó la introducción la cual contiene una exposición general sobre el tema que se viene investigando.

En el capítulo II: Se desarrolla el planteamiento del problema, el cual se evaluará la situación problemática en la investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca.

En el capítulo III: Se desarrolla la revisión de la literatura mediante antecedentes extranjeros, nacionales y regionales o locales, así como la construcción del marco teórico y conceptual.

En el capítulo IV: Se desarrolló el marco metodológico, en donde se describe el tipo, diseño, enfoque y el instrumento de recolección de datos para la presente investigación.

En el capítulo V: Se evaluaron los resultados de las entrevistas realizadas a los expertos del tema.

En el capítulo VI: El capítulo sexto se dedica al análisis de las discusiones, las cuales fueron construidas a partir de la revisión de los antecedentes y el procesamiento de los resultados, dándose a conocer conclusiones y recomendaciones; asimismo se mencionan las diferentes referencias bibliográficas y seguidamente los anexos.

Joselyn Karen Churata Chuquipalla / Dianeth Adelayda Quispe Machaca.

II. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

2.1. Situación problemática.

La investigación pertenece al área del derecho penal, en la línea de investigación del derecho Procesal Penal.

Recientemente el delito Informático se ha convertido en conductas delictivas que burlan los sistemas electrónicos, ya que en su mayoría son ocasionados por uso de la tecnología. Hasta la fecha el fraude informático ha continuado siendo el centro de los ciberdelitos, por lo que sigue siendo el más frecuente ya que tiene un alto costo económico, pero es relativamente fácil cometerlo, sobre todo debido al impacto económico y al crecimiento del comercio electrónico (Mayer & Oliver, 2020).

Además, según INTERPOL (2022), el delito informático posee un carácter transnacional, y esto hace que se dificulte la investigación, así como la persecución de los responsables por lo que los recursos económicos y humanos destinados a la investigación de delitos informáticos son insuficientes en muchos países. La rápida evolución de las tecnologías de la información y la comunicación dificulta que las leyes y los procedimientos judiciales se adapten de manera oportuna (EUROPOL, 2021).

Por lo que uno de los principales obstáculos es la carencia de conocimientos especializados en ciberseguridad por parte de jueces, fiscales y policías. Esta situación dificulta la comprensión de la complejidad de los delitos informáticos y limita la capacidad de realizar investigaciones efectivas (Estrada & Cano, 2024).

Por su parte, según el diario Oficial el Peruano la situación del delito informático en el Perú, registran datos sorprendentes:

En el Perú se registran más de 300 denuncias de delitos informáticos cada mes. Si bien en el 2018 se contaron con 2,878 denuncias, en el 2020 se observó una creciente con 4,162 denuncias llegándose a cerrar el 2022 con 5,420 denuncias por Fraude Informático, ciberdelitos denunciados ante la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú. Al igual que el año previo, los delitos informáticos más denunciados fueron el fraude informático y la suplantación de identidad. Además, en solo el primer mes del 2023 ya se han registrado 319 denuncias. El coronel PNP Luis Huamán Santamaría, jefe de la DIVINDAT, dijo a El Peruano que durante el año pasado se obtuvo un récord de 229 detenidos y que este año se espera mantener o elevar esta cifra. También destacó que el personal está capacitado en el manejo de evidencias digitales gracias a las capacitaciones que recibe frecuentemente, lo que ha permitido que -en solo un mes de este año- se haya detenido a 16 nuevos implicados en ciberdelitos. En noviembre del año pasado, en alianza con la Agencia Nacional de Policía de Corea del Sur, se inició el proyecto de cooperación sobre el fortalecimiento de capacidades de investigación de delitos cibernéticos por medio del laboratorio de análisis forense digital y dark web (Pichihua, 2023).

Es así que en la ciudad de Puno como hace mención la revista de derecho, también sufre un incremento consecutivo en los delitos informáticos, esto a razón de la desinformación, la constante evolución tecnológica y muchas veces por falta de conciencia, así también se considera como otra causa la vulnerabilidad en el sistema informático y ello trae como consecuencias a más víctimas a personas entre 27 a 59 años de edad en este tipo de delitos, este tipo de estudio nos proporciona una idea clara de la problemática en la ciudad de Puno, y nos señala el camino a seguir para hacer frente este a este desafío (Arapa et al., 2024).

Asimismo, basado en el conocimiento empírico, se tiene que la evolución de la tecnología no cesa, por lo que representa un desafío constante para las autoridades, siendo uno de ellos la Fiscalía, que deben mantenerse actualizadas, con las últimas técnicas de investigación. Se debe tomar en cuenta también que la coordinación entre las diferentes instituciones involucradas en la investigación de delitos informáticos (Policía, Fiscalía, Poder Judicial) puede ser deficiente, lo que generaría retrasos y obstaculización en la resolución de los casos.

2.2. Formulación del problema.

2.2.1. Problema general.

¿La investigación del delito de Fraude Informático se vienen realizando de forma eficaz en la Fiscalía de la Provincia de San Román – Juliaca, 2024?

2.2.2. Problemas específicos.

P.E.1:

¿Cuáles son las causas que dificultan la eficacia en la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024?

P.E.2:

¿La Fiscalía, cuenta con herramientas tecnológicas y recursos disponibles para la Investigación del delito de Fraude Informático?

2.3. Justificación.

El delito de fraude Informático no es ajeno al impacto de los conflictos generados, por el contrario, estos cobran mayor fuerza, en el tema, ya que

dentro y fuera de estas presentan realidades que hace necesario una adecuada investigación de delitos de fraude informático en la Fiscalía. Y a pesar de los esfuerzos del Ministerio Público y la Policía Nacional por investigar los delitos informáticos de manera inaplazables y urgentes, que coadyuven con la investigación y esclarecimiento de los hechos, así como la identificación del ciberdelincuente, los actos de investigación resultan insuficiente e ineficaces debido a diversos factores tales como la falta de personal capacitado, herramientas tecnológicas, anonimato del delincuente e inclusive la lentitud en cumplir con los requerimientos que el Fiscal a cargo realiza a las diversas compañías de internet, para recabar información, archivándose por ello las investigaciones quedando impune el delito (Valdivia, 2023).

Ahora en cuanto a la viabilidad de la investigación, se tiene que los delitos informáticos son perpetrados mediante el uso de herramientas digitales avanzadas, por lo que es indispensable que los investigadores encargados de abordar este tipo de delitos deben poseer, como mínimo, las mismas herramientas utilizadas por los delincuentes, es decir estar al mismo recurso superior, como software y hardware actualizado, etc. Toda vez que va a permitir realizar una lucha efectiva contra la ciberdelincuencia, en consecuencia, resulta necesario y urgente la adquisición de estas herramientas para enfrentar este tipo de delito con eficacia (Estrada, 2024).

La investigación se centrará en la provincia de San Román, distrito de Juliaca, donde será nuestro límite de investigación, para poder analizar los principales obstáculos y deficiencias en la investigación de delitos de Fraude Informático. Ello mediante una entrevista en la Fiscalía de la Provincia de San Román – Juliaca.

Ahora bien, para llevar una investigación penal particularmente en fraude informático, se vuelve increíblemente desafiante. Esto se debe al hecho de que este crimen ocurre a través del uso de dispositivos como una computadora, una tableta o un teléfono móvil. Por lo tanto, es difícil identificar un delincuente, que

a menudo disfruta del anonimato y modifica sus datos personales. Además, este crimen puede ser cometido desde cualquier parte del mundo ya que los crímenes en línea se realizan a través del uso de tecnologías digitales (Valdivia, 2023).

Por lo que la presente investigación del delito informático beneficia a la sociedad en general, ya que ayuda a combatir la ciberdelincuencia y a prevenir que se cometan más delitos. Haciendo énfasis (Ruiz, 2010) menciona que la fusión universidad y la investigación aporta resultados útiles, de hecho, cuando se critica a las universidades por realizar investigación, uno de los argumentos más comunes es que la mayor parte de su producción no se aplica, por lo que es inútil y en absoluto beneficiosa para la sociedad.

2.4. Objetivos.

2.4.1. Objetivo general.

Determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

2.4.2. Objetivos específicos.

O.E.1:

Analizar las causas que dificultan la eficacia de la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román – Juliaca.

O.E.2:

Determinar las herramientas tecnológicas y recursos que estén disponibles para los Fiscales en la Investigación de los delitos de fraude Informático.

2.5. Impacto de la Investigación

El impacto de la presente investigación radica en determinar la eficacia del proceso de la investigación del delito de fraude informático, relacionada a las causas, necesidades de los recursos humanos y tecnológicos, los que son más comunes.

El estudio realizado contribuirá al desarrollo del conocimiento sobre delitos informáticos en el contexto del ámbito peruano y regional. A su vez incluirá recomendaciones para la implementación de nuevas tecnologías, así como programas de capacitación para el personal fiscal.

En este contexto, la presente investigación busca proponer soluciones concretas que impacten positivamente en el Sistema Judicial y contribuya una mejor administración de justicia frente a los delitos de fraude informático en la provincia de San Román – Juliaca.

2.6. Alcances y limitaciones

Alcances

El alcance de la investigación se dio en la fiscalía de la Provincia de San Román-Juliaca periodo 2024, donde se aplicara un alcance descriptivo al analizar y detallar si se viene realizando de manera eficaz la investigación del delito de Fraude Informático en dicha jurisdicción, recopilando información proveniente de los fiscales la cual mediante el alcance interpretativo se llegara a comprender el significado de sus experiencias y desafíos en este proceso; identificando fortalezas y debilidades en la investigación lo cual permitirá plantear propuestas de mejora.

Limitaciones

En la presenta investigación se enfrentó a diversas limitaciones, tanto en la etapa de recolección como en la disponibilidad y calidad de las fuentes, todo ello debido a la sobrecarga laboral de los entrevistados y la escasez de fuentes bibliográficas limitó la profundidad del análisis. Dado que el fraude informático es un campo de constante evolución debido a los avances tecnológicos, los resultados podrían verse variados sino se actualizan.

III. REVISIÓN DE LA LITERATURA

3.1. Antecedentes de investigación.

Al revisar las fuentes físicas y virtuales se ha podido ubicar trabajos que guardan relación indirecta con cada una de nuestras variables, siendo estos valiosos aportes:

Internacionales

Ospina & Sanabria (2020), en Colombia, tuvieron como objetivo de estudio analizar el tema de la seguridad de la información frente a las amenazas cibernéticas que existen en el ámbito global realizando como revisión la situación actual que se vive en Colombia. Su metodología de investigación fue cualitativa, teórica, documental y descriptiva. Su resultado fue que a pesar de los esfuerzos que se realiza el país de Colombia este presenta importantes deficiencias ante las amenazas cibernéticas, las cuales se incrementaron durante la pandemia (COVID-19), por lo que es necesario promover políticas de seguridad que protejan la información personal de las personas así como la creación de diversas organizaciones que incorporen las reglas y procedimientos para gestionar la información, lo cual se abordara mediante la implementación de nuevas normativas sobre el uso del software, el impulso a las denuncias y la sanción de los delitos informáticos en respuesta a su evolución reciente.

Cuenca & Núñez (2024) en Ecuador, tuvieron como objetivo realizar un análisis documental sobre los delitos informáticos y el impacto en la seguridad jurídica. Para desarrollar su trabajo realizaron una descripción cuantitativa de los tipos de delitos informáticos que se cometieron desde los años 2018 hasta el 2023. En conclusión pese a haber fortalecido su marco jurídico para protegerse de los delitos informáticos, sigue enfrentando desafíos debido a la constante evolución digital , teniendo en cuenta que Ecuador cuenta con leyes

que penalizan diversos tipos de delitos informáticos, como acceso ilícitos de sistemas, sabotaje, entre otros, asimismo cuenta con la Ley Orgánica de Comunicación la cual protege los datos personales así como la divulgación ilegal de información, por ende Ecuador creo un entorno jurídico solido que ayuda a mantener confianza en las tecnologías digitales creando conciencia en la ciudadanía sobre la seguridad en línea.

Ponce (2024) en Ecuador, tuvo como propósito analizar los desafíos informáticos y sus respuestas legales en ecuador. Para lo cual adopto una metodología de investigación cualitativa con un nivel descriptivo realizando la investigación exhaustiva de la literatura ecuatoriana existente en donde se incluyeron libros especializados, artículos académicos sobre los diferentes tipos de delitos informáticos, características y herramientas disponibles para su prevención y sanción. Se concluyo que Ecuador carece de una legislación adecuada para combatir eficazmente los delitos informáticos, identificándose deficiencias tanto en la tipificación de estos delitos como en el reconocimiento de las actividades que los promueven por lo que la falta de protocolos de seguridad sólidos agrava aún más la vulnerabilidad de los usuarios ante los peligros informáticos.

Hernández et al. (2024) en Ecuador, tuvo como objetivo analizar la efectividad de las políticas implementadas para garantizar la seguridad cibernética en Ecuador. Su metodología de investigación es de tipo cualitativo, combinado con un análisis documental con entrevistas y cuestionarios, como métodos de recolección de datos se utilizaron las encuestas y revisión documentaria. Concluyendo que de forma mayoritaria el sistema de seguridad cibernética es poco eficaz debido a la falta de comunicación entre instituciones y entidades de ciberseguridad, asimismo la falta de capacitación en la personal evidencia la urgencia de destinar recursos a programas de formación continua. Por lo tanto, resulta fundamental desarrollar iniciativas de sensibilización y capacitación en ciberseguridad enfocadas en distintos sectores, con el objetivo

de concienciar a la sociedad sobre los peligros en el ámbito digital y ofrecer herramientas y competencias necesarias para proteger la información.

Ojeda et al. (2023) en Ecuador, tuvieron como objetivo estudiar los desafíos legales que atraviesa el país de Ecuador frente a los delitos informáticos y la importancia de cómo prevenirlos. La metodología utilizada fue de tipo Mixta Cualitativa -Cuantitativa obteniendo información cerrada con la finalidad de medir actitudes hacia el objeto de estudio, información abierta para poder analizar la diversidad de ideas sobre el tema que se investiga asimismo el instrumento utilizado fueron las entrevistas. Llegando a la conclusión de que el ordenamiento jurídico ecuatoriano necesita la inclusión de nuevas figuras jurídicas que penalicen más las acciones u omisiones que se desarrollan a través de mecanismos informáticos, también resalta, la necesidad de capacitar al personal judicial y bancario para que puedan abordar de manera más eficaz estos crímenes.

Nacionales

Arellano & Galindo (2022) su objetivo fue analizar las insuficiencias normativas observadas en el tipo penal de fraude informático en Lima entre los años 2019 y 2021, contemplado en el artículo 8 de la Ley N° 30096. Se empleó una metodología cualitativa básica, de carácter no experimental, para la cual se revisaron a fondo publicaciones jurídicas relevantes y se realizaron entrevistas dirigidas a una población. Concluyendo que el fraude informático se define como una acción deliberada cometida mediante el uso de tecnologías de la información y la comunicación (TIC). Asimismo, se ha identificado que la tasa de criminalidad relacionada a este delito se ha triplicado en los últimos cuatro años. Sin embargo, la normativa vigente, presenta importantes deficiencias legales, destacando la dificultad para identificar al autor del delito y la falta de protección adecuada para la víctima, quien queda vulnerable frente al agresor.

Malca (2023) se buscó analizar el efecto de la persecución penal eficaz en la investigación inicial de casos de Fraude informático en el Callao durante el 2022. La metodología utilizada fue de enfoque cualitativo, tipo básico, con un diseño fenomenológico, aplicando como instrumentos una guía de entrevista realizada a 10 personas especialistas en el tema. En conclusión, la encuesta revela que los encuestados manifiestan la existencia de una ineficacia penal en la etapa de investigación preliminar del delito de Fraude informático, debido a la falta de fiscalías especializadas en Ciberdelincuencia en el distrito fiscal del Callao, lo que ha derivado en investigaciones insuficientes realizadas por las Fiscalías Corporativas.

Arista & Castro (2024) tuvieron como objetivo analizar el delito de Fraude Informático a partir de una revisión bibliográfica especializada en el contexto de la Ley N° 30096. En su metodología utilizada, resalto el enfoque cualitativo, con tipo básico y diseño de investigación de teoría fundamentada. Concluyendo que existe un vacío normativo con relación a los avances de la tecnología por lo que la legislación peruana debería de adquirir herramientas que el ayuden a combatir el fraude informático, como es el establecimiento de alianzas internacionales las cuales ayudaran a combatir el delito de Fraude informático de manera más factible.

Valentín (2022) se centró en determinar los elementos que contribuyen al archivo de las investigaciones preliminares por el delito de Fraude informático en la jurisdicción de Trujillo durante el año 2021, considerando factores como la complejidad de las pruebas digitales, las limitaciones de los recursos investigativos y la falta de especialización de los operadores de justicia. La metodología aplicada era cualitativa, tipo básica, de alcance descriptivo-interpretativo, analizando 10 carpetas fiscales archivadas por el delito de fraude informático utilizando la entrevista y recolección documentaria como instrumentos de recolección de datos. Se concluyo que los factores de

incidencia para el archivo de las investigaciones preliminares fue la falta de identificación del autor, falta de elementos de convicción para imputar el delito, la falta de logística que ayuden a recabar los elementos de convicción.

Quispe (2020) el propósito de este estudio es determinar las causas del archivo de las investigaciones en fraude informático en la región La Libertad en 2019, demostrar que se archivan debido a la falta de evidencia y porque es difícil identificar a los responsables. La metodología utilizada es descriptiva-analítica, encontrando soluciones a la problemática analizada, comparando lo que la norma y la doctrina señalan sobre el archivo de investigaciones. Concluyendo que las empresas financieras y telefónicas no cooperan con la investigación de los delitos de fraude informático dado que brindan una deficiente y limitada colaboración asimismo **l**a escasez en cuanto a equipamiento, instalaciones, personal y habilidades dificultan el desempeño de la DIVINCRI y del Ministerio Público.

Locales o regionales

Saulo (2019) la finalidad de la investigación es analizar los riesgos y políticas de seguridad de información, la cual se lleva cabo en la oficina de tecnología de información (OTI) - UNAP 2018. La metodología utilizada fue un diseño experimental basado en encuestas. Concluyendo que la Oficina de Tecnologías de la Información de la OIT enfrenta un promedio de 12 riesgos informáticos que ponen en peligro la seguridad de sus datos. Ante esta situación, se hace necesario que el Estado refuerce las medidas de seguridad para garantizar la confiabilidad, integridad y disponibilidad de la información, con el objetivo de salvaguardar los activos digitales de la organización.

3.2. Bases teóricas

3.2.1 Fraude Informático

3.2.1.1 Definición del Fraude Informático

En nuestra normativa, el delito de Fraude informático se encuentra tipificado en el artículo 8 de la ley N° 30096 (Ley de delitos Informáticos) la cual establece y tipifica como delito, la acción de introducir, modificar, eliminar o dañar datos informáticos, así como interferir en el funcionamiento de sistemas informáticos, con el objetivo de obtener un beneficio económico propio o de terceros, a través de medios tecnológicos. Acurio del Pino, (2016) define al Fraude informático como, el delito que es cometido mediante la utilización de medios tecnológicos o el uso de un sistema informático para que el activo patrimonial se transfiera al infractor o una tercera persona, tomando en cuenta que este tipo de delitos se cometen solamente de mamera virtual debido a que no es posible efectuarlos en forma física.

Por lo que el delito de fraude informático se caracteriza por causar un perjuicio económico a través de la manipulación de datos y/o programas. Sin embargo, este concepto va más allá de las acciones consumadas, abarcando también conductas preparatorias y tentativas, como el phishing y el pharming, los cuales suelen utilizarse en el contexto de operaciones bancarias (Mayer y Oliver, 2020).

3.2.1.2 Modalidades del fraude Informático.

El delito de fraude informático ha ido evolucionando en la misma medida que la tecnología, los ciberdelitos comúnmente se dan mediante el uso de medios digitales - tecnológicos, empleando el celular u otras formas digitales, siendo uno de los medios más viables para la ejecución de esta conducta punible (Wuerges & Borba, 2014).

Por lo que, debemos de conocer las distintas modalidades y métodos que utilizan los ciberdelincuentes para la realización de estos delitos informáticos, Núñez & Carhuancho (2020) describen cuatro modalidades:

(1) El Phishing: la cual es una sofisticada técnica que se basa en engañar a las personas haciéndoles creer que están interactuando con una entidad legítima. Esta se lleva a cabo mediante correos electrónicos falsos y sitios web clonados, los ciberdelincuentes intentan sustraer información confidencial de las cuentas bancarias de sus víctimas.

(2) Vishing: Esta modalidad consiste llamadas telefónicas en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima e inducir a que el usuario abra una página web controlada por el atacante.

(3) Rasomware: La cual trata sobre el desfalco de suma de dinero en cantidades modestas y por lo general se repite de una cuenta bancaria a otra. Es decir, los delincuentes roban a sus víctimas en pequeñas sumas progresivas para no causar alarma, poniendo software malicioso en los dispositivos de la víctima, en cuyo caso el monto crocante será relativamente pequeño, pero al afectar a un gran número de personas, los criminales obtendrán miles de millones.

(4) Sim swapping: Esta modalidad es llamada también suplantación de SIM o duplicado de SIM, donde el delincuente cibernético se apodera fraudulentamente de la cuenta personal o financiera de una persona al secuestrar el número de teléfono de esa persona. Este proceso implica que los delincuentes engañen a las compañías de teléfono para que transfieran el número de la víctima a una nueva tarjeta SIM en la que ellos mismos tengan control.

Asimismo (Rextie, 2022) señala otras modalidades tales como:

1. Thief Transfer: El cual es un tipo de fraude donde los ladrones roban celulares y los utilizan para extraer dinero de las cuentas bancarias de las víctimas, acceden a las aplicaciones de banca móvil y, si no pueden, se hacen pasar por la víctima para pedir dinero a todos sus contactos. La mejor forma de evitar este fraude es manteniendo protegida la tarjeta SIM con un PIN. De esa forma, si alguna persona sufre del robo de su celular, los ladrones no podrán usar su información bancaria, aunque saquen tu tarjeta SIM y la pongan en otro teléfono.
2. Smishing: En esta modalidad los criminales intentan "pescar" la información personal o dinero a través de mensajes de texto, donde remiten mensajes engañosos, a menudo con premios falsos o alertas de problemas en tus cuentas, para que ingreses en los enlaces o compartas tus datos.

3.2.2 Investigación del delito de fraude informático

3.2.2.1 El Ministerio Público

En materia penal el Ministerio Público es un organismo constitucional autónomo, dado que actúa en defensa de los intereses de la sociedad, cuando estos se ven perturbados por la comisión de un hecho delictivo imponiendo un castigo a los culpables, su función es vigilar la aplicación de las leyes de procedimientos que son de orden público (García, 1964).

Asu vez, (Moras Mom, 2004) define al Ministerio Público como:

> “Un órgano jurídico procesal instituido para actuar en el proceso penal, como sujeto público acusador, en calidad de titular de la actuación penal oficiosa” (p.45)

Por lo que, esta entidad, se encarga de dirigir las investigaciones de los delitos de acción pública los cuales pueden ser de conocimiento público, pedido de parte o por acción popular, realizando la recolección de pruebas de cargo y de descargo para poder determinar la participación del autor materia de delito o la inocencia del imputado, así como también utiliza medidas de protección para proteger a las víctimas o testigos.

Adicionalmente, se debe tener en cuenta que el Ministerio Publico no es el único órgano especializado en la investigación por delitos de Fraude informático sino que en el 2005 se creó la División de Investigación de Alta Tecnología (DIVINDAT) el cual se encuentra a cargo de la Policía Nacional del Perú quienes tienen la función de prevenir, combatir, investigar y denunciar los delitos Informáticos que atenten contra la libertad, el patrimonio, la seguridad pública, la defensa y seguridad nacional, la propiedad industrial entre otros los cuales son cometidos mediante la utilización de tecnologías, llegando a recabar medios probatorios suficientes para imputar el delito todo ello bajo la supervisión de un fiscal (Armestar & Toche, 2023).

Posteriormente en el 2020, mediante la Resolución de la Fiscalía de la Nación N° 1503-2020-MP-FN, se creó la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con única sede en Lima pero teniendo competencia a nivel nacional la cual emplea mecanismos tecnológicos para rastrear la evidencia en estos crímenes, por lo que cualquier fiscal a nivel nacional que tenga una investigación en delitos informáticos cometidos mediante la sustracción de datos de las tarjetas de crédito y ahorro, así como requerir orientación de las principales diligencias que tendrá que llevar a cabo para recaudar los suficientes medios probatorios en la investigación, puede inscribirse en plataforma del UCIVER a efectos de obtener el apoyo técnico de la unidad quienes investigaran el ciberespacio levantando el secreto de las

comunicaciones, solicitando información a un proveedor internacional como Facebook entre otros.

Asimismo, el ministerio público con el fin de dirigir la investigación y proporcionar una base sólida para el juicio, elabora su teoría del caso, la cual funciona como hipótesis fáctica, jurídica y probatoria. Dicha teoría del caso se construirá a partir de las pruebas disponibles, sus deducciones y el tipo penal aplicable, y se somete a evaluación en el juicio oral, culminando en su validación o refutación mediante la sentencia (Benavente, 2011).

3.2.2.2 Teoría del Delito

Busca determinar si un echo configura como delito o no, para poder ser investigado, esta teoría cuenta con cuatro calificativos, el primero es la conducta, la cual puede ser una acción o omisión; es típica por que incluye los elementos que fundamentan una figura delictiva dividiéndose en tipicidad subjetiva y objetiva, también es antijuridica, esto quiere decir que es contrario al derecho; asimismo es culpable por que se adjudica al autor el hecho delictivo, por lo que no puede existir la comisión de un delito propiamente, ante la inconcurrencia de uno o más elementos (Mezger, 1935).

Teniendo como base la configuración jurídica de un delito, con los elementos que la componen analizaremos el delito de Fraude informático el cual se caracteriza por la sustracción, transferencia o apoderamiento de un bien a través de la manipulación informática siendo un delito de resultado mediante un acceso ilícito atentando contra la integridad de datos para su consumación.

En el fraude informático el sujeto activo y el sujeto pasivo pueden llegar a ser cualquier persona, el bien jurídico protegido es el patrimonio; la tipicidad objetiva es “el que procura para si o para otro un provecho ilícito en perjuicio de un tercero” causando un perjuicio patrimonial al sujeto pasivo; en cuanto a la tipicidad subjetiva esta exige dolo en su accionar en la medida que se

destina a obtener un provecho ilícito implicando la exigencia de un dolo directo para la consumación del tipo penal (Vega & Arévalo, 2022).

3.2.2.3 Teoría de las Oportunidades Criminales

La teoría de las oportunidades criminales sostiene que el delito se materializa cuando se presentan circunstancias favorables para su comisión (Cohen & Felson, 1979) por lo que ciertos delitos como el fraude informático, se ven facilitados por la falta de vigilancia, la disponibilidad de víctimas y la escasa reacción de las autoridades en palabras simples, el crecimiento del acceso a la tecnología y la falta de educación digital pueden generar un entorno propicio para este tipo de delito.

3.2.3 Antecedentes legales

3.2.3.1 Legislación Nacional: LEY N°30096

En nuestro sistema legislativo el delito de Fraude informático ha ido evolucionando desde el antiguo hurto telemático hasta su regulación actual en la Ley 30096, lo cual refleja la adaptación del derecho penal peruano a los desafíos planteados por el desarrollo de las tecnologías de la información y las comunicaciones.

La Ley de Delitos Informáticos (Ley 30096), modificada por la Ley 30171 en Perú, prevé en su artículo 8 el delito de fraude informático estableciendo que este tipo penal es cometido cuando el perpetrador a propósito y sin autorización, manipula los datos de una computadora o altera el funcionamiento de un sistema informático para obtener un beneficio personal o para un tercero, llegando a causar un perjuicio patrimonial a otra persona, este puede ser castigado con una pena de prisión de entre 3 y 8 años estableciéndose como agravante las situaciones donde se afecte el patrimonio del Estado del cual se encontraría destinado a fines asistenciales

o a programas de apoyo social, en este caso la pena pasará a ser no menor de cinco ni mayor de diez años; en resumen, cualquier acción como cambiar, eliminar, copiar o interferir en la información de una computadora con la intención de estafar a alguien está considerada un delito grave en Perú por lo que esta ley busca proteger a las personas y empresas de los daños que pueden causar los ciberdelincuentes quienes serán sancionados con una pena (Armestar & Toche, 2023).

Asimismo, gracias a la influencia del Convenio de Budapest, el derecho penal peruano se fue adaptando a los desafíos legales que nos trae el desarrollo de las tecnologías de la información y las comunicaciones mostrando una evolución en su legislatura la cual se dio a través de diversas leyes y decretos como La Ley Nº 27269 la cual fue la ley pionera en la materia ya que se reconoció la validez jurídica de las firmas y certificados digitales, sentando de esta manera bases para el desarrollo del comercio electrónico y la autenticación en línea, esta ley fue complementada por la Ley Nº 27291, la cual modifico el Código Civil para permitir que se puedan manifestar voluntades a través de medios electrónicos, ampliando así las posibilidades de contratación y comunicación en el entorno digital.

La lucha contra el crimen organizado también ha impulsado la creación de leyes relevantes. La Ley Nº 27697 la cual fue expresamente modificada por la Ley Nº 30096, sobre delitos informáticos, donde se tipifica y sancionan diversas conductas ilícitas en el ámbito digital, como el acceso no autorizado a sistemas informáticos, el daño a datos y el fraude informático, entre otros, en esta ley se otorgan facultades a los fiscales para poder levantar el secreto de las comunicaciones y secretos bancarios en casos excepcionales empero esta solicitud tiene que aprobada el juez. Asimismo, la Ley Nº 30077 fortaleció el marco legal contra el crimen organizado, abarcando también las actividades ilícitas que se valen de medios informáticos.

La protección de datos personales es otro aspecto fundamental abordado por la legislación peruana. La Ley Nº 29733 establece un marco legal para la protección de datos personales, garantizando el derecho de los ciudadanos a controlar y acceder a su información personal. Esta ley es importante para preservar la privacidad y seguridad de los datos en un entorno digital.

El Decreto Supremo Nº 081-2013-PCM aprobó la Política Nacional de Gobierno Electrónico 2013-2017, la cual busca modernizar la administración pública y mejorar los servicios ofrecidos a los ciudadanos mediante la utilización de tecnologías de la información y la comunicación.

La Resolución Nº 2432-2016-MP-FN aprueba las Cláusulas de Confidencialidad y de Protección de Datos Personales, estableciendo lineamientos para el tratamiento de información sensible en el Ministerio Público. Asimismo, la Resolución Nº 2189-2018-MP-FN aprueba el Reglamento Interno para el Acceso y uso de Herramientas y Servicios Informáticos en el Ministerio Público, garantizando la seguridad y confidencialidad de la información manejada por esta institución.

Finalmente, con la Resolución Nº 1503-2020-MP-FN se crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con la cual se busca fortalecer la capacidad de investigación y persecución de estos delitos en el ciberespacio.

Por lo que, este conjunto de leyes y decretos refleja el compromiso del estado peruano con la protección de la información y la lucha contra la ciberdelincuencia. Sin embargo, se debe destacar que este es un campo en constante evolución, por lo que es necesario mantener una actualización constante de la legislación adaptándola a las nuevas amenazas y desafíos tecnológicos.

3.2.3.2 Legislación internacional: El convenio de budapest

Es el primer convenio internacional, creado por los países miembros de Europa firmado el 23 de noviembre del 2001 y entro en vigencia internacional el 2004, siendo participe el Perú en el año 2019 mediante la Resolución Legislativa N° 30913 y ratificado por el Ejecutivo con Decreto Supremo N° 010-2019-RE a fin de fortalecer la seguridad digital en el país, dicho convenio se encuentra dedicado exclusivamente a combatir los delitos cometidos a través de internet, su objetivo principal es facilitar la cooperación internacional en la lucha contra la ciberdelincuencia, compartiendo información sobre leyes y procedimientos entre países, gracias a este convenio, se establecieron normas globales para regular el ciberespacio y proteger a los ciudadanos de los delitos informáticos (Barrios & Vargas, 2018).

Asimismo, este convenio trae una serie de importantes beneficios los cuales serán aprovechados cuando se eliminen las diferencias tecnológicas existentes entre cada Estado Parte, llegándose a contar con la cooperación de cada uno de ellos para el intercambio de conocimientos y recursos; por lo que, Tenorio (2018) hace mención de algunos beneficios que trae consigo el Convenio de Budapest para lo cual se tiene los siguientes:

- Establecer un marco legal común para combatir la ciberdelincuencia y proteger a sus ciudadanos.
- Fortalecer sus leyes nacionales existentes en materia de ciberseguridad.
- Garantizar el uso seguro y responsable de las tecnologías de la información.
- Prevenir y sancionar los delitos que afecten a los sistemas y datos informáticos.

- Cooperar de manera eficiente para identificar, investigar y castigar a los cibercriminales.
- Fomentar la capacitación y el intercambio de conocimientos en ciberseguridad.

En tanto, se puede afirmar que este es el único convenio internacional vinculado a los ciberdelitos el cual trata de dar soluciones a lucha contra los delitos informáticos y de Internet; mediante la persecución a los ciberdelincuentes y cooperación de conocimientos entre países miembros para poder regular el Ciberespacio (Cavada, 2020).

3.3. Marco conceptual

Fraude Informático. Son actos delictivos realizados mediante la utilización de medios tecnológicos que causan perjuicios a una o varias personas.

Legislación Nacional. La legislación nacional está compuesta por una jerarquía de normas jurídicas, donde la Constitución es la norma suprema, cada norma inferior encuentra su validez en la norma superior.

Phishing: Se le denomina a la estrategia de fraude electrónico con la cual se busca obtener información personal o bancaria mediante engaños persuasivos por medios digitales.

Ministerio Público: Es el Órgano estatal que representa el interés público y la legalidad, investigando delitos y ejerciendo la acción penal.

Delitos Informáticos: Son las conductas ilegales que afectan sistemas de información o tecnologías de la comunicación.

Convenio de Budapest: Es el Tratado internacional que establece normas para combatir los delitos informáticos y coordinar esfuerzos de justicia transnacional mediante la cooperación de los países miembros.

Eficacia de la investigación: Es la capacidad de una investigación para lograr cumplir los objetivos establecidos de manera eficiente y exitosa ya que se encarga de medir cuán bien se logra lo que se propone, considerando tanto la calidad como la eficiencia en el proceso.

Limitaciones de la investigación: Son los factores o circunstancias que restringen o condicionan el alcance, la profundidad o los resultados de un estudio.

Herramientas tecnológicas: Son recursos, aplicaciones o sistemas que nos ayudan a realizar tareas de manera más eficiente y efectiva en diversas áreas de la vida.

Recursos disponibles: Son todos aquellos elementos que se pueden utilizar para llevar a cabo una actividad, y su correcta gestión es clave para el éxito de cualquier iniciativa.

IV. MARCO METODOLÓGICO

4.1. Tipo y Nivel de Investigación.

Enfoque.

La investigación adopto un enfoque cualitativo, dado que esta se centra en las evidencias, buscando una explicación detallada de un fenómeno para entenderlo a fondo y poder explicarlo utilizando los métodos y herramientas propias de su campo de estudio (Sánchez, 2019).

Tipo.

El presente proyecto se fundamenta en una investigación de tipo básica, ya que su propósito es generar y recopilar información que brinde un aporte al conocimiento existente, con el único fin de ampliar la comprensión sobre el tema (González, 2009).

Nivel.

El nivel de la investigación es descriptivo e interpretativo, ya que se describe detalladamente todas las características y dimensiones del fenómeno entendiendo como se manifiesta de forma natural, asimismo, se analizan las interpretaciones que los participantes atribuyen al objeto de estudio (Castillo López et al., 2023).

4.2. Diseño de la Investigación

En el desarrollo de la presente tesis se utilizó el diseño de investigación fenomenológico, pues este se basa en la recolección de experiencias vividas para posteriormente brindar una reflexión profunda sobre dichas experiencias dando como resultado la redacción y reflexión final lo cual nos ayudara a determinar las deficiencias existentes en la investigación de los delitos por Fraude informático (Fuster, 2019).

4.3. Matriz de operacionalización de categorías.

CATEGORÍA(S) DE ESTUDIO	DEFINICIÓN CONCEPTUAL	SUB CATEGORÍAS	DEFINICIÓN CONCEPTUAL	UNIDADES DE ANÁLISIS
Eficacia en la Investigación de los delitos por Fraude informático	La investigación de delitos de fraude informático es un proceso complejo que enfrenta diversas deficiencias, la eficacia implica el uso exitoso de técnicas y herramientas adecuadas para recopilar evidencia digital, identificar a los	Fraude informático Investigación Fiscal Capacitación	Según el autor este delito se caracteriza por causar un perjuicio económico a través de la manipulación de datos y/o programas (Mayer & Oliver, 2020). Es una previa audiencia preliminar, donde se evalúan diversos aspectos y se recaudan elementos de convicción (Insignares, 1998). Mecanismo diseñado para instruir a los nuevos empleados sobre las competencias esenciales requeridas para realizar sus funciones laborales de manera efectiva	Entrevista a fiscales de la Provincia de San Román – Juliaca.

	responsables y llevarlos ante la justicia(Valdivia, 2023).	Instrumentos Tecnológicos	(Dessler & Varela, 2011) Facilitan el desempeño de tareas y procesos dentro de una entidad ayudando a realizar tareas complejas (García et al., 2020).	
		Normatividad	Ayuda a mantener el orden social estableciendo un conjunto de leyes y reglas que determinan qué acciones son aceptables y cuáles no (Aguirre, 2021).	

4.4. Procedimiento de muestreo.

4.4.1. Población

En la presente investigación, la población estudiada está conformada por fiscales provinciales y fiscales adjuntos los cuales laboran en la Fiscalía de la Provincia de San Román – Juliaca, responsables de investigar el delito de Fraude informático.

4.4.2 Muestra

La muestra se definió mediante un muestreo no probabilístico por conveniencia, seleccionando a los participantes según su accesibilidad y disponibilidad. Este enfoque es útil cuando no se puede acceder a toda la población. Se incluirán 02 fiscales provinciales y 05 fiscales adjuntos activos en la jurisdicción.

4.5. Recolección y análisis de la información.

4.5.1. Técnica

La técnica establecida para el desarrollo de esta investigación es la entrevista, ya que es una técnica que nos permite recolectar datos por medio de preguntas diseñadas en un esquema ordenado. Hernández et al., (2014), afirma que la entrevista faculta a que el entrevistado pueda obtener un margen amplio en sus respuestas.

4.5.2. Instrumento

Para la presente investigación se aplicó una guía de entrevista como técnica de recolección de datos. La cual consta de una serie de preguntas estructuradas, que ayuda a obtener la opinión de los participantes sobre el tema en estudio; facultando al entrevistado a obtener un margen amplio de respuesta (Baena, 2017).

Tabla 1

Estructura de matriz de validación

Nombre del experto (a)	**DNI**	**Grado Académico**	**Evaluación** Cumple/ No cumple
Mg. Wilfredo Flores Espillico	013453559	Magister en derecho constitucional	Cumple
Dr. Luis Ruben Yanqui Machaca	73813424	Abogado	Cumple
Dra. Judy del Rosario Condori Luque	70082632	Magister	Cumple

4.6. Aspectos éticos y regulatorios.

Para Gonzales (2022), la ética juega un papel importante en la investigación cualitativa la cual se fortalece con la participación de expertos académicos como de personas sin formación académica específica, asimismo la colaboración de individuos provenientes de diversas instituciones y organizaciones que realizan investigaciones, contribuye a una mejor comprensión de los desafíos y las implicaciones de la investigación cualitativa, siendo relevante los enfoques éticos para guiar este proceso y asegurar la integridad de la investigación.

En el ámbito de la investigación científica y tecnológica, los aspectos éticos son cruciales, los cuales se rige por principios y valores que orientan la observación y análisis de las conductas en el ámbito científico, desde una perspectiva específicamente humana (Universidad Tecnológica de Investigación Científica - UTIC, 2019).

En la presente investigación el consentimiento informado será nuestro principio ético y esencial, a la cual nuestros entrevistados tendrán acceso ya que cuentan con el derecho inalienable a la libre manifestación de sus ideas y opiniones decidiendo libremente si desean participar o no.

V. RESULTADOS

5.1. Descripción de los resultados.

En esta sección se examinarán los resultados recabados a partir del instrumento planteado el cual es la guía de entrevista, dirigida a fiscales especializados.

En lo que respecta a las entrevistas, se plantearon 10 interrogantes a un grupo de siete fiscales entre los cuales dos son Fiscales Provinciales expertos en la investigación del delito por aproximadamente 6 años y cinco Fiscales Adjuntos los cuales son expertos en la investigación del delito por aproximadamente 5 años, los fiscales pertenecen a la Fiscalía de la Provincia de San Román – Juliaca, quienes desde su punto de vista han permitido que se logre determinar nuestro objetivo general el cual es, determinar si se viene realizando de manera eficaz la investigación de delito de Fraude informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

Por consiguiente, las preguntas se formularon en base a nuestros objetivos planteados, conforme a lo detallado en lo siguiente:

Objetivo General: "Determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024", encontramos:

Tabla 01. *¿Cuántas denuncias por el delito de fraude informático ingresan mensualmente a su despacho y cuáles serían los factores de su comisión?*

ENTREVISTADO	RESPUESTA
E1	Mensualmente ingresan alrededor de seis denuncias y los factores están relacionados al desarrollo de la tecnología.
E2	Mensualmente ingresan de 5 a 7 denuncias en promedio y los factores del fraude informático son los anonimatos en las redes sociales.

E3	En promedio ingresan siete denuncias mensualmente, en donde utilizan los avances tecnológicos enviando links para obtener datos personales o solicitar que se les deposite a un número de cuenta.
E4	Unas cinco aproximadamente, teniendo como factores el uso de las tecnologías.
E5	La cantidad de denuncias que ingresan mensualmente son en promedio cinco de las cuales los factores de su comisión son el avance y uso de tecnologías en las transacciones financieras como el uso de yape, plin, el comercio electrónico de tarjetas de crédito, entre otros.
E6	Solamente en mi despacho ingresarían al mes unas 3 a 4 veces, no más, ello porque el Turno se hace cada 28 días y los Factores de su comisión los más comunes son las clonaciones de tarjeta, uso indebido de las tarjetas.
E7	Ocho denuncias mensualmente, aproximadamente.

Elaboración propia

Interpretación: En la tabla 1, los fiscales en su gran mayoría señalan que mensualmente a su respectivo despacho ingresan aproximadamente entre 3 a 7 denuncias del delito de Fraude informático teniendo como factor común el avance tecnológico como el uso de transacciones financieras (Yape y Plin), el anonimato en redes sociales, el envío de enlaces fraudulentos para obtener datos personales y la conación de tarjetas entre otros.

***Tabla 02**. ¿Cuál es la proporción de casos de fraude informático que se archivan frente a los que avanzan a la etapa de formalización?*

ENTREVISTADO	RESPUESTA
E1	La mayoría son archivados, de diez casos uno se formaliza.
E2	De diez casos solo uno pasa a formalización.
E3	Del 100 % solo el 10 % se formaliza y el resto se archiva.
E4	De cinco denuncias unas tres o cuatro se archivan.
E5	La proporción de casos es de 1 a 5, uno es el que prospera y cuatro se archivan.
E6	Particularmente todos los casos que me han entregado caso todos se han archivado al 100%.
E7	Se archivarán entre 80 y 90 %.

Elaboración propia

Interpretación: En la tabla 2, la mayoría de nuestros entrevistados coinciden que entre el 80 y el 90% de las denuncias terminan archivándose, teniéndose solo una pequeña fracción aproximada del el 10% de denuncias que llegan a pasar a una etapa de formalización.

Objetivo Especifico uno: "Analizar las causas que dificultan la eficacia de la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román - Juliaca", encontramos:

Tabla 03. *¿Cuáles son las diligencias necesarias para la investigación del delito de fraude informático?*

ENTREVISTADO	RESPUESTA
E1	El levantamiento de secreto bancario y comunicaciones, los IP de los sistemas informáticos y el peritaje informático, siendo esta la que más demora.

E2	La declaración de la agraviada, solicitar las IPS, levantamiento del secreto bancario y de las comunicaciones son las que demoran más tiempo.
E3	En principio la declaración del agraviado, posterior a ello la localización de la dirección IP y la que más suele demorar es el levantamiento del secreto bancario o levantamiento del secreto de las comunicaciones
E4	Toma de declaraciones, solicitud de video vigilancias, Levantamiento del secreto bancario y de las comunicaciones (siendo esta la que más demora)
E5	La principal diligencia propiamente es recabar el extracto financiero de los depósitos, las capturas de pantalla, los extractos bancarios o también información de las entidades financieras y la que más demora es el levantamiento del secreto bancario
E6	Y las diligencias necesarias serian el LSC, LSB que en algunos casos el Juzgado te suele demorar.
E7	Las diligencias necesarias serían más de cuestión tecnológica

Elaboración propia

Interpretación: En la tabla número 3, los entrevistados coincidieron en que las investigaciones del delito de Fraude informático son complejas, teniendo como primera diligencia necesaria la declaración del agraviado, con la cual se dará inicio a la investigación para posteriormente solicitar las diligencias que más tiempo demoran en recabarse como el levantamiento del secreto bancario y de las comunicaciones, los IPS de los sistemas informáticos y el peritaje Informático.

Tabla 04. *¿Cuáles son las principales limitaciones que enfrenta, en la etapa de la investigación Preliminar por el delito de fraude informático?*

ENTREVISTADO	RESPUESTA
E1	Demora en la obtención de datos y no contar con un equipo especializado.
E2	La sobrecarga procesal y la falta de capacitación.
E3	La falta de capacitación necesaria, tanto personal fiscal como administrativo para poder investigar este delito, así como falta de especialistas tales como ingenieros en sistemas, peritos especializados, etc.
E4	Falta de tecnología para ubicar a los responsables del hecho delictivo.
E5	Las principales limitaciones son el tema tecnológico, esto es propiamente tener equipos necesarios que permitan conservar la evidencia para ello se debería de contar con una oficina de peritajes especiales para poder peritar teléfonos. Recabar información de las cuentas bancarias. No contar con peritos especializados que nos permitan establecer algunos temas técnicos respecto al fraude informáticos ya que las empresas únicamente nos remiten informes técnicos de las cuales nosotros no sabemos qué información nos están remitiendo entonces necesitamos una explicación conceptual respecto a ello.
E6	Primero el personal capacitado. Segundo, que los Juzgados no suelen otorgar el LSB, LSC, porque el monto de la cuantía no es mucho, entonces no le dan relevancia.

	Tercero, que no hay suficientes medios como aparatos tecnológicos, y Recursos Humanos. Cuarto, que en el M.P los peritos son limitados al menos debería haber uno o dos peritos.
E7	En este despacho falta de tecnología.

Elaboración propia

Interpretación: En la tabla 4, respectos a las limitaciones que se enfrentan para poder investigar en la etapa de la Investigación Preliminar, en su gran mayoría los entrevistados señalaron que la carencia de herramientas tecnológicas como laboratorios de peritaje forense para teléfonos, equipos especializados de peritaje, la falta de capacitación en el personal genera falta de dominio de investigación, escasez de personal especializado como Ingenieros de Sistemas y la carga procesal generan un escenario en el que la impunidad de estos delitos se vea favorecida al no lograr identificar plenamente a los responsables del hecho delictivo del Fraude Informático.

Tabla 05. *¿Encontró limitaciones en el marco normativo actual que dificulten su labor como fiscal en la investigación del delito de fraude informático? Si es así, ¿podría mencionar cuáles son esas limitaciones?*

ENTREVISTADO	RESPUESTA
E1	No, las herramientas normativas existen, el problema está en la recaudación de los elementos de convicción.
E2	No, no tiene limitaciones.
E3	No, la norma es clara respecto a lo que indica por ese lado no existe una limitación por ende no podría mencionar ninguna.
E4	No, no encontré limitaciones.

E5	Si bien no he visto un tema de limitación propiamente dentro de la ley especial, pero sí respecto a recabar evidencia esto es muchas veces las personas agraviadas no permiten el acceso a su cuenta bancaria y es razón para poder nosotros solicitar el levantamiento de secreto bancario pero esto no se puede realizar en contra de los agraviados únicamente en contra de los investigados o imputados en este sentido la norma procesal no establece o posibilita en este caso ingresar a cuenta bancaria de los agraviados este es un tema que dificulta la investigación se debería dotar al ministerio público para que pueda tener acceso a esto y así de oficio previamente iniciar con estas investigaciones.
E6	Claro, que para este tipo de investigación el LSC no sea una limitación por la cuantía, debería a ver una modificatoria en ese aspecto.
E7	El tipo penal está escrito de una manera maravillosa, es decir no hay limitaciones en el marco normativo.

Elaboración propia

Interpretación: En la tabla 5, los entrevistados señalan que el marco normativo no presenta limitaciones por lo que es clara y precisa, sin embargo, dos de los entrevistados indican que existen limitaciones en cuanto a la recaudación de elementos de convicción, ya que, si bien la norma se encarga de proteger la privacidad de la víctima, esta protección puede obstaculizar la investigación en casos donde se requiera la información bancaria y de comunicaciones.

Tabla 06*.¿Cuáles son las causas que contribuyen al archivo de investigaciones del delito de fraude informático?*

ENTREVISTADO	RESPUESTA

E1	La principal causa seria la falta de individualización del imputado.
E2	Muchas veces por la falta de individualización del imputado.
E3	La carga procesal no deja que nos avoquemos específicamente a un solo delito, el desistimiento del agraviado, la falta de identificación del imputado, demora en la remisión de medios probatorios y la falta de recursos tecnológicos.
E4	Falta de declaración del agraviado para poder coadyubar con la investigación.
E5	Desistiendo del caso por parte de las víctimas al no continúan de manera dinámica con el aporte de evidencia. No contar con suficientes elementos de convicción Falta de tecnologías que nos permita recabar evidencia. Falta de declaración de la victima
E6	No se logra obtener suficientes elementos de convicción para una Formalización de Investigación, menos para una Acusación.
E7	La principal sería la falta de tecnología.

Elaboración propia

Interpretación: En la tabla 6, respecto a las causas que generan el archivo de casos, de las entrevistas realizadas se determinó que en su gran mayoría se deben a la falta de individualización del imputado ya que estos no llegan a ser plenamente identificados otra causa es la falta de interés que la víctima muestra en el caso al no presentarse para brindar su declaración o desisten de las investigaciones , sumado a ello la demora en la recaudación de los elementos de convicción como la autorización para levantar los secretos bancarios o de comunicaciones y la falta de recursos tecnológicos al tratarse de un delito que se lleva a cabo de manera digital los investigadores no cuentan con las herramientas necesarias para analizar la

evidencia, limitando su capacidad para rastrear a los delincuentes y recuperar los fondos robados.

Tabla 07. *¿Qué estrategias se podrían implementar para mejorar la eficacia en la resolución de casos de fraude informático?*

ENTREVISTADO	RESPUESTA
E1	La creación de fiscalías especializadas y unidades en la PNP.
E2	Que sea obligatorio remitir a la unidad de ciberdelincuencia el acompañamiento cuando se tenga ese tipo de delitos.
E3	Por un lado, la creación de fiscalías especializadas y por otro lado sería justamente que dicha fiscalía debería estar dotado de personal fiscal debidamente capacitado y contar con la logística necesaria para realizar la persecución de este delito.
E4	Que existan mecanismos de cooperación directa con las entidades financieras y de telecomunicación para poder conseguir los elementos de convicción asimismo implementación de tecnologías como softwares e identificación de IP.
E5	Las estrategias que se deberían implementar previamente es que la víctima en compañía de la policía se apersone a los establecimientos bancarios o de telefonía para que les puedan proporcionar cualquier tipo de información respecto a sus estados de cuentas o de comunicaciones.
E6	Que se otorguen herramientas técnicas, Software especializado, también debería haber una capitación porque tampoco somos ingenieros, somos abogados.

E7	Para mí debería haber una unidad especializada en la policía que se dote de esos equipos especializados para poder identificar el fraude informático.

Elaboración propia

Interpretación: De la tabla 7, tres de los entrevistados refieren que para mejorar la eficacia en la investigación de casos de Fraude informático se debería crear una Fiscalía especializada que se encargue de la investigación de este delito la cual cuente con personal debidamente capacitado así como suficientes recursos terminológicos como software especializado para el análisis forense de dispositivos electrónicos, herramientas de identificación de direcciones IP y equipos para la preservación de evidencia digital, por otro lado también se menciona que es necesaria una cooperación interinstitucional para poder obtener sin demoras lo solicitado en las diligencias o dotar al Ministerio Publico de una facultad especial para acceder a información relevante de manera cautelar y por ultimo capacitación continua en personal fiscal como policial respecto a las últimas técnicas utilizadas por los delincuentes cibernéticos.

Objetivo Específico dos: "Determinar las herramientas tecnológicas y recursos que estén disponibles para los Fiscales en la Investigación del delito de fraude Informático", encontramos:

Tabla 08*. ¿Cuántas veces ha sido capacitado en temas relacionados a delitos informáticos y cree que es necesaria una mayor capacitación para la existencia de una mejor investigación?*

ENTREVISTADO	RESPUESTA
E1	A través de la entidad del M.P solo en dos ocasiones, por lo que se necesita mayor capacitación, pero con la implementación correspondiente.

E2	Yo varias, el resto de fiscales creo que ninguna, necesitan capacitarse porque son temas muy específicos.
E3	Algunas veces fui capacitado con talleres o cursos, pero las capacitaciones deberían darse mediante pasantías o diplomados sobre tecnología debido a que la carga procesal nos limita el hecho de poder ingresar algún curso, dado que estos se programan en horarios laborales.
E4	Ninguna, siendo necesaria que exista una mayor capacitación para poder investigar mejor el delito
E5	Unas dos veces, yo creo que debería de existir una mayor capacitación para poder recabar la evidencia y así también poder procesarla entendiendo previamente el tema técnico.
E6	Nunca he sido capacitado, solo una autocapacitación de los pocos libros que he leído, pero tampoco dice, de cómo llevar a cabo una investigación del delito de Fraude informático, o las modalidades, tampoco te dicen de qué forma lo van a combatir o que Software deberían utilizar.
E7	Nunca he sido capacitado en este tema de delito de Fraude informático.

Elaboración propia

Interpretación: En la tabla 8, de las entrevistas realizadas tres fiscales mencionan nunca haber sido capacitados, mientras que cuatro fiscales si bien recibieron capacitación algunas veces refieren que se requiere una mayor capacitación debido a que este es un delito complejo y que aquellas capacitaciones no se deberían dar dentro del horario laboral siendo lo más factible pasantías o diplomados.

***Tabla 09**. ¿Considera que en la Fiscalía de la Provincia de San Román – Juliaca, cuenta con los recursos tecnológicos y humanos suficientes para investigar delitos informáticos de manera eficiente?*

ENTREVISTADO	RESPUESTA
E1	Contamos con el conocimiento, pero hace falta implementación de herramientas tecnológica, así como mayor personal especializado.
E2	Actualmente se cuenta con una computadora que ayuda a validar los medios probatorios recaudados por el fiscal en su investigación preliminar, sin embargo, esta esta no es utilizada debido a su desconocimiento, careciendo de personal especializado en el tema, así como peritos.
E3	No, porque en principio carecemos de personal humano donde un asistente asiste a dos fiscales lo que dificulta la existencia de un equipo que trabaje de forma eficiente, fuera de ello tampoco contamos con los recursos tecnológicos suficientes.
E4	No, pese a que actualmente se cuenta con una computadora que ayuda a validar los medios probatorios recaudados por el fiscal en su investigación preliminar esta no es utilizada debido a su desconocimiento, careciendo de personal especializado en el tema, así como peritos.
E5	No, la fiscalía en la cual laboramos no cuenta con recursos tecnológicos ni previamente el personal que nos ayude a investigar estos delitos en vista de que previamente dependemos de la sede central para poder realizar este tipo de pericias siendo necesario dotar a cada fiscalía con peritos en esta materia.

E6	No cuentan, debería de crearse un despacho con un Provincial y 4 Fiscales adjuntos, Fiscales especializados que tengan competencia Regional, porque el delito de fraude Informático, se podría frenar con investigaciones especializadas.
E7	No, porque no nos han capacitado tanto asistente o fiscales, para al menos saber de cómo empezar o cómo se puede investigar un delito informático estamos al libre albedrío, así oficialmente no.

Elaboración propia

Interpretación: En la tabla 09, los entrevistados respecto a los recursos tecnológicos con los que cuentan respondieron que existe de una computadora útil que valida las pruebas digitales empero esta herramienta no se utiliza debido al desconocimiento sobre su manejo por parte del personal fiscal, evidenciando una clara necesidad de capacitación en el uso de tecnologías aplicadas a la investigación de delitos informáticos asimismo se señala la falta de equipos y herramientas especializadas para este tipo de investigaciones, lo que dificulta la preservación y el análisis de la evidencia digital, el cual es un elemento fundamental en los casos de fraude informático, por otro lado respecto al recurso humano revelaron la falta de personal especializado en este delito, como peritos informáticos y analistas forenses. Por lo que se evidencia una clara necesidad de recursos tecnológicos y humanos.

Tabla 10. *¿Cómo se pueden optimizar los recursos y herramientas disponibles para abordar eficazmente los casos del delito de Fraude informático?*

ENTREVISTADO	RESPUESTA
E1	Con la creación de fiscalías especializadas.
E2	Solicitando ayuda a la unidad de ciberdelincuencia para que se les orienten en las diligencias necesarias que se deben llevar a cabo

	para una mejor investigación asimismo capacitación para utilizar las herramientas tecnológicas con las que se cuentan.
E3	Lo más correcto sería la creación de fiscalías especializadas en cada distrito fiscal que cuenten con personal capacitado el cual pueda trabajar de forma óptima y tengan los recursos tecnológicos suficientes para investigar el delito, debido a que pese a contar con la unidad especializada en ciberdelitos de Lima a la cual tenemos acceso esta solo nos guía en los medios probatorios que debemos recabar sin embargo, no nos ayuda a recabar aquellos medios probatorios o a veces demorarán tiempo en respondernos ya que priorizarán su propia carga en su distrito fiscal, asimismo se debería capacitar a la población sobre este tipo de delito para poder prevenirlos.
E4	No contamos con los recursos y herramientas suficientes por lo que se debería de crear una Fiscalía Especializada a nivel Regional.
E5	Los recursos pueden ser optimizados mediante la implementación de peritos especializados asimismo contar con los aplicativos, programas y propiamente herramientas que nos permitan recabar estas evidencias optimizando las necesidades que presenta cada distrito fiscal.
E6	Primero no hay recursos tampoco herramientas, pero con la creación de una Fiscalía especializada de competencia Regional, ello sería lo más prudente conocer determinado delito, porque es una Ley especial.
E7	No hay herramientas, recursos humanos tampoco, en conclusión, con la capacitación y tecnología.

Elaboración propia

Interpretación: En la tabla 10, las respuestas de los Fiscales revelan la falta total de herramientas y recursos humanos, por lo que la creación de una Fiscalía especializada de competencia Regional sería una forma de abordar eficazmente los casos de fraude Informático, atribuido a ello, es necesario un enfoque integral que combine la especialización y capacitación del personal fiscal, mejorar la coordinación interinstitucional para agilizar la obtención de información, la disponibilidad de peritos especializados, la dotación de recursos tecnológicos incluyendo software especializado para el análisis forense de dispositivos electrónicos y herramientas de identificación de direcciones IP, asimismo implementar estrategias para capacitar a la población en general sobre este tipo de delito y sus modalidades.

VI. DISCUSIÓN

6.1. Discusión de los resultados.

En este apartado, se discutirán los resultados obtenidos a partir de las entrevistas realizadas.

Con referencia al objetivo general de esta investigación, el cual consistió en determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024, al respecto se logró analizar que la fiscalía recibe un promedio de 3 a 7 denuncias mensuales, esta cifra, no es alarmante pero tomando en cuenta, que se encuentra conformada por 28 fiscales, la suma de denuncias en promedio mensual seria de 196 denuncias como máximo y 84 denuncias como mínimo lo que evidencia la creciente incidencia de este delito en la jurisdicción siendo el factor de su comisión la utilización de tecnologías, la cual tuvo un desarrollo agigantado a inicios del 2020 siendo favorable para la sociedad al optimizar su tiempo, sin embargo cada acción tiene una reacción y en la era digital, paradójicamente se obtuvieron resultados negativos al desarrollarse nuevas modalidades en actos delictivos para afectar el patrimonio de las personas, dejando ver claramente la desventaja en la que nos encontramos, ya que nuestros medios de defensa no están a la altura de las circunstancias.

Esto guarda relación de acuerdo a lo mencionado por Ospina & Sanabria (2020), quien, en su investigación concluye que en Colombia el aumento en casos sobre Fraude informático se evidenció claramente desde el 2020 donde existió un aumento de usuarios interactuando por internet y otras TIC, impulsados por el aislamiento preventivo derivado del COVID-19, la cual se dio a nivel mundial.

Asimismo Ponce (2024), enfatiza que en Colombia el uso de internet experimentó un auge significativo desde el inicio de la pandemia, siendo los

ataques cibernéticos más comunes el Ransomware, la suplantación de IP, suplantación de MAC, las cuales son diversas técnicas que se basan en el anonimato, así como la manipulación de direcciones MAC para simular la presencia de nodos legítimos en la red.

Por lo que, si bien el COVID-19 actuó como un catalizador para que las personas se expongan al mundo digital generando un escenario propicio para su comisión los cuales al ser denunciados, el 90% de casos se archivan siendo un 10 % el que pasa a formalizarse sin embargo estos no logran llegar a una etapa de acusación; lo cual se alinea con la investigación de Valentín (2022), quien, al realizar el análisis de carpetas fiscales sobre Fraude informático concluyo que si bien en todas las carpetas se apertura una investigación preliminar al final el 100% de estos casos se archivaron bajo el fundamento de la falta de individualización del imputado debido a los anonimatos que se presentan.

En relación al primer objetivo específico que consistió en analizar las causas que dificultan la eficacia de la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román – Juliaca, los entrevistados señalaron distintas causas que dificultan la investigación, las cuales estarán distribuida en cuatro apartados como son: la falta de individualización del imputado, carencia de herramientas tecnológicas, capacitación para el personal fiscal como administrativo, falta de colaboración entre las entidades existiendo demora en la recaudación de los elementos de convicción.

En cuanto al primer apartado, la falta de individualización del imputado se debe a que al tratarse de delitos tecnológicos los ciberdelincuentes camuflan su identidad o se crean identidades falsas para no ser ubicados, el cual no solo puede ser cometido por personas nacionales sino también extranjeras de cualquier parte del mundo.

Esto guarda relación de acuerdo a lo mencionado por Quispe (2020), para quien, el anonimato que proporcionan los sistemas informáticos utilizados para cometer estos delitos es un obstáculo importante para la individualización de los delincuentes, aunque se pueda seguir el rastro digital hasta el terminal, la falta de información personal asociada a estas herramientas dificulta la identificación fehaciente del usuario.

Respecto al segundo apartado sobre la carencia de herramientas tecnológicas es menester saber que al tratarse de delitos donde los delincuentes utilizan la tecnología para propiciar el hecho delictivo las pruebas digitales pueden ser eliminadas o alteradas, por lo que el fiscal debe de realizar una investigación rápida utilizando instrumentos tecnológicos que permitan detectar las direcciones IP, subrayando a su vez la importancia de la capacitación continua del personal fiscal y policial en la utilización de las nuevas tecnologías así como en las últimas técnicas utilizadas por los delincuentes cibernéticos las cuales se actualizan a medida que avanza la tecnología , para ello es importante destacar la investigación de Ospina & Sanabria (2020), que se presenta como antecedente y en la cual destaca que se les debe de brindar mayor capacitación a los profesionales requeridos para trabajar en la investigación de los ciberdelitos.

Asimismo Ojeda et al. (2023) en su investigación concluye que para Ecuador el delito de Fraude informático representa un gran desafío, requiriendo peritos técnicos para recopilar evidencia digital e innovaciones tecnológicas para los persecutores del delito quienes a su vez requieren de una mayor especialización para abordar de manera efectiva estos delitos adaptándose a las nuevas innovaciones tecnológicas y métodos empleados por los delincuentes cibernéticos.

Por otro lado Valentín (2022), que se presenta como antecedente en su investigación concluyo que existe un gran desconocimiento por los fiscales sobre los protocolos y normas que se deben llevar a cabo para abordar este

delito, sugiriendo que la capacitación debe enfocarse en la práctica y no solo en la teoría para que tengan un amplio conocimiento sobre que diligencia realizar y que solicitudes presentar.

Pero también debe de existir capacitación a la población en general sobre este delito para prevenir futuros casos tal como señala Ponce (2024) en su investigación donde destaca que el gobierno debe de promover campañas de informativas para toda la población en vista de los avances tecnológicos que van evolucionando constantemente para poder ejercer buenas prácticas en ciberseguridad.

Asimismo, se considera necesaria una cooperación interinstitucional más fluida para recabar sin demoras la información, o bien, dotar al Ministerio Público de una facultad especial para acceder a información relevante de manera cautelar, tal como menciona Hernández et al.(2024), en su investigación citada como antecedente que en Ecuador la falta de coordinación entre instituciones y organismos encargados de la seguridad informática presenta una limitante significativa en la eficacia de la lucha contra la ciberdelincuencia; ya que, si bien mencionaron que el marco normativo no presenta limitaciones en sí mismo, la recaudación de elementos de convicción se ve obstaculizada por la protección de la privacidad de la víctima la cual se encuentra plasmada en la Ley N° 29733 (Ley de protección de datos personales), la cual es fundamental, pero puede dificultar la investigación en casos donde se requiere información bancaria y de comunicaciones, generando un conflicto entre la protección de la privacidad y la necesidad de esclarecer el delito, tal como lo menciona Arellano & Galindo (2022) en su investigación citada como antecedente donde concluye que existe una deficiencia en el artículo 8 de la Ley N° 30096, la cual no establece medidas preventivas o protectoras que pueda realizar la persona agraviada ante un ataque cibernético, así como la existencia de barreras burocráticas que limitan la identificación sin demora del destinatario a quien se le realizo la trasferencia

bancaria no autorizada, de la misma forma menciona que en los delitos de Fraude informático se protege el patrimonio de la persona por lo que si no existe alguna vulneración en su patrimonio no existe delito, lo cual debería ser modificado, implementándose una pena para aquellas personas que por medio de un sistema informático busquen realizar un perjuicio económico, sin la existencia de un perjuicio patrimonial resultante.

Por lo que la dificultad para identificar plenamente a los responsables, sumada a la falta de interés de la víctima en el caso y la demora en la recaudación de elementos de convicción, como la autorización para levantar los secretos bancarios o de comunicaciones, limitan la capacidad de los investigadores para llevar los casos a juicio. Los entrevistados coinciden en que se trata de un delito que requiere de múltiples diligencias, siendo la declaración del agraviado el punto de partida. Sin embargo, la obtención de elementos de convicción cruciales, como el levantamiento del secreto bancario y de las comunicaciones, los IPS de los sistemas informáticos y el peritaje informático, demanda un tiempo considerable, lo que dilata el avance de la investigación.

En cuanto al segundo objetivo específico, consistió en determinar las herramientas tecnológicas y recursos que estén disponibles para los Fiscales en la Investigación del delito por fraude informático, de la cual los entrevistados coinciden en que no hay suficientes herramientas tecnológicas como recursos, para la disponibilidad de los Fiscales, así también destacan varias limitaciones en la investigación del delito de fraude informático, de la cual se detallará a continuación:

En primer lugar, destacan la capacitación insuficiente; de lo cual tres Fiscales mencionan no haber recibido nunca una capacitación respecto a este tipo de delito, y de los que han recibido alguna capacitación estas resultarían ser insuficientes, por lo que debería realizarse fuera del horario laboral mediante pasantías o diplomados, para mejorar sus conocimientos y

habilidades, ya que de ese modo se contaría con fiscales altamente capacitados.

Así también, se enfatiza la falta notable de recursos tecnológicos y humanos, si bien existen una herramienta como la computadora en la Fiscalía, para validar pruebas digitales, su utilización es limitado esto debido al desconocimiento de su manejo. La escasez de equipos especializados y personal capacitado, como peritos informáticos, plantea un desafío significativo para el análisis y preservación de evidencia digital. Esta situación puede tener consecuencias graves para la administración de justicia, ya que la evidencia digital juega un papel cada vez más importante en la resolución de delitos.

Conforme a ello autores como Hernández et al (2024), en su investigación concluyen que de forma mayoritaria el sistema de seguridad cibernética es poco eficaz debido a la falta de comunicación entre instituciones y entidades de ciberseguridad, asimismo la falta de capacitación en la personal evidencia la urgencia de destinar recursos a programas de formación continua.

De igual manera Quispe (2020), concluye que las empresas financieras y telefónicas no cooperan con la investigación de los delitos de fraude informático dado que brindan una deficiente y limitada colaboración asimismo **l**a escasez en cuanto a equipamiento, instalaciones, personal y habilidades dificultan el desempeño de la DIVINCRI y del Ministerio Público, sin embargo para combatir proponen desarrollar iniciativas de sensibilización y capacitación en ciberseguridad enfocadas en distintos sectores, con el objetivo de concienciar a la sociedad sobre los peligros en el ámbito digital y ofrecer herramientas y competencias necesarias para proteger la información.

En este aspecto se puede indicar que los entrevistados coincidieron en que se necesita una capacitación especializada en este tipo de delitos, con expertos en la materia, tomando énfasis la falta de entidades de

ciberseguridad, son esas razones por la que no se ha tenido éxito en las resoluciones de casos de este tipo de delito, a pesar de la labor que realizan los Fiscales la lucha contra la ciberdelincuencia. Estos avanzan significativamente, junto a las limitaciones.

CONCLUSIONES

Primero: Los delitos de Fraude informático son cometidos mediante el uso de la tecnología por lo que sus comicios se encuentra en el desarrollo de las tecnologías informáticas, estos tuvieron un avance significativo durante el COVID-19 debido al confinamiento los usuarios empezaron a utilizar mayores plataformas digitales en su vida cotidiana lo que los convirtió en personas dependientes de las TIC, conllevo el aumento de denuncias por este delito ocasionando que la Fiscalía enfrente desafíos considerables, los cuales se ven reflejados en el alto índice de archivo de casos donde como principal fundamento se tiene la falta de individualización del imputado, evidenciado tanto en esta investigación como en estudios previos, que no existe eficacia en la investigación Preliminar.

Segundo: El Ministerio Publico utiliza diversas técnicas para la persecución penal del delito de Fraude informático como son las declaraciones, pericias, levantamientos del secreto bancario y de las telecomunicaciones las cuales son insuficientes para lograr individualizar a los responsables debido a que estos enmascaran su identidad, llegando a operar desde cualquier parte del mundo; esta situación se agrava debido a la carencia de herramientas tecnológicas que ayuden a identificar los IPs, la falta de capacitación continua a fiscales y personal policial, falta de cooperación interinstitucional, demora sobre el pronunciamiento del juez sobre los requerimientos de medidas limitativas debido a las barreras burocráticas, por todas estas causas los casos de Fraude informático en su mayoría son archivados.

Tercero: La investigación revela una serie de deficiencias en la capacidad de los fiscales para una investigación del delito de Fraude informático, ello junto a la escasez de personal especializado, como son los peritos informáticos, y más. Por lo que resulta ser necesario y fundamental adoptar medidas prácticas e iniciativas concretas, para abordar estas limitaciones, ello abarca a que no solo la previsión de herramientas tecnológicas adecuadas resultaría útil, sino también el desarrollo

de programas de capacitación actualizados y especializados, que permitan a los fiscales adquirir los conocimientos necesarios para enfrentar eficazmente los desafíos del fraude informático. En conclusión, no se cuenta con las herramientas tecnológicas ni recursos adecuados, para una investigación eficaz en la investigación del delito de fraude informático.

RECOMENDACIONES

Primero: El aumento de denuncias tras la pandemia, sumado al masivo archivo de casos en el Ministerio Público, plantea serias interrogantes sobre la capacidad del sistema para abordar estos delitos por lo que se recomienda la creación de una Fiscalía especializada en la investigación de este delito, dotada del personal debidamente capacitado y recursos tecnológicos adecuados, como software especializado para el análisis forense de dispositivos electrónicos, herramientas de identificación de direcciones IP y equipos para la preservación de evidencia digital.

Segundo: Se recomienda mejor capacitación a los operadores de justicia sobre las nuevas técnicas cibernéticas así como los protocolos para investigar el delito, implementado nuevos equipos tecnológicos que ayuden a identificar a los responsables también se sugiere establecer un sistema de cooperación interinstitucional entre la Fiscalía, la Policía Nacional, el Poder Judicial y las entidades bancarias y de telecomunicaciones, este sistema debería incluir protocolos de actuación estandarizados que permitan una respuesta más rápida en la recopilación y análisis de pruebas digitales, evitando demoras procesales que favorezcan la impunidad de los ciberdelincuentes, asimismo la capacitación por parte del estado, entidades bancarias y de comunicación a la sociedad sobre las distintas modalidades de este delito y la manera en que deben actuar ante los ciberdelincuentes.

Tercero: Para potenciar la eficacia en la investigación de fraude informático, con las herramientas tecnológicas y recursos disponibles, se requiere una estrategia que abarque la modernización tecnológica, así como habilidades especializadas con la colaboración interinstitucional, ello implica no solo la adquisición adecuada de herramientas tecnológicas o la asignación de recursos adecuados, sino también la implementación de programas de capacitación eficaz para los fiscales, con los capacitadores adecuados o conocedores del tema del fraude informático, es decir expertos en la materia. Al abordar estas áreas claves, se verá un fortalecimiento

significativo en la capacidad de la fiscalía para prevenir, detectar y procesar eficazmente los delitos de fraude informático, de ese modo protegiendo los intereses de la sociedad y promoviendo la justicia en el entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

Acurio del Pino, S. (2016). DELITOS INFORMATICOS: GENERALIDADES. *Pontificia Universidad Católica de Ecuador*, 1–67.

Aguirre, R. M. (2021). La normatividad como objeto: doctrina, teoría, metateoría. *Anuario Del Área Socio-Jurídica*, 29–49.

Arapa Ticona, J. C., Cari Calcina, K. M., Laura Lipe, J. J., Laura Valero, M., Merma Cabrera, R. M., Tarapa García, H. L., & Condori Parí, N. (2024). CAUSAS Y CONSECUENCIAS DEL INCREMENTO DE LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE PUNO 2023. *REVISTA DE DERECHO*, *9*(1). https://doi.org/10.47712/rd.2024.v9i1.262

Arellano Casimiro, G. L., & Galindo Martínez, S. E. (2022). *Deficiencias Legislativas en el Tratamiento de la Ley N° 30096, Ley de Delitos Informáticos – Fraude Informático, Lima 2019 – 2021*. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/102672/Arellano_CGL-Galindo_MSE-SD.pdf?sequence=4&isAllowed=y

Arista Navarro, A. J., & Castro Segovia, M. V. (2024). *El fraude informático: una revisión de su literatura científica en el marco de la Ley 30096*. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/148779/B_Arista_NAJ-Castro_SMV-SD.pdf?sequence=1&isAllowed=y

Armestar Bruno, G. M., & Toche Vega, F. L. (2023, July 20). *El tratamiento del fraude informático: Un estudio del Derecho Comparado entre Peru y EE.UU*. La Voz Juridica. https://revistas.uarm.edu.pe/index.php/lavozjuridica/article/view/390/256

Baena Paz, G. (2017). *Metodología de la investigación Grupo Editorial Patria Sistema de aprendizaje en línea Metodología de la investigación* (Grupo Editorial Patria, Ed.; 3a edición). www.editorialpatria.com.mxwww.sali.org.mx

Barrios Achavar, V., & Vargas Cárdenas, A. (2018). *Convenio sobre la Ciberdelincuencia: Convenio de Budapest Introducción Autor*.

Benavente Chorres, H. (2011). *La aplicación de la teoría del caso y la teoría del delito en el proceso penal acusatorio*. J.M. Bosch Editor.

Castillo López, M., Romero Sánchez, E., & Mínguez Vallejos, R. (2023). El método fenomenológico en investigación educativa: una revisión sistemática. *Latinoamericana de Estudios Educativos*, *18*(2), 241–267. https://doi.org/10.17151/RLEE.2023.18.2.11

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

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *Source: American Sociological Review*, *44*(4), 588–608.

Constancio, G. M. (2009, April 2). La Investigación Básica. La Investigación en Ciencias Fisiológicas: Bioquímica, Biología Molecular y Fisiología. Cuestiones Previas. *Basic Research. Research in Physiological Sciences: Biochemistry*.

Cuenca Gonzaga, A. I., & Núñez Portilla, J. E. (2024). Análisis documental: impacto de la seguridad jurídica antes los delitos informáticos. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, *5*(4). https://doi.org/10.56712/latam.v5i4.2437

Dessler, G., & Varela, R. (2011). *Administración de recursos humanos Administración de recursos humanos Quinta edición Enfoque latinoamericano* (quinta). www.pearsoneducacion.net

Edmundo Mezger. (1935). *DERECHO PENAL: Vol. I*. Editorial Bibliográfica Argentina.

EUROPOL. (2021). *Internet Organised Crime Threat Assessment 2021*. https://doi.org/10.2813/113799

Fuster Guillen, D. E. (2019). Investigación cualitativa: Método fenomenológico hermenéutico. *Propósitos y Representaciones*, *7*(1), 201–229. https://doi.org/10.20511/pyr2019.v7n1.267

García, H., Del Rocío, K., Bravo, G., Elizabeth, M., Briones, T., Marjorie, R., Vaca, C., & Marisol, A. (2020). Las nuevas herramientas e instrumentos tecnológicos incorporados a la organización *new technological tools and instruments incorporated into the organization*. *Edición, 12*(71), 1014–1023.

García Rada, D. (1964). *Comentarios al Código de Procedimientos Penales*.

Gonzales Ávila, M. (2022). *Aspectos Éticos de la Investigación Cualitativa*.

Hernández Alvarado, V. J., Arias Hernández, J. L., & Granja Huacon, S. H. (2024). EFECTIVIDAD DE LAS POLÍTICAS IMPLEMENTADAS PARA GARANTIZAR LA SEGU- RIDAD CIBERNÉTICA EN ECUADOR. *Revista Científica de la Universidad de Cienfuegos*, *16*, 288–296. https://rus.ucf.edu.cu/index.php/rus/article/view/4623/4502

Hernández Sampieri, R., Fernández Collado, C., María del Pilar Baptista Lucio, D., & Méndez Valencia Christian Paulina Mendoza Torres, S. (2014). *Metodología de la Investigación*.

Insignares Gómez, R. C. (1998). LA INVESTIGACIÓN EN EL Departamento de Derecho Fiscal. *Centro de Estudios Fiscales*, 57–72.

Jorge Alberto Vega Aguilar, & Maguin Arévalo Minchola. (2022, February). *Ciberdelitos.* https://www.mpfn.gob.pe/escuela/contenido/archivosbiblioteca/del0438.pdf

Juan Pablo, C. H. (2020). *Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera Autor*.

Laura Mayer Lux, & Oliver Guillermo Calderón. (2020, June 30). *El delito de fraude informático: Concepto y delimitación*. https://doi.org/10.5354/0719-2584.2020.53447

Malca Leandro, E. C. (2023). Eficacia de la persecución penal en la investigación preparatoria del delito de fraude informático, Callao, 2022. *Universidad Cesar Vallejo*. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/129112/Malca_LEC-SD.pdf?sequence=1&isAllowed=y

Mayer, L. L. (2020). El delito de fraude informático: Concepto y delimitación. *REVISTA CHILENA DE DERECHO TECNOLOGICO*. https://doi.org/10.5354/0719-2584.2020.53447

Moras Mom, J. R. (2004). *Manual de derecho procesal penal: juicio oral y público penal nacional: Vol. sexta*. Lexis Nexis Abeledo Perrot.

Núñez Pérez, F. V., & Carhuancho Zaldaña, B. (2020). Ciberdelincuencia en tiempos de covid-19: ¿La vulneración a derechos constitucionales? *Lumen*, *16*(1), 93–100. https://doi.org/10.33539/lumen.2020.v16n1.2287

Ojeda Sotomayor, P. M., Diaz Basurto, I. J., Cajas Parraga, C. M., & Cabrera Ripalda, E. P. (2023). DESAFIOS LEGALES EN ECUADOR FRENTE A LOS DELITOS INFORMÁTICOS, IMPORTAN- CIA DE SU PREVENCIÓNDESAFIOS LEGALES. *Revista Científica de La Universidad de Cienfuegos*, *15*, 746–754. https://rus.ucf.edu.cu/index.php/rus/article/view/4195/4102

Ospina Díaz, M. R., & Sanabria Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Rev.Crim.*, *62*, 199–217. https://www.researchgate.net/publication/348405715_Desafios_nacionales_frente_a_la_ciberseguridad_en_el_escenario_global_un_analisis_para_Colombia_-_National_Challenges_for_Cybersecurity_on_a_Global_Level_an_Analysis_for_Colombia

Ponce Tubay, M. A. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio*, *1*(58), 119–123. https://doi.org/10.36097/rsan.v1i58.2667

Quispe Rodríguez, S. E. (2020). *Factores que determinan el archivo de investigaciones por delito de Fraude informático en el Distrito Fiscal de la Libertad año 2019*. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/91512/Quispe_RSE-SD.pdf?sequence=1

Rextie. (2022, July 12). *Los tipos de delitos informáticos más recurrentes que amenazan a las empresas*.

Ruiz Ramirez, J. (2010, March). Importancia de la Investigación. *Revista Científica - Scielo*. http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S0798-22592010000200001&lng=es&tlng=es.

Sánchez Flores, F. A. (2019). Fundamentos Epistémicos de la Investigación Cualitativa y Cuantitativa: Consensos y Disensos. *Revista Digital de Investigación En Docencia Universitaria*, 101–122. https://doi.org/10.19083/ridu.2019.644

SAULO GUSTAVO MACHICAO MOLLOCONDO. (2019). *ANÁLISIS DE RIESGO Y POLÍTICAS DE SEGURIDAD DE INFORMACIÓN DE LA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN (OTI) – UNA PUNO 2018*. https://repositorio.unap.edu.pe/bitstream/handle/20.500.14082/13958/Machicao_Mollocondo_Saulo_Gustavo.pdf?sequence=1&isAllowed=y

Sofia Pichihua Vegas. (2023, February 13). Sepa cómo evitar ser víctima de un delito informático. *El Peruano*. https://elperuano.pe/noticia/204416-sepa-como-evitar-ser-victima-de-un-delito-informatico

Tenorio Pereyra, J. E. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia*.

Universidad Tecnológica de Investigación Científica. (2019). *Código de ética de Investigación Científica y Tecnológica*. https://bit.ly/3vW71ES

Valdivia Zapata Jose Adrian. (2023). *La eficacia de la persecución penal del delito de fraude informático en el Perú*.

Valentín Horna, A. P. (2022). *Factores de incidencia en el archivo de las investigaciones preliminares por delito de fraude informático, Trujillo 2021. Mecanismos de mejora.* https://hdl.handle.net/20.500.12692/102926

Wuerges, A. F. E., & Borba, J. A. (2014). Fraudes contables: una estimación de la probabilidad de detección. *Revista Brasileira de Gestao de Negocios*, *16*(52), 466–483. https://doi.org/10.7819/rbgn.v16i52.1555

ANEXOS

Anexo 1: Matriz de categorización apriorística o cualitativa

Título: Investigación del Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

Responsables: Joselyn Karen Churata Chuquipalla y Dianeth Adelayda Quispe Machaca.

<table>
<tr><th>ÁMBITO TEMÁTICO</th><th>PROBLEMA DE INVESTIGACIÓN</th><th>OBJETIVO DE INVESTIGACIÓN</th><th>CATEGORÍAS Y SUBCATEGORÍAS</th><th>METODOLOGÍA</th></tr>
<tr><td rowspan="2">La eficacia en la investigación por el delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.</td><td>Problema general.
¿La investigación del delito de Fraude Informático se viene realizando de manera eficaz en la Fiscalía de la Provincia de San Román – Juliaca, 2024?</td><td>Objetivo general.
Determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.</td><td rowspan="2">Categoría Única:
Eficacia en la Investigación por delitos de Fraude Informático:

• Fraude informático
• Capacitación del personal
• Instrumentos Tecnológicos
• Normativa</td><td rowspan="2">Tipo de investigación:
Básico

Diseño de investigación:
Fenomenología

Población y muestra:
Fiscalía de la Provincia de San Román – Juliaca:

- 02 Fiscales Provinciales.

- 05 Fiscales Adjuntos.</td></tr>
<tr><td>Problemas específicos.</td><td>Objetivos específicos.</td></tr>
</table>

	P.E.1: ¿Cuáles son las causas que dificultan la eficacia en la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román – Juliaca? **P.E.2:** ¿La fiscalía cuenta con herramientas tecnológicas y recursos disponibles para la Investigación de los delitos de Fraude Informático?	**O.E.1:** Analizar las causas que dificultan la eficacia en la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román – Juliaca. **O.E.2:** Determinar las herramientas tecnológicas y recursos que estén disponibles para los Fiscales en la Investigación de los delitos de fraude Informático.		**Técnicas de instrumentos:** Entrevista- Guía de Entrevista.

Anexo 2: Instrumentos de recolección de información

GUIA DE ENTREVISTA DIRIGIDO A FISCALES

La finalidad de la entrevista es buscar información relacionada con el tema de la **"Investigación del Fraude informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024".**

Entrevistado:

……

Cargo:

……

Institución:

.....

OBJETIVO GENERAL

Determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

1.- En base a su experiencia, **¿Cuántas denuncias por el delito de fraude informático ingresan mensualmente a su despacho y cuáles serían los factores de su comisión?**

……
……
……
……
……

2.- Referente a la pregunta anterior, **¿Cuál es la proporción de casos de fraude informático que se archivan frente a los que avanzan a la etapa de formalización?**

……
……
……
……
……..

OBJETIVO ESPECÍFICO 01

Analizar las causas que dificultan la eficacia de la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román – Juliaca.

3.- Desde su experiencia, **¿Cuáles son las diligencias necesarias para la investigación del delito de fraude informático?**

……
……
……
……
……..

4. En base a la pregunta anterior**, ¿Cuáles son las principales limitaciones que enfrenta el Ministerio Público en la etapa preliminar de las investigaciones por fraude informático?**

……
……
……
……
……..

5.- A su criterio, **¿Encontró limitaciones en el marco normativo actual que dificulten su labor como fiscal en la investigación del delito de fraude informático?** Si es así, **¿podría mencionar cuáles son esas limitaciones?**

……
……
……
……
……..

6.- En base a su experiencia, **¿Cuáles son las causas que conttribuyen el archivo de las investigaciones por el del delito de fraude informático?**

……
……
……
……
……..

7.- Asu criterio, **¿Qué estrategias se podrían implementar para mejorar la eficacia en la resolución de casos de fraude informático?**

……
……
……
……
……..

OBJETIVO ESPECÍFICO 02

Determinar las herramientas tecnológicas y recursos que estén disponibles para los Fiscales en la Investigación de los delitos por fraude Informático.

8.- A su criterio, **¿Cuántas veces ha sido capacitado en temas relacionados a delitos informáticos y cree que es necesaria una mayor capacitación para la existencia de una mejor investigación?**

……
……
……
……
……..

9.- A su criterio, **¿Considera que en la Fiscalía de la Provincia de San Román – Juliaca, cuenta con los recursos tecnológicos y humanos suficientes para investigar delitos informáticos de manera eficiente?**

……
……
……
……
……..

10.- En base a su experiencia **¿Cómo se pueden optimizar los recursos y herramientas disponibles para abordar eficazmente los casos del delito de Fraude Informático?**

……
……
……
……
……..

Anexo 3: Ficha de validación por juicio de expertos

UNIVERSIDAD AUTÓNOMA DE ICA

INFORME DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES

Título de la Investigación: Investigación del Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

Nombre del Experto: Wilfredo Flores Espillico

II. ASPECTOS QUE VALIDAR EN EL INSTRUMENTO:

Aspectos Para Evaluar	Descripción:	Evaluación Cumple/ No cumple	Preguntas por corregir
1. Claridad	Las preguntas están elaboradas usando un lenguaje apropiado	Cumple	
2. Objetividad	Las preguntas están expresadas en aspectos observables	Cumple	
3. Conveniencia	Las preguntas están adecuadas al tema a ser investigado	Cumple	
4. Organización	Existe una organización lógica y sintáctica en el cuestionario	Cumple	
5. Suficiencia	El cuestionario comprende todos los indicadores en cantidad y calidad	Cumple	
6. Intencionalidad	El cuestionario es adecuado para medir los indicadores de la investigación	Cumple	
7. Consistencia	Las preguntas están basadas en aspectos teóricos del tema investigado	Cumple	
8. Coherencia	Existe relación entre las preguntas e indicadores	Cumple	
9. Estructura	La estructura del cuestionario responde a las preguntas de la investigación	Cumple	
10. Pertinencia	El cuestionario es útil y oportuno para la investigación	Cumple	

III. OBSERVACIONES GENERALES

—

MINISTERIO PÚBLICO
WILFREDO FLORES ESPILLICO
Fiscalía Provincial

Apellidos y Nombres del validador: Flores Espillico Wilfredo
Grado académico: Magistor en Derecho
N° DNI: 01345359

UNIVERSIDAD AUTÓNOMA DE ICA

INFORME DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES

Título de la Investigación: Investigación del Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

Nombre del Experto: Judy del Rosario Condori Luque

II. ASPECTOS QUE VALIDAR EN EL INSTRUMENTO:

Aspectos Para Evaluar	Descripción:	Evaluación Cumple/ No cumple	Preguntas por corregir
1. Claridad	Las preguntas están elaboradas usando un lenguaje apropiado	Cumple	
2. Objetividad	Las preguntas están expresadas en aspectos observables	Cumple	
3. Conveniencia	Las preguntas están adecuadas al tema a ser investigado	Cumple	
4. Organización	Existe una organización lógica y sintáctica en el cuestionario	Cumple	
5. Suficiencia	El cuestionario comprende todos los indicadores en cantidad y calidad	Cumple	
6. Intencionalidad	El cuestionario es adecuado para medir los indicadores de la investigación	Cumple	
7. Consistencia	Las preguntas están basadas en aspectos teóricos del tema investigado	Cumple	
8. Coherencia	Existe relación entre las preguntas e indicadores	Cumple	
9. Estructura	La estructura del cuestionario responde a las preguntas de la investigación	Cumple	
10. Pertinencia	El cuestionario es útil y oportuno para la investigación	Cumple	

III. OBSERVACIONES GENERALES

Judy del Rosario Condori Luque
ASISTENTE EN FUNCIÓN FISCAL

Apellidos y Nombres del validador: Judy del Rosario Condori Luque

Grado académico: Magister

N° DNI: 70082632

UNIVERSIDAD AUTÓNOMA DE ICA

INFORME DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN

I. DATOS GENERALES

Título de la Investigación: Investigación del Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

Nombre del Experto: LUIS RUBEN YANQUI MACHACA

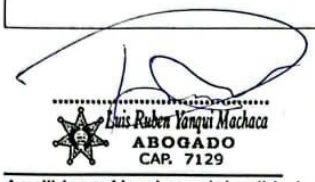
II. ASPECTOS QUE VALIDAR EN EL INSTRUMENTO:

Aspectos Para Evaluar	Descripción:	Evaluación Cumple/ No cumple	Preguntas por corregir
1. Claridad	Las preguntas están elaboradas usando un lenguaje apropiado	Cumple	
2. Objetividad	Las preguntas están expresadas en aspectos observables	Cumple	
3. Conveniencia	Las preguntas están adecuadas al tema a ser investigado	Cumple	
4. Organización	Existe una organización lógica y sintáctica en el cuestionario	Cumple	
5. Suficiencia	El cuestionario comprende todos los indicadores en cantidad y calidad	Cumple	
6. Intencionalidad	El cuestionario es adecuado para medir los indicadores de la investigación	Cumple	
7. Consistencia	Las preguntas están basadas en aspectos teóricos del tema investigado	Cumple	
8. Coherencia	Existe relación entre las preguntas e indicadores	Cumple	
9. Estructura	La estructura del cuestionario responde a las preguntas de la investigación	Cumple	

10. Pertinencia	El cuestionario es útil y oportuno para la investigación	Cumple	

III. **OBSERVACIONES GENERALES**

Ninguna.



Apellidos y Nombres del validador: YANQUI MACHACA LUIS RUBEN
Grado académico:
N°. DNI: 48457087

Anexo 4: Ficha de consentimientos Informados

UNIVERSIDAD AUTÓNOMA DE ICA

CONSENTIMIENTO INFORMADO

INVESTIGACIÓN DEL FRAUDE INFORMÁTICO EN LA FISCALÍA DE LA PROVINCIA DE SAN ROMÁN – JULIACA, 2024

Institución : Universidad Autónoma de Ica.

Responsables : CHURATA CHUQUIPALLA, Josselyn Karen
QUISPE MACHACA, Dianeth Adelayda

Objetivo de la investigación: Por la presente lo estamos invitando a participar de la investigación que tiene como objetivo determinar si se viene realizando de manera eficaz, la investigación del delito de fraude informático en la Fiscalía Provincial de la Provincia de San Román - Juliaca, 2024.

Al participar del estudio, deberá responder 10 preguntas, las cuales serán respondidas de forma anónima.

Procedimiento: Si acepta ser partícipe de este estudio, usted deberá llenar el cuestionario denominado "Guía de entrevista dirigido a Fiscales". El cual deberá ser resuelto en un tiempo prudencial según cada participante, dicha entrevista será grabada en audio y llevada a cabo por los investigadores.

Confidencialidad de la información: El manejo de la información es a través de códigos asignados a cada participante, las responsables de la investigación garantizan que se respetará el derecho de confidencialidad e identidad de cada uno de los participantes, no mostrándose datos que permitan la identificación de las personas que formaron parte de la muestra de estudio.

Consentimiento: Yo, en pleno uso de mis facultades mentales y comprensivas, he leído la información suministrada por el/las Investigadoras, y acepto, voluntariamente, participar del estudio, habiéndose informado sobre el propósito de la investigación, así mismo, autorizo la toma de fotos (evidencia fotográfica), durante la resolución del instrumento de recolección de datos.

Juliaca, 29 de enero de 2025

Firma: .....

Apellidos y nombres: Araoz Homari Jhiny

DNI: 46644884

UNIVERSIDAD AUTÓNOMA DE ICA

CONSENTIMIENTO INFORMADO

INVESTIGACIÓN DEL FRAUDE INFORMÁTICO EN LA FISCALÍA DE LA PROVINCIA DE SAN ROMÁN – JULIACA, 2024.

Institución : Universidad Autónoma de Ica.

Responsables : CHUARATA CHUQUIPALLA, Joselyn Karen
QUISPE MACHACA, Dianeth Adelayda

Objetivo de la investigación: Por la presente lo estamos invitando a participar de la investigación que tiene como objetivo determinar si se viene realizando de manera eficaz, la investigación del delito de fraude informático en la Fiscalía Provincial de la Provincia de San Román - Juliaca, 2024.

Al participar del estudio, deberá responder 10 preguntas, las cuales serán respondidas de forma anónima.

Procedimiento: Si acepta ser partícipe de este estudio, usted deberá llenar el cuestionario denominado "Guía de entrevista dirigido a Fiscales". El cual deberá ser resuelto en un tiempo prudencial según cada participante, dicha entrevista será grabada en audio y llevada a cabo por los investigadores.

Confidencialidad de la información: El manejo de la información es a través de códigos asignados a cada participante, las responsables de la investigación garantizan que se respetará el derecho de confidencialidad e identidad de cada uno de los participantes, no mostrándose datos que permitan la identificación de las personas que formaron parte de la muestra de estudio.

Consentimiento: Yo, en pleno uso de mis facultades mentales y comprensivas, he leído la información suministrada por el/las Investigadoras, y acepto, voluntariamente, participar del estudio, habiéndose informado sobre el propósito de la investigación, así mismo, autorizo la toma de fotos (evidencia fotográfica), durante la resolución del instrumento de recolección de datos.

Juliaca, 28 de enero de 2025

Firma: .....

Apellidos y nombres: Medina Romero Carlos Pedro

DNI: 21570441

UNIVERSIDAD AUTÓNOMA DE ICA

CONSENTIMIENTO INFORMADO

INVESTIGACIÓN DEL FRAUDE INFORMÁTICO EN LA FISCALÍA DE LA PROVINCIA DE SAN ROMÁN – JULIACA, 2024

Institución : Universidad Autónoma de Ica.

Responsables : CHURATA CHUQUIPALLA, Josselyn Karen
QUISPE MACHACA, Dianeth Adelayda

Objetivo de la investigación: Por la presente lo estamos invitando a participar de la investigación que tiene como objetivo determinar si se viene realizando de manera eficaz, la investigación del delito de fraude informático en la Fiscalía Provincial de la Provincia de San Román - Juliaca, 2024.

Al participar del estudio, deberá responder 10 preguntas, las cuales serán respondidas de forma anónima.

Procedimiento: Si acepta ser partícipe de este estudio, usted deberá llenar el cuestionario denominado "Guía de entrevista dirigido a Fiscales". El cual deberá ser resuelto en un tiempo prudencial según cada participante, dicha entrevista será grabada en audio y llevada a cabo por los investigadores.

Confidencialidad de la información: El manejo de la información es a través de códigos asignados a cada participante, las responsables de la investigación garantizan que se respetará el derecho de confidencialidad e identidad de cada uno de los participantes, no mostrándose datos que permitan la identificación de las personas que formaron parte de la muestra de estudio.

Consentimiento: Yo, en pleno uso de mis facultades mentales y comprensivas, he leído la información suministrada por el/las Investigadoras, y acepto, voluntariamente, participar del estudio, habiéndose informado sobre el propósito de la investigación, así mismo, autorizo la toma de fotos (evidencia fotográfica), durante la resolución del instrumento de recolección de datos.

Juliaca, 30 de enero de 2025

Firma: .....
Apellidos y nombres: Supo Pilco
Harold Rudy
DNI: 44735867

Anexo 5: Evidencia de las entrevistas realizadas

UNIVERSIDAD AUTÓNOMA DE ICA

GUIA DE ENTREVISTA DIRIGIDO A FISCALES

La finalidad de la entrevista es buscar información relacionada con el tema de la **"Investigación del Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024".**

Entrevistado: [redacted]

Cargo: [redacted]

Institución: [redacted]

INSTRUCCIONES: Lea detenidamente el presente cuestionario de entrevista y desde su vasta experiencia, conocimientos y opinión sobre el tema, responda de manera clara y veraz, tomando en cuenta que las respuestas consignadas tendrán por finalidad obtener los resultados y por tanto ayudarnos a cumplir con nuestros objetivos. La finalidad de la entrevista es buscar información relacionada con el tema de la **"Investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024"**

OBJETIVO GENERAL

Determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

1.- En base a su experiencia, **¿Cuántas denuncias por el delito de fraude informático ingresan mensualmente a su despacho y cuáles serían los factores de su comisión?**

En promedio ingresan 7 denuncias mensualmente, en donde utilizan los avances tecnológicos enviando links para obtener datos personales o astutos que no les deposite a un numero de cuenta:

2.- Referente a la pregunta anterior, **¿Cuál es la proporción de casos de fraude informático que se archivan frente a los que avanzan a la etapa de formalización?**

1

Del 100%: solo el 10% se formaliza y el resto se archiva.

OBJETIVO ESPECÍFICO 01

Analizar las causas que dificultan la eficacia de la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román - Juliaca.

3.- Desde su experiencia, **¿Cuáles son las diligencias necesarias para la investigación del delito de fraude informático y cuál de ellas suele demorar más tiempo en recabarse?**

En principio la declaración del agraviado y pericias a ello la localización de la dirección IP y la que más suele demorar es el levantamiento del secreto bancario y levantamiento del secreto de las comunicaciones.

4. En base a la pregunta anterior, **¿Cuáles son las principales limitaciones que enfrenta, en la etapa de la investigación preliminar por el delito fraude informático?**

La falta de capacitación necesaria tanto personal fiscal como administrativo para poder entregar este delito, así como falta de especialistas todo cada ingreso en peritos y peritos especializados etc.

5.- A su criterio, **¿Encontró limitaciones en el marco normativo actual que dificulten su labor como fiscal en la investigación del delito de fraude informático?** Si es así, **¿podría mencionar cuáles son esas limitaciones?**

No la normas no dan respuesta a lo que investiga por ese lado no existe una limitación pero podría mencionar alguna.

6.- En base a su experiencia, **¿Cuáles son las causas que contribuyen al archivo de investigaciones del delito de fraude informático?**

La carga procesal no deja que nos aboquemos exclusivamente a un solo delito, el desarrollo del agraviado y la falta de identificación del imputado, demoras en la remisión de medios probatorios y la falta de nuevas tecnologías.

7.- Asu criterio, **¿Qué estrategias se podrían implementar para mejorar la eficacia en la resolución de casos del fraude informático?**

Por un lado, la creación de fiscalías especializadas y por otro lado que dichas fiscalías deberán estar dotado de personal fiscal debidamente capacitado y contar con herramientas necesarias para realizar la persecución de este delito.

OBJETIVO ESPECÍFICO 02

Determinar las herramientas tecnológicas y recursos que estén disponibles para los Fiscales en la Investigación del delito de fraude Informático.

8.- A su criterio, **¿Cuántas veces ha sido capacitado en temas relacionados al delito de fraude informático y cree que es necesaria una mayor capacitación para la existencia de una mejor investigación? ¿Por qué?**

Algunas veces fui capacitado en talleres o cursos y pero las capacitaciones deberían darse mediante ponentes o diplomados sobre tecnología debido a que la carga procesal no da cuenta al hecho de darles interés al caso.

9.- A su criterio, **¿Considera que, la Fiscalía de la Provincia de San Román – Juliaca, ¿cuenta con los recursos tecnológicos y humanos suficientes para investigar el delito de fraude informáticos de manera eficiente? ¿Por qué?**

No, porque en principio carecemos de personal humano donde un contenido ante todos fraudes de que cuenta la fiscalía de un equipo que trabaje de forma efectiva, siempre contamos con las herramientas tecnológicas apropiadas.

10.- En base a su experiencia **¿Cómo se pueden optimizar los recursos y herramientas disponibles para abordar eficazmente los casos de fraude informático?**

Yo no conto una la creación de fiscalías especializadas en cada distrito fiscal que cuenten con personal capacitado el cual pueda trabajar de forma óptima y teniendo como laboratorio peritos para ver el delito, debido a que solo a cierta cierta unidad encargada en el ámbito de lima o de cual tenemos acá entre todos nos [illegible] con los medios probatorios, [illegible] al [illegible] en el tipo de delito [illegible] puede [illegible]

4

UNIVERSIDAD AUTÓNOMA DE ICA

GUIA DE ENTREVISTA DIRIGIDO A FISCALES

La finalidad de la entrevista es buscar información relacionada con el tema de la **"Investigación del Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024".**

Entrevistado: [redacted]

Cargo: [redacted]

Institución: [redacted]

INSTRUCCIONES: Lea detenidamente el presente cuestionario de entrevista y desde su vasta experiencia, conocimientos y opinión sobre el tema, responda de manera clara y veraz, tomando en cuenta que las respuestas consignadas tendrán por finalidad obtener los resultados y por tanto ayudarnos a cumplir con nuestros objetivos. La finalidad de la entrevista es buscar información relacionada con el tema de la **"Investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024"**

OBJETIVO GENERAL

Determinar si se viene realizando de manera eficaz, la investigación del delito de Fraude Informático en la Fiscalía de la Provincia de San Román – Juliaca, 2024.

1.- En base a su experiencia, **¿Cuántas denuncias por el delito de fraude informático ingresan mensualmente a su despacho y cuáles serían los factores de su comisión?**

Ocho denuncias mensualmente

2.- Referente a la pregunta anterior, **¿Cuál es la proporción de casos de fraude informático que se archivan frente a los que avanzan a la etapa de formalización?**

1

Se advierte entre 80 % y 90 %.

OBJETIVO ESPECÍFICO 01

Analizar las causas que dificultan la eficacia de la investigación del delito de fraude informático en la Fiscalía de la Provincia de San Román - Juliaca.

3.- Desde su experiencia, ¿Cuáles son las diligencias necesarias para la investigación del delito de fraude informático y cuál de ellas suele demorar más tiempo en recabarse?

Las diligencias necesarias serían más de cuestión tecnología.

4. En base a la pregunta anterior, **¿Cuáles son las principales limitaciones que enfrenta, en la etapa de la investigación preliminar por el delito fraude informático?**

En este despacho falta Tecnología

5.- A su criterio, **¿Encontró limitaciones en el marco normativo actual que dificulten su labor como fiscal en la investigación del delito de fraude informático?** Si es así, **¿podría mencionar cuáles son esas limitaciones?**

El tipo penal está escrito de manera maravillosa, es decir, no hay limitaciones en el marco normativo.

2

6.- En base a su experiencia, **¿Cuáles son las causas que contribuyen al archivo de investigaciones del delito de fraude informático?**

.....

.....

La principal sería la falta de tecnología.

.....

.....

7.- Asu criterio, **¿Qué estrategias se podrían implementar para mejorar la eficacia en la resolución de casos del fraude informático?**

.....

Para mí debería haber una unidad especializada en la policía que se dote de esos equipos especializados para poder identificar el fraude informático ello conforme a la ley.

OBJETIVO ESPECÍFICO 02

Determinar las herramientas tecnológicas y recursos que estén disponibles para los Fiscales en la Investigación del delito de fraude Informático.

8.- A su criterio, **¿Cuántas veces ha sido capacitado en temas relacionados al delito de fraude informático y cree que es necesaria una mayor capacitación para la existencia de una mejor investigación? ¿Por qué?**

.....

Nunca he sido capacitado en este tema del delito de Fraude Informático.

.....

.....

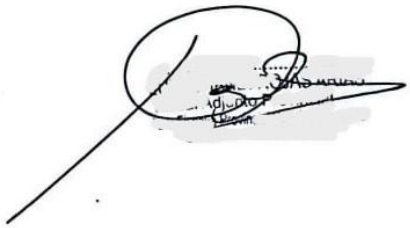
9.- A su criterio, **¿Considera que, la Fiscalía de la Provincia de San Román – Juliaca, ¿cuenta con los recursos tecnológicos y humanos suficientes para investigar el delito de fraude informáticos de manera eficiente? ¿Por qué?**

.....

No, porque no nos han capacitado tanto Asistentes a fiscales, para al menos saber de como empezar o como se puede investigar el delito informatico, estamos al libre albedrio, así a nivel nacional no.

10.- En base a su experiencia **¿Cómo se pueden optimizar los recursos y herramientas disponibles para abordar eficazmente los casos de fraude informático**

.....
.....No...hay....herramientas...y...recursos...humanos....tampoco.....
.....
.....en....conclusion.....con...la.....capacitación.....y....tecnología:.....
.....
.....
.....



Anexo 6: Evidencia fotográfica

Ilustración 1. Imagen de la entrevista con el Fiscal Adjunto Provincial

Ilustración 2. Imagen de la entrevista con el fiscal provincial

Ilustración 3. Imagen de la entrevista con el Fiscal Adjunto Provincial

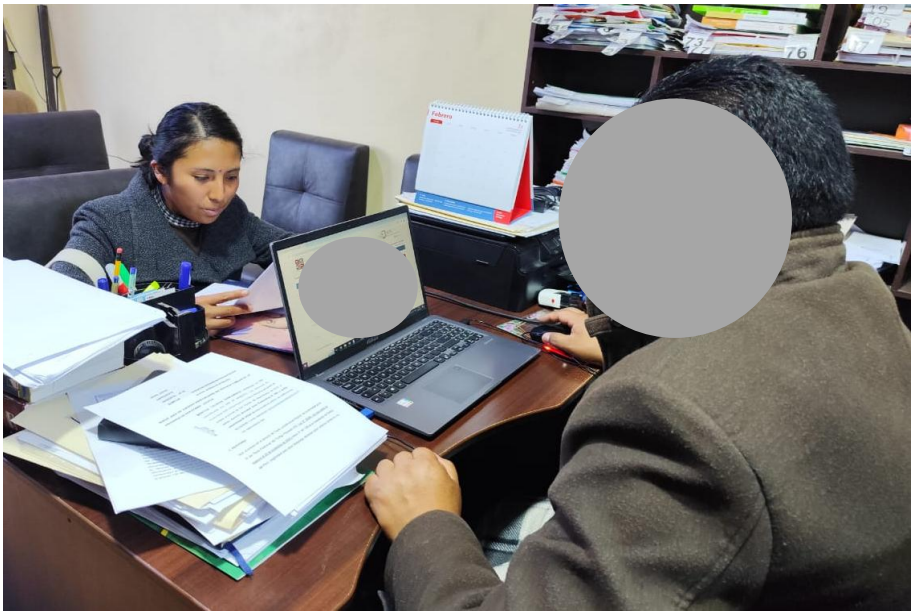


Ilustración 4. Imagen de la entrevista con el Fiscal Adjunto Provincial

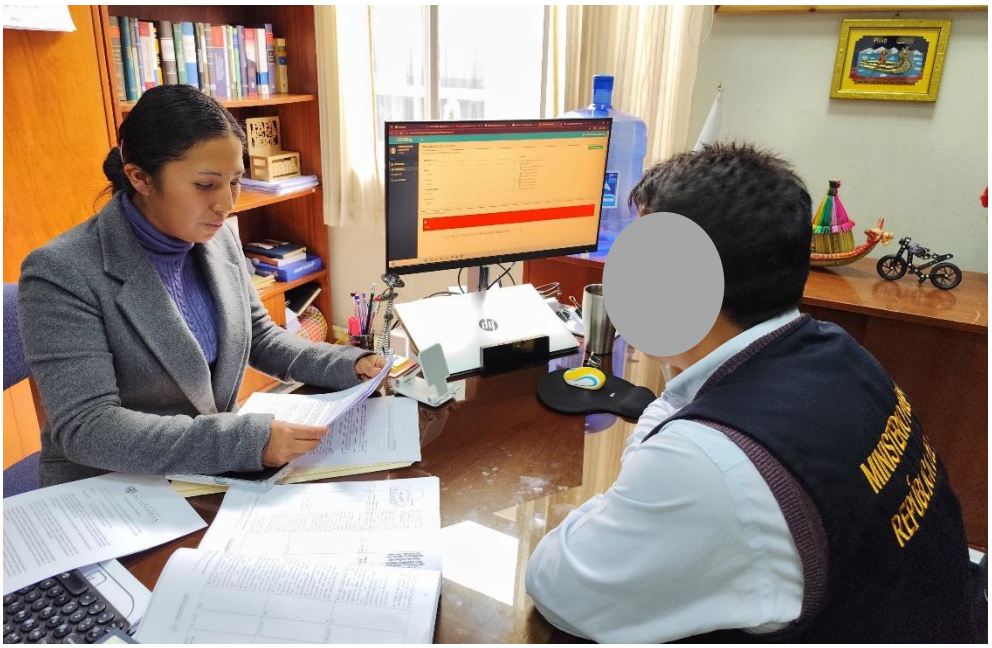


Ilustración 5. Imagen de la entrevista con el fiscal provincial

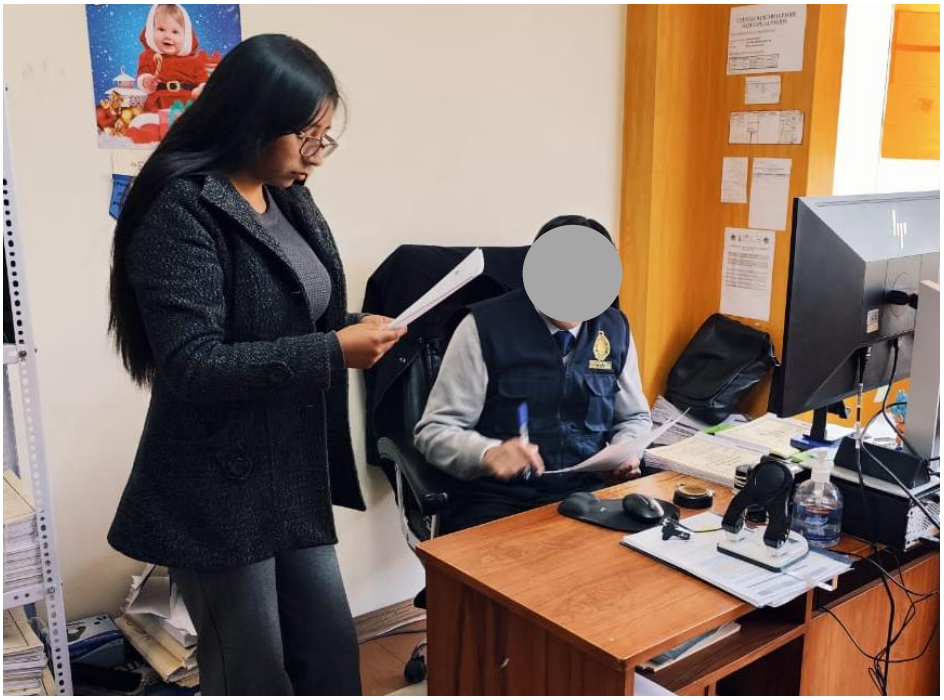


Ilustración 6. Imagen de la entrevista con el Fiscal Adjunto Provincial

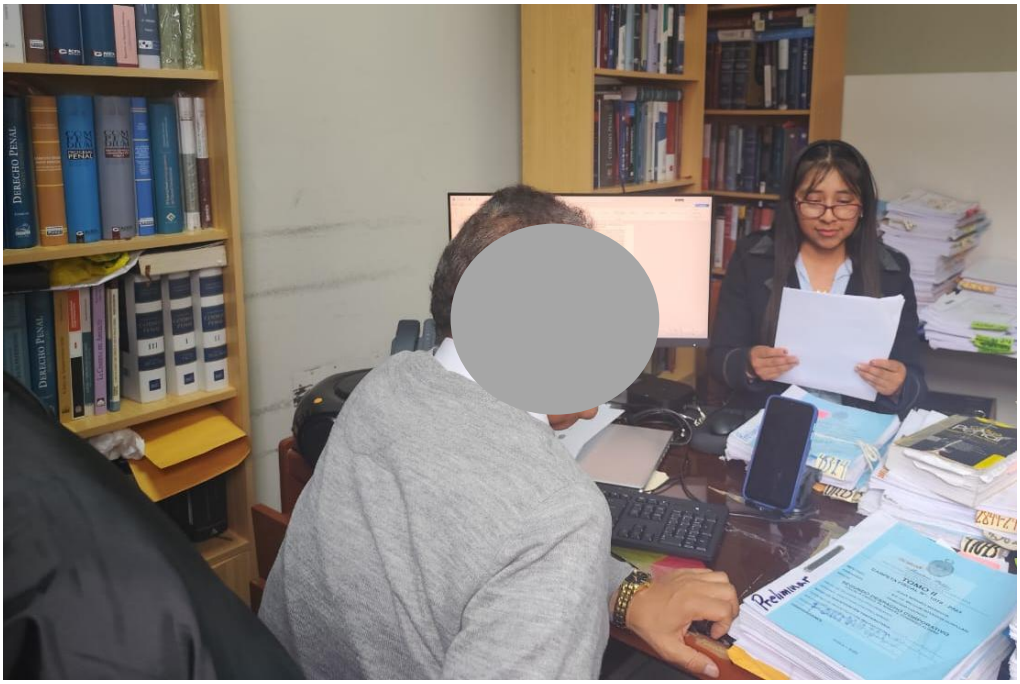


Ilustración 7. Imagen de la entrevista con el Fiscal Adjunto Provincial

Anexo 7: Informe de Turnitin al 7% de similitud

TESIS - JOSELYN y DIANETH- FRAUDE INFORMATICO.docx

2025

2025

Universidad Autónoma de Ica

Detalles del documento

Identificador de la entrega
trn:oid:::3117:440422781

Fecha de entrega
18 mar 2025, 8:41 a.m. GMT-5

Fecha de descarga
18 mar 2025, 9:00 a.m. GMT-5

Nombre de archivo
TESIS - JOSELYN y DIANETH- FRAUDE INFORMATICO.docx

Tamaño de archivo
4.5 MB

100 Páginas

16.115 Palabras

93.889 Caracteres

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Small Matches (less than 15 words)

Top Sources

6% Internet sources
0% Publications
5% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.