UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Delitos cibernéticos en Perú 2023: Análisis y propuesta de prevención para una mayor responsabilidad bancaria

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Derecho Penal y Procesal Penal

AUTORA:

Carlin Ruiz, Licenia Esmith (orcid.org/0009-0001-1755-8778)

ASESORES:

Dra. Alva Diaz, Lyda Palmira (orcid.org/0000-0002-3230-2981)

Dr. Florian Plasencia, Roque Wilmar (orcid.org/0000-0002-3475-8325)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

CHIMBOTE - PERÚ

2024

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Autenticidad de los Asesores

Nosotros, ALVA DIAZ LYDA PALMIRA , FLORIAN PLASENCIA ROQUE WILMAR, docente de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - CHIMBOTE, asesores de Tesis titulada: "Delitos Cibernéticos en Perú 2023: Análisis y propuesta de prevención para una mayor responsabilidad bancaria", cuyo autor es CARLIN RUIZ LICENIA ESMITH, constato que la investigación tiene un índice de similitud de 9%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

Hemos revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

CHIMBOTE, 08 de Setiembre del 2024

Apellidos y Nombres del Asesor:	**Firma**
ALVA DIAZ LYDA PALMIRA **DNI:** 06240404 **ORCID:** 0000-0002-3230-2981	Firmado electrónicamente por: ADIAZLP el 08-09-2024 21:44:34
FLORIAN PLASENCIA ROQUE WILMAR **DNI:** 27144066 **ORCID:** 0000-0002-3475-8325	Firmado electrónicamente por: RFLORIANP el 08-09-2024 21:44:34

Código documento Trilce: TRI - 0866235

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Originalidad del Autor

Yo, CARLIN RUIZ LICENIA ESMITH estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - CHIMBOTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Delitos Cibernéticos en Perú 2023: Análisis y propuesta de prevención para una mayor responsabilidad bancaria", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	Firma
LICENIA ESMITH CARLIN RUIZ **DNI:** 42265964 **ORCID:** 0009-0001-1755-8778	Firmado electrónicamente por: LCARLINRU el 23-07-2024 09:28:30

Código documento Trilce: TRI - 0832640

INVESTIGA UCV

Dedicatoria

Dedico este proyecto, titulado ‘Delitos Cibernéticos en Perú 2023: Análisis y propuesta de prevención para una mayor responsabilidad bancaria’, a mis queridas hijas, Luana y Gaela y a mi madre Rosita. Este trabajo es un testimonio de mi esfuerzo por contribuir a un mundo más seguro y justo para ustedes y para todos.

La autora

Agradecimiento

Agradezco a todos los que me han apoyado en este viaje, especialmente a mis hijas y a mi madre Rosita, que han sido mi mayor motivación.

En segundo lugar, expreso mi sincero agradecimiento a la Universidad César Vallejo por brindarme la oportunidad de realizar esta investigación. A mis asesores de tesis, cuyos valiosos consejos y orientación han sido fundamentales para el desarrollo de este proyecto, les agradezco profundamente por su dedicación y compromiso.

Este proyecto tiene como objetivo determinar los factores que contribuyen a que las fiscalías penales en Perú archiven las denuncias por fraude informático y valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos para que también los bancos asuman una mayor responsabilidad en la lucha contra los delitos cibernéticos, un tema de gran importancia en nuestra sociedad digital.

Espero que este trabajo pueda hacer una diferencia positiva y ayudar a prevenir futuros delitos cibernéticos.

La autora

Índice de contenidos

Índice de tablas

Resumen

La presente investigación se enmarca en el Objetivo de Desarrollo Sostenible (ODS) 16: Paz, justicia e instituciones sólidas, con el propósito de analizar las causas y consecuencias del archivo de denuncias por delito informático por parte de las fiscalías penales en Perú y evaluar la responsabilidad de las entidades bancarias en estos casos durante el año 2023. Los objetivos específicos incluyen determinar las razones del archivo de denuncias, analizar el rol de las entidades bancarias, valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos, desarrollar recomendaciones para las fiscalías penales y crear un marco de acción conjunto para prevenir y gestionar delitos cibernéticos. Se adopta un enfoque cualitativo, con entrevistas a fiscales y revisión de casos de fraude informático. La población en estudio incluye fiscales penales y casos de fraude informático reportados en 2023. Los principales resultados muestran una falta de elementos de convicción suficientes para identificar a los responsables y una tendencia a resolver los conflictos por vías ajenas a lo penal, como INDECOPI o la Defensoría del Consumidor Financiero. Las conclusiones resaltan la necesidad de medidas preventivas más rigurosas y de una legislación actualizada para reducir la incidencia de delitos cibernéticos y mejorar la seguridad financiera de los clientes.

Palabras clave: Delito informático, Responsabilidad, prevención del crimen, legislación.

Abstract

This research is part of Sustainable Development Goal (SDG) 16: Peace, justice and strong institutions, with the purpose of analyzing the causes and consequences of the filing of cybercrime complaints by criminal prosecutors in Peru and assessing the responsibility of banking entities in these cases during 2023. The specific objectives include determining the reasons for the filing of complaints, analyzing the role of banking entities, proposing legislative changes, developing recommendations for criminal prosecutors and creating a joint action framework to prevent and manage cybercrimes. A qualitative approach is adopted, with interviews with prosecutors and a review of computer fraud cases. The population under study includes criminal prosecutors and cases of computer fraud reported in 2023. The main results show a lack of sufficient evidence to identify those responsible and a tendency to resolve conflicts through non-criminal channels, such as INDECOPI or the Financial Consumer Ombudsman. The findings highlight the need for more rigorous preventative measures and updated legislation to reduce the incidence of cybercrime and improve the financial security of customers.

Keywords: Cybercrime, Accountability, Crime Prevention, Legislation.

I. INTRODUCCIÓN

En 2023, los delitos cibernéticos se convirtieron en una amenaza creciente a nivel global, y Perú no fue la excepción. Estos crímenes afectaron gravemente a los clientes bancarios, quienes sufrieron la sustracción de su dinero debido a vulnerabilidades tecnológicas que los ciberdelincuentes aprovecharon para cometer fraudes. En el contexto de la Ley 30096, Ley de Delitos Informáticos, estos delitos incluyeron el fraude informático, regulado en el artículo 8, y la suplantación de identidad, contemplada en el artículo 9, ambos capítulos tratan sobre delitos contra el patrimonio y la fe pública. Además, muchas denuncias involucraron estafa agravada, según lo estipulado en el artículo 196-A del Código Penal Peruano, que abarca la sustracción o acceso a datos de tarjetas emitidas por el sistema financiero. Sin embargo, lo más preocupante es que las fiscalías penales tendían a archivar estas denuncias, lo que hacía aún más alarmante la situación.

El diario El Peruano reportó que el fraude informático se ha convertido en el delito informático más investigado en Perú durante 2023, con un incremento del 58% en los casos respecto al año anterior. En el último año, se registraron 21,842 denuncias en las fiscalías provinciales penales y mixtas del país, y entre enero y febrero de 2024 se contabilizaron 3,903 denuncias. Aurora Castilla jefa de la Unidad Fiscal Especializada en Ciberdelincuencia, afirmó que el fraude informático sigue siendo el delito más denunciado y el que ha tenido más sentencias en el año en curso (El Peruano, 2024).

Frente a esta realidad, la investigación se enfocó en el análisis de los delitos cibernéticos en Perú básicamente en el distrito Fiscal del Santa y en el manejo de estos por parte de las fiscalías penales, así como en la responsabilidad de las entidades bancarias, de ello surgió la inquietud de responder al enigma ¿Cuáles son los factores que contribuyen a que las fiscalías penales en Perú archiven las denuncias por fraude informático?

La investigación abordó la inacción de las fiscalías penales en Perú ante los crecientes delitos de fraude informático, que afectaron gravemente a clientes bancarios víctimas de suplantación de identidad y robo de dinero. Las denuncias, frecuentemente archivadas sin respuesta adecuada, dejaron a las víctimas sin protección y a los ciberdelincuentes impunes. El estudio se centró en identificar las

razones detrás de esta inacción fiscal y la falta de responsabilización de las entidades bancarias, proponiendo medidas para mejorar la protección ciudadana y reforzar la confianza en la justicia penal frente a estos delitos.

Desde una perspectiva metodológica, la investigación empleó un enfoque cualitativo para examinar las prácticas actuales tanto de las fiscalías penales como de las entidades bancarias. Se indagó en cómo la identificación de los responsables y la percepción de auto exposición al riesgo por parte de las víctimas influían en el proceso judicial. Este enfoque permitió una comprensión integral del problema y proporcionó una base sólida para las recomendaciones prácticas orientadas a mejorar la eficacia del sistema y asegurar una mayor protección para las víctimas de fraude informático.

En términos prácticos, Los hallazgos de la investigación tuvieron el potencial de influir en la reforma de los procedimientos de las fiscalías penales y en la política de responsabilidad bancaria. Dichas reformas pudieron haber incrementado la efectividad en la persecución de los delitos informáticos, además de mejorar la compensación a las víctimas. El impacto práctico se extendió al ámbito social, ya que una mejor gestión de los casos y una respuesta institucional más adecuada fortalecieron la confianza de la sociedad en las instituciones financieras y judiciales. De esta manera, se protegió a los ciudadanos, se redujo el miedo al fraude y se fomentó una mayor estabilidad social (Elson, 1979).

Desde una perspectiva económica, la investigación abordó un problema que generaba pérdidas financieras significativas tanto para individuos como para empresas. La propuesta de reformas y mejoras en la gestión de los casos contribuyó a reducir dichas pérdidas, lo que fortaleció la estabilidad económica general. Menores fraudes implicaron un menor impacto negativo en la economía local y nacional, promoviendo el crecimiento económico y la inversión. A nivel institucional, la investigación influyó en las prácticas de las fiscalías y entidades bancarias, mejorando los procedimientos de investigación y procesamiento de casos, lo que resultó en una mayor eficiencia judicial y mejor protección de fondos y datos bancarios (Smith, 2020).

Se planteó el objetivo general de determinar los factores que contribuyen a que las fiscalías penales en Perú archiven las denuncias por fraude informático. De este objetivo general se desprendieron los siguientes objetivos específicos: a) Identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023; b) Evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos; y c) Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos.

A nivel internacional, tenemos a Morris (2023) quien analizó cómo los avances en informática, telecomunicaciones e Internet facilitaron el surgimiento de conductas fraudulentas asociadas con el uso de medios electrónicos de pago, ella destacó la dificultad de encuadrar estos nuevos delitos en los tipos penales tradicionales, lo cual impulsó una revisión legislativa significativa, ejemplificada por la reforma del Código Penal español en 2010. El trabajo de la autora subrayó la necesidad de una legislación actualizada para abordar eficazmente estos delitos emergentes y evitar la impunidad. Este análisis es particularmente relevante para la investigación sobre delitos cibernéticos en Perú 2023, ya que refleja una problemática similar en la que la legislación y los procedimientos judiciales deben adaptarse para enfrentar la evolución de los fraudes electrónicos.

Desde otro punto de vista, la tesis de Vera (2011) resalta la urgente necesidad de una legislación especializada en delitos informáticos en Honduras, un país sumergido en la revolución digital. La investigación revela que, aunque el Internet y las redes sociales han tenido un impacto positivo en la educación y la comunicación, también han facilitado la comisión de delitos como el fraude y la explotación infantil, que ahora se llevan a cabo en el ámbito digital. El trabajo de Vera se enfoca en los retos que enfrentan las organizaciones, las cuales se ven afectadas por la acción de ciberdelincuentes que operan en las sombras, comprometiendo datos y sistemas para beneficio propio o para extorsionar, utilizando métodos como el malware. Propone una reforma integral a su legislación que defina y aborde los delitos informáticos en una referencia fragmentada en diversas leyes, abarcando desde la gestión inapropiada de la información hasta la destrucción de registros digitales que impiden la recuperación de datos.

En la misma línea Riofrío (2012) realiza un análisis profundo sobre la carencia de disposiciones penales específicas para los delitos informáticos en Ecuador. Su estudio pone de manifiesto el impacto negativo de esta deficiencia legal en la protección de los derechos de los ciudadanos y propone una revisión del Código Penal basándose en un estudio comparativo de legislaciones de varios países. Riofrío sumerge en temas como la doctrina penal y los derechos humanos, evaluando cómo las TIC han cambiado el panorama del crimen transnacional, por lo que las fiscalías penales deben adaptarse a estos cambios. Su análisis, resalta la necesidad de dotar a las fiscalías de recursos tecnológicos y capacitación especializada para enfrentar eficazmente estos nuevos desafíos, similar a la problemática observada en Perú, donde la falta de implementación efectiva y de recursos adecuados en las fiscalías limita la lucha contra los delitos cibernéticos.

Sin embargo, para Nuñez (2022) la crisis sanitaria global desencadenada por el Covid-19 ha acelerado la metamorfosis de los crímenes digitales, el en su investigación de Maestría en posgrado, indica que la necesidad de aislamiento y las nuevas dinámicas sociales han sido el caldo de cultivo para el surgimiento y la proliferación de variantes de delitos en el ciberespacio. Estos incidentes han escalado en número, repercutiendo adversamente en individuos y estructuras corporativas, así como en la estabilidad económica a gran escala. Núñez subraya que la gravedad de estos delitos trasciende la esfera de la seguridad de la información, convirtiéndose en precursores de actividades de lavado de dinero, lo que evidencia la intrincada y multifacética naturaleza del problema que afronta la región. Además, señala que la ciberdelincuencia, al ser un fenómeno global sin barreras, ha evolucionado con rapidez, explotando la interconexión digital para perpetrar actos ilícitos que explotan las falencias de infraestructuras tecnológicas en todo el mundo.

A nivel Nacional, la tesis de Quiroz (2019) examina cómo la creciente dependencia de la tecnología informática en la sociedad ha abierto la puerta a nuevos tipos de criminalidad, especialmente en sectores críticos como la banca y los seguros. A pesar de los avances tecnológicos que han traído innumerables beneficios, también han surgido riesgos significativos, incluyendo la manipulación y destrucción malintencionada de datos. El trabajo de Quiroz establece un precedente importante para futuras investigaciones, ofreciendo una guía técnica y

científica para aquellos encargados de administrar justicia en Lima. Su objetivo es perfeccionar los procesos de investigación y juicio de delitos informáticos y fortalecer la protección de la intimidad personal. La tesis identifica y analiza los factores que contribuyen a la inexactitud en el trabajo de policías, fiscales y jueces en casos de delitos informáticos durante el periodo de 2008 a 2012, buscando soluciones para mejorar la eficacia en tratamiento de estos crímenes.

La tesis de Morales (2016) examina cómo la informática, a pesar de sus ventajas, ha sido el cultivo para los otros delitos cibernéticos. Destaca que el desarrollo tecnológico abrió la puerta a crímenes antes impensables, con repercusiones en la privacidad y daños tanto materiales como morales. La era de Internet ha cambiado la percepción del crimen, donde el temor a los delitos cibernéticos se basa más en una evaluación lógica que en una reacción emocional. Critica las medidas legislativas iniciales de Perú en respuesta a los delitos informáticos, argumentando que no capturan la complejidad de los crímenes modernos. Aunque se han hecho intentos por actualizar las leyes, como en los casos de turismo sexual y fraude electrónico, aún hay deficiencias en la regulación. Cita como ejemplo el Artículo 2º de la Ley de Delitos Informáticos, que sanciona el acceso ilícito sin considerar las intenciones detrás de la acción, y el Artículo 3º, que introduce términos ambiguos y potencialmente superfluos que podrían ir en contra de los principios fundamentales del Derecho Penal.

Así también la defensoría del pueblo indico que los delitos cibernéticos en Perú están experimentando un crecimiento alarmante, lo que representa un desafío urgente que requiere atención y soluciones efectivas. Según un informe reciente, las denuncias por ciberdelincuencia se incrementaron en un 150% en el 2023, reflejando una tendencia preocupante que se extiende más allá de las fronteras nacionales. Este aumento se atribuye a la adopción masiva de tecnologías digitales y a la falta de medidas de seguridad adecuadas. En este contexto, la calidad de las respuestas institucionales y la eficacia de las estrategias de prevención son críticas, lo que evidencia que la gestión en Perú sobre la ciberseguridad y la protección contra delitos informáticos son insuficientes, lo que subraya la necesidad de un conocimiento más profundo sobre la percepción de la seguridad digital y un sistema de gestión de la calidad mejorado para combatir eficazmente la ciberdelincuencia (Poder Judicial, 2023).

Diagnostico que no es ajeno con la realidad Santeña, especialmente en la fiscalía provincial penal corporativa del Santa, como es el caso de Melquin Joel Trujillo Gamarra un operador de la empresa COGA S.A., confiaba en la seguridad de su cuenta bancaria en el Banco Continental - BBVA. Utilizaba un aplicativo móvil instalado en su teléfono celular para acceder a su información financiera. Sin embargo, un mensaje de texto cambió su vida de manera drástica, pues el 11 de abril de 2020, Melquin recibió un mensaje en su teléfono celular N° 984000479. El remitente, supuestamente el Banco Continental - BBVA, le solicitaba actualizar sus datos a través de un enlace. Sin sospechar nada, Melquin accedió al enlace y proporcionó sus datos personales y bancarios. Creyó que estaba cumpliendo con una solicitud legítima del banco. Días después, se dio cuenta de que se había realizado una transferencia no autorizada desde su cuenta hacia el teléfono celular N° 934838456. La pérdida financiera fue significativa y aquí es donde la situación se complica. A pesar de la gravedad del fraude, el banco no asumió responsabilidad ni devolvió el dinero sustraído. Melquin quedó en una situación desesperada, enfrentando una pérdida financiera considerable. El caso fue archivado sin consecuencias para la entidad financiera. Esta impunidad bancaria no solo afecta a los individuos, sino también erosiona la confianza en todo el sistema financiero (Ministerio Publico, 2023).

Para comprender el problema de los delitos cibernéticos, se exploraron diversas teorías relevantes, entre ellas la Teoría de la Tipicidad en Cibercrimen formulada por Posada (2010). Esta teoría explicó cómo los delitos cibernéticos desafían y amplían el concepto de tipicidad penal, ya que su rápida evolución y complejidad técnica frecuentemente superan los marcos legales existentes, generando vacíos legales. Esto contribuye a la dificultad de tipificar y sancionar adecuadamente dichos delitos, lo que, en consecuencia, provoca la impunidad en muchos casos de fraude informático debido a la falta de un marco legal actualizado y específico.

Complementariamente, la Teoría de las Obligaciones de Resultado propuesta por Perez (2018) aborda la responsabilidad de las entidades bancarias en la protección de los fondos y datos financieros de sus clientes frente a fraudes electrónicos. Según esta teoría, las instituciones financieras tienen una obligación casi objetiva de asegurar la seguridad en las transacciones financieras. Esta teoría

establece que las entidades bancarias deben implementar medidas de seguridad adecuadas y adoptar una postura proactiva para prevenir fraudes, así como educar a sus clientes sobre prácticas seguras en línea, el exponente subraya que la creciente frecuencia de transacciones electrónicas y la proliferación de delitos cibernéticos resaltan la importancia de una responsabilidad activa por parte de los bancos para mantener la confianza en el sistema financiero digital. Esta teoría postula que son los bancos quienes deben de implementar medidas de seguridad adecuadas para prevenir el delito de fraude informático, en base a ello, alguna perpetuación de este delito debe ser responsabilidad de la entidad Bancaria.

Otra teoría relevante es la Teoría del Delito de Rutina, propuesta por Felson (1979) Esta teoría sostiene que la probabilidad de que ocurra un delito depende de la presencia simultánea de tres factores: un delincuente motivado, un objetivo adecuado y la ausencia de un guardián capaz. En el contexto de los delitos cibernéticos, los bancos actúan como guardianes responsables de proteger los fondos y datos de sus clientes. La teoría sugiere que aumentando la responsabilidad de los bancos y mejorando sus medidas de seguridad, se puede reducir la probabilidad de delitos cibernéticos. En merito a ello Peña (2019) un doctrinario indica que esta teoría es consistente con la propuesta de incrementar la responsabilidad bancaria en la prevención y gestión de delitos cibernéticos, sugiriendo que las entidades bancarias son guardianes capaces, requisito indispensable para evitar que ocurra un delito de fraude informático.

Por otro lado, la Teoría de la Auto exposición al Peligro, formulada por Roxin (2006) ofrece una perspectiva crítica para entender la justificación de algunas fiscalías al archivar casos de delitos cibernéticos. Roxin argumentó que la auto exposición al peligro puede ser tratada como un factor independiente en la imputación. Según esta teoría, si una persona expone voluntariamente su propio riesgo, la responsabilidad por los daños puede ser atribuida a la persona que asumió el peligro, excluyendo la responsabilidad del tercero que facilitó el riesgo. Martínez (2019) discuten con la teoría de la auto puesta en peligro indicando que, en casos de fraude cibernético, si el cliente del banco se expone conscientemente a riesgos, la responsabilidad del banco podría verse reducida, puesto que es la actuación del cliente del banco quien permite la perpetuación de algún delito de fraude informático.

La problemática de los delitos cibernéticos en Perú durante 2023 se centraba en la creciente vulnerabilidad de los clientes bancarios frente a fraudes y otros delitos informáticos. Este fenómeno no solo afectaba la seguridad financiera de los individuos, sino que también minaba la confianza en el sistema bancario y en las instituciones encargadas de proteger los derechos de los ciudadanos. Para abordar esta situación, era esencial comprender las teorías y enfoques conceptuales que subyacían a estas problemáticas, así como los aportes teóricos que podrían ofrecer soluciones efectivas (Muñante 2016).

La teoría de la tipicidad en cibercrimen, resultaba fundamental para entender cómo los delitos cibernéticos desafiaban y expandían el concepto de tipicidad penal. Posada destacaba que estos delitos, por su naturaleza, a menudo caían en vacíos legales debido a su rápida evolución y complejidad técnica. La falta de un marco legal actualizado y específico contribuía a la dificultad en la tipificación y sanción de estos delitos. Esto subrayaba la necesidad de una revisión y adaptación constante de las leyes para abordar adecuadamente los delitos cibernéticos y evitar que los delincuentes se beneficiaran de lagunas jurídicas (Gamarra, 2020).

En paralelo, la teoría de las obligaciones de resultado ofrecía una perspectiva sobre la responsabilidad de las entidades bancarias en la protección de los fondos y datos financieros de sus clientes. Según esta teoría, las entidades bancarias tenían una responsabilidad casi objetiva de asegurar la ejecución segura de las transacciones financieras. La falta de medidas de seguridad adecuadas o la ausencia de una diligencia debida podría resultar en una responsabilidad significativa para los bancos en casos de fraude electrónico. Este enfoque resaltaba la importancia de que las instituciones financieras no solo implementaran robustas medidas de seguridad, sino que también educaran a sus clientes sobre prácticas seguras en línea.

La teoría del delito de rutina, aportaba otra dimensión al análisis de los delitos cibernéticos. Según esta teoría, la probabilidad de que ocurriera un delito dependía de la presencia de un delincuente motivado, un objetivo adecuado y la ausencia de un guardián capaz. En el contexto de los delitos cibernéticos, los bancos podían ser vistos como los guardianes. La falta de medidas de seguridad efectivas por parte de los bancos aumentaba la vulnerabilidad de los clientes y

facilitaba la comisión de fraudes. Esta teoría sugería que mejorar las medidas de seguridad y aumentar la vigilancia por parte de los bancos podría reducir significativamente la incidencia de estos delitos (Maya, 2019).

En contraste, la teoría de la auto exposición al peligro, ofrecía una explicación de por qué algunas fiscalías optaban por archivar casos de delitos cibernéticos. Según Roxin, si una víctima se exponía voluntariamente al riesgo, la responsabilidad podría recaer en la víctima misma en lugar de en el delincuente. Esto podía llevar a que las fiscalías consideraran que ciertos casos de fraude cibernético no ameritaban una persecución penal activa si se percibía que la víctima no había tomado las precauciones necesarias. Esta teoría planteaba la importancia de la autoprotección y la educación de los usuarios en prácticas seguras en línea, aunque también resaltaba la necesidad de un equilibrio justo en la atribución de responsabilidades (Sampiere, 2018).

Entonces, estas teorías en el estudio resaltaron la necesidad de una acción concertada por parte de las instituciones financieras, las fiscalías y los legisladores para abordar de manera efectiva los desafíos planteados por los delitos cibernéticos. Reformas legales específicas, la creación de unidades especializadas en delitos informáticos dentro de las fiscalías peruanas equipadas con tecnología avanzada y personal altamente capacitado en ciberseguridad y derecho informático, una mayor responsabilidad bancaria, una educación continua para los usuarios eran fundamentales para reducir la incidencia de estos delitos y mejorar la seguridad financiera en Perú (Navarro, 2022).

Inicialmente, se afirmaba que la implementación de medidas preventivas más rigurosas por parte de las fiscalías penales y entidades bancarias, junto con una legislación reforzada, sería clave para reducir los delitos cibernéticos en Perú y mejorar la seguridad financiera y la confianza en el sistema bancario en 2023. Esta hipótesis se basaba en la teoría de las obligaciones de resultado, que planteaba una responsabilidad casi objetiva de los bancos en la protección de fondos y datos de sus clientes. La teoría del delito de rutina también reforzaba esta idea, al sugerir que una mayor seguridad por parte de las instituciones reduciría la probabilidad de fraudes. Sin embargo, se proponía también que estas medidas no tendrían un impacto significativo si los usuarios no tomaban las precauciones

necesarias, según la teoría de la auto exposición al peligro. En este caso, la falta de autoprotección limitaría la efectividad de las reformas propuestas (Bermúdez, 2021).

Es importante tener en cuenta que, para entender este tipo de delitos, se recurrió a sus definiciones, siendo que los crímenes cibernéticos, igualmente referidos como crímenes informáticos, representan una amenaza considerable en el contexto actual de la tecnología. Dichos crímenes están asociados con el uso de computadoras y redes; en ciertas situaciones, las computadoras son el medio a través del cual se perpetra el crimen, mientras que, en otras, son el blanco directo del acto delictivo (Jiménez, 2022).

Los delitos cibernéticos abarcan una variedad de actividades ilícitas que se ejecutan a través de la red o con la ayuda de dispositivos digitales. Estos crímenes incluyen el robo de identidad, la piratería, el phishing, las botnets, el ciberespionaje, la extorsión en línea, el malware, el ransomware, la pornografía infantil y el acoso cibernético. Estas acciones, reconocidas legalmente como delictivas, requieren de la tecnología informática para su perpetración y tienen consecuencias graves tanto en el ámbito personal, así como también en el sector colectivo (Gonzales, 2021).

Los delitos cibernéticos se definen como conductas ilícitas perpetradas a través de sistemas informáticos, redes y dispositivos digitales, que pueden involucrar la manipulación, destrucción o acceso no autorizado a datos y sistemas. Estos delitos abarcan una amplia gama de actividades delictivas, desde el fraude y la estafa hasta el espionaje y el sabotaje informático. Según Tellez (2021), los delitos cibernéticos no solo afectan la integridad y disponibilidad de la información, sino que también comprometen la privacidad y seguridad de los individuos y organizaciones.

La legislación y el marco normativo en Perú sobre delitos cibernéticos abordan las leyes y regulaciones diseñadas para prevenir, sancionar y controlar los delitos cometidos en el entorno digital. San Martin (2012) indica que el marco normativo peruano ha evolucionado lentamente para adaptarse a los nuevos desafíos que presentan los delitos cibernéticos, con una legislación que todavía enfrenta dificultades para abarcar todas las formas de ciberdelincuencia emergentes.

Las medidas preventivas y estrategias de manejo por parte de instituciones bancarias incluyen prácticas y políticas destinadas a proteger los sistemas financieros y la información de los clientes contra los ataques cibernéticos. Según Pernias (2020), estas medidas pueden incluir la implementación de tecnologías de seguridad avanzadas, procedimientos internos de monitoreo y auditoría, así como la formación continua del personal para detectar y responder a amenazas cibernéticas.

La gestión de casos de delitos cibernéticos por parte de las fiscalías implica la investigación, procesamiento y resolución de casos relacionados con la ciberdelincuencia. Según Ramos (2022), esta gestión requiere de habilidades especializadas y recursos adecuados para manejar la complejidad técnica de los delitos cibernéticos, además de una colaboración efectiva con entidades tecnológicas y de seguridad.

La responsabilidad y el rol de las entidades bancarias en el contexto de delitos cibernéticos implican garantizar la seguridad de las transacciones y la protección de la información del cliente. Porthé (2007) sostiene que las entidades bancarias tienen la obligación de implementar medidas de seguridad robustas y responder de manera adecuada a los incidentes de fraude, para evitar daños financieros y preservar la confianza del cliente.

Las perspectivas y experiencias de profesionales en el ámbito de los delitos cibernéticos se refieren a la visión y vivencias de expertos que trabajan en la prevención, investigación y resolución de estos delitos. Donolo (2018) señala que las experiencias de estos profesionales son fundamentales para comprender las dificultades prácticas y las brechas existentes en la lucha contra la ciberdelincuencia, así como para desarrollar estrategias más efectivas.

I. METODOLOGÍA

La presente investigación se enmarcó dentro del ámbito de la investigación básica, conforme al Manual Oslo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2018). Este tipo de investigación se caracterizó por su enfoque en la adquisición de conocimientos fundamentales sin una aplicación inmediata, buscando entender los principios subyacentes y generar resultados que beneficien a la comprensión de la ciberseguridad y la responsabilidad bancaria en Perú. La investigación básica tuvo como propósito profundizar en el conocimiento de fenómenos complejos, sentando las bases para futuras estrategias de prevención y protección en el ámbito de la seguridad cibernética y el sistema financiero.

El enfoque de investigación adoptado en este estudio fue cualitativo, subdividido en un diseño fenomenológico. Este enfoque se centró en explorar y comprender en profundidad las experiencias, percepciones y significados asociados con el fenómeno de los delitos cibernéticos y la responsabilidad bancaria en Perú. Según Hernández (2018), el enfoque cualitativo permite recolectar datos detallados y ricos en contexto a través de técnicas como entrevistas y análisis documental, proporcionando una visión integral de las dinámicas y complejidades involucradas en la problemática investigada. El diseño fenomenológico, en particular, se enfocó en captar y describir la esencia de las experiencias vividas por los participantes en relación con los delitos cibernéticos y su manejo por parte de los fiscales penales.

Este método fue especialmente útil para identificar patrones, interpretar comportamientos y elaborar teorías basadas en la observación directa y la interacción con los participantes del estudio. Al no buscar generalizar los resultados a través de una muestra representativa, sino más bien profundizar en la comprensión del fenómeno, el enfoque cualitativo se mostró adecuado para los objetivos de esta investigación, permitiendo obtener insights valiosos que pudieran guiar futuras acciones y políticas en el ámbito de la ciberseguridad y la responsabilidad bancaria (Mitnick,2017).

En el estudio se definieron categorías específicas de interés, junto con sus subcategorías e indicadores, para proporcionar una estructura clara y coherente al análisis de los datos. A continuación, se detallan las principales categorías de estudio, sus definiciones conceptuales, subcategorías e indicadores correspondientes.

La categoría de delitos cibernéticos se definió como las acciones ilícitas realizadas mediante el uso de tecnologías de la información y la comunicación, cuyo objetivo era comprometer la seguridad de los sistemas informáticos, la integridad de los datos y la privacidad de las personas. Dentro de esta categoría, se exploraron las siguientes subcategorías: tipos de delitos cibernéticos, métodos de ejecución y frecuencia e impacto de estos delitos. Los indicadores para esta categoría incluyeron el número de casos reportados, la descripción de los métodos empleados y la evaluación del impacto financiero y personal en las víctimas (Clark,2021).

La responsabilidad bancaria se definió como las obligaciones y deberes que tenían las entidades bancarias para proteger los fondos y datos financieros de sus clientes. Las subcategorías dentro de esta categoría fueron medidas de seguridad, respuesta a incidentes y educación y concienciación. Los indicadores incluyeron la evaluación de políticas de seguridad, el análisis de casos de respuesta a incidentes y el número de programas educativos ofrecidos a los clientes (Harris, 2020).

La gestión de delitos cibernéticos por las fiscalías penales se definió como los procesos y procedimientos seguidos por las fiscalías para investigar, perseguir y resolver casos de delitos cibernéticos. Las subcategorías incluyeron procedimientos de investigación, barreras y desafíos, y eficacia en la resolución de casos. Los indicadores abarcaron la descripción de los procedimientos de investigación, la identificación de barreras comunes y las tasas de resolución de casos (Jenkis, 201).

La legislación y el marco normativo se definieron como el conjunto de leyes, regulaciones y normativas vigentes que regían la prevención, persecución y sanción de delitos cibernéticos en Perú. Las subcategorías incluyeron leyes específicas sobre ciberseguridad, eficacia de la legislación y propuestas de reforma. Los indicadores contemplaron el análisis de leyes específicas, el estudio

de casos para evaluar la efectividad de la legislación y las propuestas documentadas de reformas legales (Johnson, 2022).

Por último, la categoría de prevención y educación en seguridad informática se definió como las estrategias y acciones orientadas a prevenir delitos cibernéticos y a educar a la población sobre prácticas seguras en el uso de tecnologías de la información. Las subcategorías fueron programas de prevención, campañas de concienciación y formación y capacitación. Los indicadores incluyeron la evaluación de programas de prevención, el análisis de campañas de concienciación y el número de programas de formación en seguridad informática.

La población objeto de estudio estuvo constituida por los fiscales que trabajaban en la Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Público en Perú. Se decidió enfocar la investigación en esta fiscalía específica debido a su relevancia y experiencia en la gestión de delitos cibernéticos. El tamaño de la muestra fue determinado utilizando un muestreo intencional, seleccionando a fiscales que pudieran proporcionar información relevante y detallada para el estudio. Se entrevistaron a ocho fiscales de la Segunda fiscalía provincial Penal Corporativa del Santa el día 22 de mayo de 2024. Estos fiscales fueron seleccionados debido a su experiencia directa en la gestión de casos de fraude informático, lo que aseguraba que poseían el conocimiento necesario para contribuir significativamente al entendimiento del fenómeno investigado.

Los criterios de inclusión aplicados fueron que los fiscales debían tener experiencia en la gestión de delitos cibernéticos y estar actualmente activos en la fiscalía mencionada. No se aplicaron criterios de exclusión adicionales, ya que todos los fiscales entrevistados cumplían con los requisitos establecidos. La elección del muestreo intencional permitió seleccionar a individuos que pudieran ofrecer perspectivas valiosas y profundas sobre la problemática de los delitos cibernéticos y la responsabilidad bancaria, asegurando así la relevancia y riqueza de la información recolectada.

Para la recolección de datos en esta investigación, se emplearon diversas técnicas e instrumentos diseñados específicamente para capturar información relevante sobre la gestión de delitos cibernéticos y la responsabilidad bancaria en

Perú. Se utilizaron entrevistas estructuradas y el análisis documental de carpetas fiscales archivadas relacionadas con casos de fraude informático.

Las entrevistas estructuradas se llevaron a cabo con ocho fiscales de la Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Público el 22 de mayo de 2024 a los cuales se les hizo la misma pregunta. Este método permitió obtener información detallada y profunda sobre las percepciones y experiencias de los fiscales en la gestión de delitos cibernéticos. Las entrevistas siguieron una guía de preguntas previamente diseñada, que abarcaba temas como los desafíos en la investigación de delitos cibernéticos, la colaboración con entidades bancarias y la eficacia de las medidas preventivas y cambios legislativos. La guía de entrevistas fue validada por expertos en derecho penal y ciberseguridad, quienes revisaron y proporcionaron retroalimentación para asegurar que las preguntas fueran claras, relevantes y adecuadas para el objetivo del estudio.

Adicionalmente, se realizó un análisis documental centrado en las fichas de revisión de carpetas fiscales relacionadas con casos de fraude informático que habían sido archivados. Este análisis se llevó a cabo utilizando una ficha de revisión de carpetas fiscales, diseñada específicamente para este estudio, que incluyó ítems como datos del caso, razones documentadas para el archivo del caso, barreras encontradas durante la investigación y acciones tomadas por las fiscalías antes de decidir archivar el caso. Este instrumento fue validado mediante un proceso de revisión por pares, en el que participaron fiscales y expertos en derecho penal, quienes evaluaron la pertinencia y claridad de los ítems incluidos.

La validación de los instrumentos se llevó a cabo mediante un proceso de revisión por expertos y un análisis de consistencia interna. Los expertos revisaron los instrumentos para asegurar que fueran adecuados y pertinentes para los objetivos del estudio. Los resultados mostraron un alto nivel de consistencia interna, indicando que los instrumentos utilizados eran fiables y adecuados para la recolección de datos en este estudio.

Los instrumentos diseñados específicamente para este estudio, incluyendo las guías de entrevistas y las fichas de revisión de carpetas fiscales, junto con las fichas de validación firmadas, se adjuntaron en los anexos bajo el título "Fichas de validación de instrumentos para la recolección de datos". Este proceso de

validación aseguró que los datos recolectados fueran válidos y fiables, proporcionando una base sólida para el análisis y las conclusiones del estudio.

Los hallazgos obtenidos del análisis cualitativo se interpretaron en el contexto de las teorías y antecedentes revisados, permitiendo una comprensión integral de la problemática y facilitando la formulación de recomendaciones para mejorar la prevención y gestión de delitos cibernéticos en el entorno bancario. Esta técnica cualitativa proporcionó una visión profunda y matizada de los desafíos enfrentados por las fiscalías y las entidades bancarias en la lucha contra el fraude informático.

En el estudio se utilizó un enfoque cualitativo para analizar los datos obtenidos. Las técnicas aplicadas incluyeron entrevistas a fiscales y revisión de carpetas fiscales. La recolección de datos se realizó mediante entrevistas estructuradas a ocho fiscales de la Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Público, llevadas a cabo el 22 de mayo de 2024. Las entrevistas se transcribieron y analizaron utilizando Excel como herramienta principal para la organización y análisis de la información.

Para el análisis de los datos cualitativos obtenidos de las entrevistas, se utilizó una metodología de codificación temática en Excel. Este proceso incluyó la identificación de temas recurrentes y patrones en las respuestas de los fiscales. Se crearon categorías y subcategorías basadas en las respuestas obtenidas, las cuales se organizaron en hojas de cálculo para facilitar el análisis y la comparación de datos. Cada respuesta se codificó de acuerdo con las categorías temáticas previamente establecidas, permitiendo una interpretación sistemática de la información.

La revisión de las carpetas fiscales se llevó a cabo mediante un análisis documental detallado, donde se evaluaron los motivos por los cuales los casos de fraude informático fueron archivados. Los datos extraídos de las carpetas se organizaron en una tabla de categorización en Excel, donde se registraron los factores y barreras identificadas durante el proceso de investigación. Esta información se utilizó para detectar patrones y tendencias en la gestión de los casos de fraude informático.

El uso de Excel permitió la creación de gráficos y tablas que ilustraron las principales conclusiones del análisis. Estos resultados descriptivos ayudaron a identificar las áreas clave que contribuyeron a la problemática de la gestión de delitos cibernéticos y a proponer recomendaciones para mejorar la responsabilidad y la prevención en el sistema financiero. El enfoque metodológico empleado garantizó un análisis riguroso y organizado de los datos cualitativos, facilitando la interpretación y la validación de los hallazgos.

En el desarrollo de la investigación, se mantuvieron rigurosos principios de integridad científica y ética, conforme a los estándares establecidos en el Código de Ética de Investigación de la Universidad César Vallejo (UCV). Se adoptaron procedimientos estrictos para garantizar el respeto y la protección de los participantes, así como la confidencialidad de la información recabada. Para asegurar el consentimiento informado de los fiscales entrevistados, se les proporcionó un documento detallado que explicaba el propósito del estudio, el alcance de su participación, y los posibles riesgos y beneficios. Este documento también incluía una declaración de confidencialidad, garantizando que la información proporcionada sería utilizada exclusivamente para fines de investigación y que los datos personales serían anonimizados.

Los fiscales fueron informados sobre su derecho a retirarse del estudio en cualquier momento sin ninguna penalización y sin afectar su relación profesional con la institución. Se obtuvo su consentimiento explícito por escrito antes de realizar las entrevistas, asegurando que comprendieran completamente el proceso de investigación y su rol en él. En cuanto a la revisión de carpetas fiscales, se obtuvo la autorización necesaria de la Segunda Fiscalía Provincial Penal Corporativa del Santa del Ministerio Público para acceder y analizar los documentos. Este permiso se obtuvo a través de una solicitud formal, en la que se especificaron los objetivos de la investigación y la forma en que se manejarían los datos.

Todos los documentos relacionados con la autorización de las instituciones y el consentimiento informado de los participantes se incluyeron en los Anexos del estudio. No obstante, para preservar la confidencialidad de las entidades colaboradoras y de los participantes, estos documentos no se publicarán en el

repositorio de la investigación. Se garantizó que toda la información personal y sensible fuese tratada con la máxima discreción y seguridad, de acuerdo con las normativas vigentes y los principios éticos de la investigación.

II. RESULTADOS

En el proceso de investigación se llevaron a cabo entrevistas con ocho fiscales de la Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Público el 22 de mayo de 2024, y se revisaron carpetas fiscales para obtener información relevante sobre la problemática del fraude informático en Perú. A continuación, se presentan los resultados obtenidos de las entrevistas, organizados de acuerdo con los objetivos de investigación.

Objetivo Específico: *Identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023.*

Tabla 1

Motivos de los archivos por fraude informático

Entrevistados (E)	Pregunta 1: ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?
E- 1	Falta de evidencia concreta.
E- 2	Dificultad para identificar a los responsables debido a falta de tecnología avanzada.
E- 3	Insuficiencia de capacitación y recursos especializados en cibercrimen.
E- 4	Falta de colaboración efectiva con las entidades bancarias.
E- 5	Carencia de procedimientos estandarizados para el seguimiento de casos.
E- 6	Limitaciones en recursos tecnológicos y falta de personal capacitado.
E- 7	Falta de evidencia suficiente y dificultades en la recolección de datos.
E- 8	Inadecuada cooperación interinstitucional y falta de herramientas especializadas.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

Análisis: La Tabla 1 ilustra las respuestas obtenidas de los fiscales muestran una convergencia en varios factores que contribuyen al archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023. Entre estos factores destacan la falta de evidencia concreta y la dificultad para identificar a los responsables, lo que se atribuye en gran medida a la carencia de tecnología avanzada. Además, la insuficiencia de capacitación y recursos especializados en cibercrimen, junto con las limitaciones en la colaboración efectiva entre las fiscalías y las entidades bancarias, agravan la situación. También se menciona la falta de procedimientos estandarizados y la inadecuada cooperación interinstitucional, lo que sugiere una falta de infraestructura y coordinación en el manejo de estos casos. Estos elementos muestran una compleja combinación de factores técnicos, humanos y organizativos que dificultan la persecución efectiva de los delitos cibernéticos.

Interpretación: La identificación de estos factores sugiere que las fiscalías penales en Perú enfrentan serias limitaciones en su capacidad para gestionar casos de fraude informático, lo que resulta en el archivo frecuente de denuncias. La falta de tecnología adecuada y de personal capacitado impide una identificación efectiva de los responsables, mientras que la insuficiente colaboración con las entidades bancarias y la ausencia de procedimientos estandarizados crean brechas significativas en la cadena de investigación y procesamiento. Esto implica que, para mejorar la respuesta ante el fraude informático, es esencial no solo invertir en tecnología y capacitación, sino también fortalecer la colaboración interinstitucional y desarrollar marcos procedimentales claros y uniformes.

Objetivo Específico: *Identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023*

Tabla 2

Principales causas de archivo por delito de Fraude informático

Entrevistados (E)	Pregunta 2: ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?
E- 1	Falta de colaboración con las entidades bancarias.
E- 2	Insuficiencia de recursos tecnológicos adecuados.
E- 3	Falta de procedimientos estandarizados para el seguimiento.
E- 4	Resistencia de las entidades bancarias a compartir información crucial.
E- 5	Carencia de personal capacitado en cibercrimen.
E- 6	Falta de recursos y falta de comunicación efectiva entre las partes.
E- 7	Falta de herramientas para el análisis de datos.
E- 8	Deficiencia en la integración de tecnologías en el proceso investigativo.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

Análisis: La tabla 1 muestra que los fiscales entrevistados identificaron varios factores que contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales de Perú durante 2023. Entre estos factores, la falta de colaboración con las entidades bancarias y la resistencia de estas a compartir información crucial se mencionaron como barreras significativas. Además, se subraya la insuficiencia de recursos tecnológicos y la carencia de personal capacitado en cibercrimen, lo cual limita la capacidad de las fiscalías para realizar un seguimiento efectivo de los casos. También se señaló la falta de procedimientos estandarizados y la deficiencia en la integración de tecnologías en el proceso investigativo, lo que sugiere una falta de coherencia y consistencia en la gestión de estos casos. La falta de herramientas para el análisis de datos y la comunicación ineficaz entre las partes implicadas agravan aún más la situación, contribuyendo a un seguimiento deficiente de las denuncias.

Interpretación: La identificación de estos factores pone de manifiesto las deficiencias estructurales y operativas que enfrentan las fiscalías penales en Perú al tratar casos de fraude informático. La falta de colaboración y la resistencia de las entidades bancarias a compartir información esencial debilitan la capacidad investigativa de las fiscalías, mientras que la insuficiencia de recursos tecnológicos y de personal especializado obstaculizan la realización de un seguimiento adecuado. La ausencia de procedimientos estandarizados y la deficiencia en la integración de tecnologías reflejan una falta de desarrollo y adaptación a las exigencias del cibercrimen moderno. Para mejorar el seguimiento de las denuncias, es crucial abordar estos problemas mediante la mejora de la cooperación interinstitucional, la inversión en tecnología, y la capacitación especializada del personal involucrado en la investigación de fraudes informáticos.

Objetivo Específico: *Identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023.*

Tabla 3

Dificultados al investigar y procesar casos de fraude informático

Entrevistados (E)	Pregunta 7: ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?
E- 1	Falta de herramientas tecnológicas adecuadas.
E- 2	Rápida evolución de las técnicas de los delincuentes y falta de capacitación.
E- 3	Colaboración inadecuada de las instituciones financieras.
E- 4	Dificultades al rastrear delincuentes internacionales.
E- 5	Tecnología obsoleta y sofisticación de los delincuentes.
E- 6	Falta de herramientas adecuadas y rápida evolución del cibercrimen.
E- 7	Insuficiente capacitación y recursos, y complejidad de los delitos.
E- 8	Falta de cooperación internacional y necesidad de tecnología avanzada.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

Análisis: Los fiscales entrevistados señalaron diversas dificultades al investigar y procesar casos de fraude informático, destacando la falta de herramientas tecnológicas adecuadas como una de las principales barreras. La rápida evolución de las técnicas utilizadas por los delincuentes cibernéticos y la falta de capacitación especializada fueron mencionadas repetidamente, subrayando un desajuste entre la capacidad de las fiscalías y la naturaleza dinámica del cibercrimen. Además, la colaboración inadecuada de las instituciones financieras y las dificultades para rastrear delincuentes internacionales fueron identificadas como obstáculos significativos, que complican la persecución efectiva de estos delitos. La mención de tecnología obsoleta y la creciente sofisticación de los delincuentes revelan la existencia de un desfase tecnológico que afecta la capacidad de respuesta de las fiscalías. La falta de cooperación internacional también fue citada como un desafío, especialmente en casos que cruzan fronteras, lo que resalta la necesidad de una mayor coordinación global en la lucha contra el fraude informático.

Interpretación: Los resultados revelan que las fiscalías penales en Perú enfrentan serias dificultades al investigar y procesar casos de fraude informático, principalmente debido a la falta de herramientas tecnológicas adecuadas y la rápida evolución de las tácticas de los delincuentes cibernéticos. La insuficiente capacitación del personal y la tecnología obsoleta limitan la capacidad de las fiscalías para adaptarse a las complejidades del cibercrimen moderno. La colaboración inadecuada con las instituciones financieras y las dificultades en el rastreo de delincuentes internacionales complican aún más la situación, impidiendo una respuesta eficaz. Estos hallazgos sugieren que, para mejorar la eficacia en el tratamiento de casos de fraude informático, es crucial actualizar las tecnologías utilizadas por las fiscalías, mejorar la capacitación continua del personal, y fortalecer tanto la cooperación con las instituciones financieras como la colaboración internacional.

Objetivo Específico: *Evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos*

Tabla 4

Rol y responsabilidad de los bancos

Entrevistados (e)	Pregunta 4: ¿qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?
E- 1	Implementar sistemas de seguridad robustos y capacitar al personal.
E- 2	Deberían tomar un papel más activo en la prevención de fraudes.
E- 3	Alta responsabilidad en mantener sistemas actualizados y prevenir vulneraciones.
E- 4	Deben ser más proactivos en la prevención y gestión de fraudes.
E- 5	Implementar medidas de seguridad avanzadas y mantener una comunicación efectiva.
E- 6	Las entidades bancarias deben cumplir con estándares de seguridad más estrictos.
E- 7	Responsabilidad clave en la protección de datos y en la respuesta a incidentes de fraude.
E- 8	Necesitan reforzar sus políticas de seguridad y educación para prevenir fraudes.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

La Análisis: Las respuestas de los fiscales reflejan un consenso sobre la alta responsabilidad que recae en las entidades bancarias en la prevención y gestión de fraudes informáticos. Se destaca la importancia de implementar sistemas de seguridad robustos y actualizados, así como la necesidad de capacitar al personal para enfrentar las amenazas cibernéticas. Además, varios fiscales señalaron que los bancos deben adoptar un papel más proactivo en la prevención de fraudes, lo que implica no solo la instalación de medidas de seguridad avanzadas, sino también una comunicación efectiva y el cumplimiento de estándares de seguridad estrictos. La protección de datos y la respuesta rápida a incidentes de fraude también fueron identificadas como responsabilidades clave de las entidades bancarias. Asimismo, se mencionó la necesidad de reforzar las políticas de

seguridad y la educación tanto para empleados como para clientes, con el fin de prevenir fraudes de manera más eficaz.

Interpretación: Los resultados indican que las entidades bancarias tienen un rol crucial y una responsabilidad significativa en la prevención y gestión de fraudes informáticos. La implementación de sistemas de seguridad avanzados y la capacitación continua del personal son consideradas medidas esenciales para proteger los fondos y datos de los clientes. La expectativa de que los bancos adopten un enfoque proactivo sugiere que no basta con reaccionar a los incidentes de fraude, sino que es fundamental prevenirlos mediante políticas de seguridad rigurosas y la educación tanto de los empleados como de los usuarios. Esto resalta la necesidad de que las entidades bancarias no solo cumplan con los estándares de seguridad más estrictos, sino que también se conviertan en actores activos en la protección contra fraudes informáticos, lo que a su vez podría contribuir a una mayor confianza de los clientes en el sistema financiero.

Objetivo Específico: *Evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos*

Tabla 5

Colaboración entre fiscalías y entidades bancarias

Entrevistados (e)	Pregunta 3: ¿cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?
E- 1	La colaboración es deficiente; falta de comunicación efectiva.
E- 2	Hay resistencia por parte de los bancos para compartir información.
E- 3	La falta de colaboración limita la efectividad de las investigaciones.
E- 4	La colaboración es crucial pero generalmente no se da de manera efectiva.
E- 5	La cooperación entre las partes es insuficiente.
E- 6	Falta de acuerdos claros entre fiscalías y entidades bancarias.
E- 7	La colaboración no siempre se establece adecuadamente.
E- 8	La falta de integración y comunicación entre las entidades es un problema.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

Análisis: Los fiscales entrevistados señalaron que la colaboración entre las fiscalías y las entidades bancarias es generalmente deficiente, lo que afecta negativamente la resolución de casos de fraude informático. La falta de comunicación efectiva entre ambas partes y la resistencia de los bancos a compartir información crucial son vistas como obstáculos significativos en la investigación de estos delitos. Los entrevistados también destacaron que la falta de colaboración limita la efectividad de las investigaciones, y que, aunque la cooperación es esencial, no siempre se da de manera adecuada. La insuficiencia de acuerdos claros y la falta de integración entre las fiscalías y las entidades bancarias fueron mencionadas como factores que complican aún más la resolución de casos. En general, la falta de colaboración y comunicación efectiva

se identificaron como problemas persistentes que dificultan la persecución efectiva del fraude informático.

Interpretación: Los resultados evidencian que la colaboración entre las fiscalías y las entidades bancarias es un factor crítico en la resolución de casos de fraude informático, pero que actualmente es insuficiente y problemática. La falta de comunicación efectiva y la resistencia de los bancos a compartir información clave son barreras que obstaculizan el avance de las investigaciones y limitan la capacidad de las fiscalías para resolver estos casos de manera eficaz. La ausencia de acuerdos claros y la falta de integración entre ambas partes refuerzan la necesidad de establecer mecanismos de colaboración más sólidos y definidos, que permitan un intercambio de información más fluido y una coordinación efectiva. Mejorar esta colaboración es fundamental para aumentar la eficacia en la gestión y resolución de fraudes informáticos, lo que a su vez podría fortalecer la confianza en las instituciones y en la protección de los derechos de los afectados.

Objetivo Específico: *Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos.*

Tabla 6

Cambios legislativos necesarios

Entrevistados (e)	Pregunta 5: ¿qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?
E- 1	Actualizar las leyes para abordar nuevas formas de cibercrimen.
E- 2	Incorporar tecnologías avanzadas y mejorar la aplicación de la ley.
E- 3	Revisión urgente para incluir cooperación interinstitucional y tecnología avanzada.
E- 4	Fortalecer la ley para mejorar la cooperación internacional y tecnológica.
E- 5	Necesidad de ajustes para enfrentar la evolución del cibercrimen.
E- 6	Incorporar medidas para enfrentar nuevas amenazas y técnicas utilizadas por los ciberdelincuentes.
E- 7	Reformas que incluyan mejor cooperación y herramientas tecnológicas.
E- 8	Enfoque integral con reformas legislativas y mejoras en la tecnología y cooperación.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

Análisis: Los fiscales entrevistados coinciden en la necesidad urgente de reformas legislativas para mejorar la efectividad en la persecución de delitos cibernéticos. Las respuestas reflejan un consenso sobre la importancia de actualizar las leyes existentes para abordar las nuevas formas de cibercrimen que han surgido con el avance tecnológico. Los entrevistados subrayaron la necesidad de incorporar tecnologías avanzadas y de mejorar la cooperación, tanto a nivel nacional como internacional, para enfrentar eficazmente estas amenazas. La revisión de la legislación debería incluir medidas específicas para mejorar la cooperación interinstitucional y fortalecer las capacidades tecnológicas, asegurando que las leyes sean lo suficientemente flexibles y adaptables para seguir el ritmo de la evolución del cibercrimen. La mayoría de los fiscales también mencionaron la

necesidad de un enfoque integral que combine reformas legislativas con mejoras en la tecnología y la cooperación entre entidades.

Interpretación: Los resultados indican que las leyes actuales no son suficientes para enfrentar la creciente complejidad y evolución de los delitos cibernéticos. Existe una necesidad clara de actualizar el marco legal para que refleje las nuevas realidades del cibercrimen, incorporando tecnologías avanzadas y mejorando la cooperación entre las instituciones encargadas de la aplicación de la ley. Las reformas propuestas por los fiscales sugieren un enfoque integral que no solo aborde las deficiencias tecnológicas y de cooperación, sino que también permita una respuesta más ágil y efectiva a las nuevas amenazas cibernéticas. La implementación de estas reformas podría fortalecer la capacidad del sistema judicial para perseguir y resolver delitos cibernéticos de manera más eficiente, contribuyendo a una mayor seguridad y confianza en el sistema de justicia.

Objetivo Específico: *Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos.*

Tabla 7

Evaluación de la ley N°30096

Entrevistados (e)	*Pregunta 6: ¿cómo evalúa la ley de delitos informáticos (ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?*
E- 1	Es un buen inicio, pero no es suficiente para la complejidad actual.
E- 2	Tiene lagunas importantes que limitan su efectividad.
E- 3	Insuficiente; necesita actualización urgente.
E- 4	Requiere revisión para incluir cooperación y tecnología avanzada.
E- 5	Es una base, pero carece de elementos para enfrentar el cibercrimen.
E- 6	La ley se queda corta frente a la evolución del cibercrimen.
E- 7	Necesita abordar tecnología y cooperación internacional.
E- 8	Requiere ajustes para modernizar herramientas y mejorar la coordinación internacional.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

Análisis: Los fiscales entrevistados expresaron una evaluación crítica de la Ley de Delitos Informáticos (Ley Nº 30096), coincidiendo en que, aunque representa un avance importante, es insuficiente para enfrentar la creciente complejidad de los delitos cibernéticos. Las respuestas revelan que la ley actual presenta lagunas significativas que limitan su efectividad, especialmente en un contexto donde el cibercrimen evoluciona rápidamente. Los entrevistados destacaron la necesidad de actualizar la ley para incluir mejoras en la cooperación interinstitucional e internacional, así como la incorporación de tecnologías avanzadas. Además, se indicó que la ley actual, aunque sirve como base, no cuenta con los elementos necesarios para abordar de manera efectiva las amenazas modernas del cibercrimen, lo que sugiere la urgencia de una revisión legislativa que permita una respuesta más adecuada y coordinada frente a estos delitos.

Interpretación: Los resultados sugieren que la Ley Nº 30096, aunque es un paso en la dirección correcta, no cumple completamente con las exigencias actuales para combatir el cibercrimen en su forma moderna y sofisticada. La falta de adecuación de la ley a las nuevas tecnologías y la carencia de mecanismos efectivos para la cooperación internacional e interinstitucional se perciben como debilidades críticas. La necesidad de una actualización urgente es evidente para cerrar las lagunas existentes y mejorar la capacidad de las autoridades para perseguir y resolver delitos cibernéticos. Una revisión de la ley que incorpore estas mejoras podría fortalecer significativamente el marco legal y aumentar la eficacia en la lucha contra el cibercrimen en Perú, adaptándose a las dinámicas cambiantes del entorno digital global.

Objetivo Específico: *Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos.*

Tabla 8

Falta de evidencia en el archivo de casos

Entrevistados (E)	Pregunta 8: ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?
E- 1	La falta de evidencia concreta a menudo lleva al archivo de los casos.
E- 2	Sin evidencia suficiente, es difícil proceder con los casos.
E- 3	La ausencia de pruebas efectivas resulta en el archivo de muchos casos.
E- 4	La falta de evidencia es una barrera importante para la prosecución de casos.
E- 5	Muchos casos se archivan debido a la falta de pruebas concretas.
E- 6	La insuficiencia de evidencia suele ser un motivo principal para el archivo de casos.
E- 7	La falta de pruebas adecuadas dificulta la prosecución efectiva de los casos.
E- 8	Sin evidencia sólida, los casos de fraude suelen ser archivados.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

Análisis: Las respuestas de los fiscales indican que la falta de evidencia concreta es un problema crítico que contribuye significativamente al archivo de casos de fraude informático. Los entrevistados mencionaron repetidamente que, sin evidencia suficiente, es extremadamente difícil proceder con la prosecución de estos casos. La ausencia de pruebas efectivas se identificó como una barrera importante para la prosecución, y muchos casos se archivan debido a la falta de pruebas concretas. La insuficiencia de evidencia no solo dificulta la prosecución efectiva de los casos, sino que también resulta en una alta tasa de archivo de denuncias, lo que refleja una deficiencia en los procesos de recolección y presentación de pruebas en casos de fraude informático.

Interpretación: El impacto de la falta de evidencia en el archivo de casos de fraude informático es significativo y contribuye de manera decisiva a la baja tasa de resolución de estos casos. La ausencia de pruebas concretas limita gravemente la capacidad de las fiscalías para avanzar en la persecución y resolución de los

delitos cibernéticos, resultando en el archivo de muchos casos mediante disposición fiscal de no procedencia de la continuación y formalización de la investigación preparatoria. Esto subraya la necesidad urgente de mejorar los mecanismos de recolección, almacenamiento y análisis de evidencia en casos de fraude informático. Reformas legislativas y mejoras en los procesos judiciales deben centrarse en fortalecer las capacidades para la obtención y presentación de pruebas sólidas, lo que podría ayudar a reducir el número de casos archivados y aumentar la eficacia en la persecución de delitos cibernéticos.

Objetivo Específico: *Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos.*

Tabla 9

Compensación para las victimas

Entrevistados (e)	Pregunta 9: ¿cómo percibe la compensación para las víctimas de fraude informático en Perú?
E- 1	La compensación es a menudo insuficiente y no satisface completamente a las víctimas.
E- 2	Las compensaciones suelen ser parciales y no siempre cubren el daño total.
E- 3	No siempre es adecuada ni suficiente para el perjuicio sufrido.
E- 4	Debe mejorar para cubrir adecuadamente las pérdidas de las víctimas.
E- 5	Las compensaciones suelen ser parciales y no siempre cubren el daño total.
E- 6	No siempre es adecuada ni suficiente para el perjuicio sufrido.
E- 7	Frecuentemente las compensaciones no cubren el impacto total del fraude.
E- 8	Las compensaciones deben ser más integrales y justas para las víctimas.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico

Análisis: Los fiscales coinciden en que la compensación para las víctimas de fraude informático en Perú es insuficiente y no siempre satisface adecuadamente a las personas afectadas. La mayoría de los entrevistados señalaron que las compensaciones ofrecidas suelen ser parciales y no cubren completamente el daño sufrido por las víctimas. Esta falta de suficiencia en las compensaciones indica que el sistema actual no está bien equipado para abordar el impacto total de los fraudes informáticos sobre las víctimas. Las respuestas reflejan una percepción generalizada de que las compensaciones deben mejorar significativamente para proporcionar un alivio adecuado a quienes han sufrido pérdidas debido a delitos cibernéticos.

Interpretación: La percepción de que las compensaciones para las víctimas de fraude informático son inadecuadas destaca una deficiencia importante en el sistema de justicia actual en Perú. La insuficiencia de las compensaciones revela una brecha significativa en la capacidad del sistema para abordar el impacto económico y emocional de los fraudes informáticos. Para aumentar la eficacia en la resolución de estos casos y mejorar la justicia para las víctimas, es esencial implementar reformas legislativas y ajustes en los procesos judiciales que aseguren compensaciones más integrales y justas. Esto no solo ayudaría a mitigar el impacto negativo de los fraudes en las víctimas, sino que también podría aumentar la confianza en el sistema judicial al demostrar un compromiso con la reparación efectiva de los daños causados por los delitos cibernéticos.

Tabla 10

Recomendaciones para mejorar el proceso y procesamiento de delitos

Entrevistados (E)	Pregunta 10: ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?
E- 1	Mejorar la tecnología utilizada y fortalecer la colaboración interinstitucional.
E- 2	Proveer capacitación especializada y recursos adecuados.
E- 3	Invertir en tecnologías avanzadas y promover la cooperación interinstitucional.
E- 4	Implementar un enfoque más coordinado y aumentar la inversión en tecnología y formación.
E- 5	Reforzar la colaboración y modernizar las herramientas investigativas.
E- 6	Proporcionar recursos tecnológicos y capacitación adecuada.
E- 7	Mejorar la cooperación y actualización tecnológica en las investigaciones.
E- 8	Adoptar un enfoque integral con reformas legislativas y mejoras tecnológicas.

Nota: Entrevista realizadas a 8 fiscales el 22 de mayo de 2024, en el Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Publico.

Análisis: Las recomendaciones proporcionadas por los fiscales reflejan un consenso en cuanto a las áreas críticas que necesitan mejora para optimizar el proceso de investigación y procesamiento de delitos cibernéticos en Perú. Las respuestas sugieren que, para enfrentar eficazmente el cibercrimen, es crucial mejorar la tecnología utilizada, fortalecer la colaboración interinstitucional, y proporcionar capacitación especializada y recursos adecuados. Los fiscales destacaron la necesidad de invertir en tecnologías avanzadas y promover un enfoque más coordinado, que incluya tanto una modernización de las herramientas investigativas como un refuerzo en la colaboración entre instituciones. Además, se identificó la importancia de adoptar un enfoque integral que combine reformas legislativas con mejoras en los recursos y capacitación.

Interpretación: Las recomendaciones apuntan a la necesidad de una transformación integral en la forma en que se abordan los delitos cibernéticos en Perú. La mejora en la tecnología y la inversión en recursos avanzados son vistas como elementos clave para fortalecer la capacidad investigativa. Además, la capacitación especializada y el aumento en la cooperación entre instituciones son esenciales para enfrentar el cibercrimen de manera efectiva. La adopción de un enfoque coordinado y la implementación de reformas legislativas que se alineen con los avances tecnológicos son pasos cruciales para mejorar el proceso de investigación y procesamiento. Estas acciones no solo mejorarían la capacidad de respuesta ante los delitos cibernéticos, sino que también contribuirían a una mayor eficacia en la persecución y resolución de estos casos, asegurando un sistema más robusto y eficiente en el combate contra el cibercrimen.

Tabla 11

Matriz de sistematización de resultados

OBJETIVO ESPECÍFICO	PREGUNTAS DE LA ENTREVISTA	RESPUESTA/RESULTADO	ANÁLISIS/COMENTARIO
a) identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023	1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?	Respuesta: Falta de evidencia suficiente, problemas en la obtención de pruebas digitales, falta de capacitación en técnicas forenses digitales, y deficiencias en la colaboración con las entidades bancarias.	La falta de evidencia y problemas en la obtención de pruebas son causas recurrentes. La falta de capacitación y deficiencias en la colaboración también contribuyen significativamente al archivo de casos.
a) identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023	2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?	Respuesta: Insuficiente personal capacitado, carencia de recursos tecnológicos adecuados, y falta de coordinación entre diferentes instituciones.	La falta de personal capacitado y recursos tecnológicos adecuados afectan negativamente el seguimiento de los casos, mientras que la falta de coordinación interinstitucional

			también es un factor importante.
b) evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos	4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?	Respuesta: Las entidades bancarias deben implementar políticas de prevención más estrictas, mejorar sus sistemas de seguridad, y proporcionar formación continua a sus empleados.	Las entidades bancarias juegan un rol crucial en la prevención y gestión de fraudes, pero actualmente su responsabilidad no se cumple de manera óptima. Se necesitan mejoras en las políticas de prevención y en la seguridad.
b) evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos	3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?	Respuesta: La colaboración es a menudo insuficiente, lo que dificulta la obtención de información crucial para resolver los casos.	La falta de colaboración efectiva entre fiscalías y entidades bancarias limita la capacidad de resolución de los casos de fraude, afectando negativamente el proceso investigativo.
c) valorar la pertinencia de implementar nuevas reformas	5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en	Respuesta: Se requiere una actualización del marco legal, inclusión de nuevas	Las reformas legislativas deben abordar la evolución del cibercrimen y mejorar la

legislativas sobre delitos cibernéticos	la persecución de delitos cibernéticos?	tecnologías en la legislación, y establecimiento de mecanismos más eficientes de cooperación entre instituciones.	cooperación institucional para aumentar la eficacia en la persecución de delitos.
c) valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos	6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?	Respuesta: La Ley Nº 30096 es un paso positivo, pero resulta insuficiente para enfrentar la rápida evolución y complejidad de los delitos cibernéticos.	La ley existente no está adaptada a las nuevas formas de cibercrimen, lo que requiere reformas para mejorar su eficacia en la persecución de delitos.
c) valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos	10. ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?	Respuesta: Se recomienda fortalecer la capacitación de personal, mejorar los recursos tecnológicos, y establecer protocolos claros de cooperación entre fiscalías y entidades bancarias.	Las recomendaciones destacan la necesidad de mejorar la capacitación, recursos y coordinación para optimizar la investigación y el procesamiento de delitos cibernéticos.
a) identificar las causas principales del archivo de denuncias por	7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?	Respuesta: Dificultades para acceder a pruebas digitales, limitaciones en las	Las dificultades incluyen problemas para acceder a pruebas y limitaciones en las

fraude informático en las fiscalías penales de Perú durante 2023		herramientas forenses, y obstáculos legales en la cooperación internacional.	herramientas tecnológicas, así como obstáculos en la cooperación internacional, que afectan el procesamiento de casos.
a) identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023	8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?	Respuesta: La falta de evidencia sólida lleva al archivo de casos debido a la imposibilidad de probar los delitos en los tribunales.	La falta de evidencia es una causa principal del archivo de casos, ya que impide la prosecución efectiva en los tribunales.
b) evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos	9. ¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?	Respuesta: La compensación para las víctimas es limitada y, a menudo, insatisfactoria, lo que puede desalentar a las víctimas a presentar denuncias.	La percepción de la compensación limitada puede desincentivar a las víctimas a buscar justicia, afectando la denuncia y resolución de casos de fraude.

Nota: Entrevistas realizadas a 8 fiscales el 22 de mayo de 2024, en la Segunda fiscalía provincial Penal Corporativa del Santa del Ministerio Público.

Comentario: En el marco de la investigación sobre los delitos cibernéticos en Perú, se ha desarrollado una matriz de sistematización de resultados con el propósito de organizar y analizar de manera estructurada la información obtenida de las entrevistas realizadas a fiscales. Esta matriz se ha diseñado para abordar los objetivos específicos de la investigación, proporcionando una visión clara de los resultados y facilitando la identificación de patrones y temas recurrentes.

La inclusión de esta matriz responde a la necesidad de clasificar y comprender las respuestas de los entrevistados en relación con los motivos del archivo de denuncias por fraude informático, la responsabilidad de las entidades bancarias en la gestión de fraudes, y la pertinencia de nuevas reformas legislativas. Al organizar las respuestas y análisis en esta tabla, se pretende ofrecer una herramienta que permita evaluar de forma exhaustiva las causas subyacentes y las recomendaciones para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú.

Tabla 12

Caso 01

Datos del caso	Caso Fiscal: 01 Fecha de la Disposición: 28 de agosto de 2023 Agraviado: 1 Imputado: LQRR Delito Atribuido: Fraude Informático - Ley de Delitos Informáticos N° 30096 Capítulo V – Delitos Informáticos contra el Patrimonio, Artículo 8°, modificado por el Artículo 1° de la Ley N° 30171. Hecho: Retiro no autorizado y compra con tarjeta de débito retenida por el cajero del Banco de la Nación en Chimbote. Monto sustraído: S/. 6,697.00 soles
Resumen	El agraviado 1 denunció la retención de su tarjeta de débito en un cajero del Banco de la Nación y subsecuentes retiros y compras no autorizadas por un total de S/. 6,697.00 soles el 28 de julio de 2023. Tras bloquear su tarjeta, descubrió los retiros no autorizados cuando solicitó un duplicado de la tarjeta y revisó su estado de cuenta.
Análisis	Elementos de Convicción: Denuncia Verbal: Hecha el 1 de agosto de 2023. Declaración de la Agraviada: Detallando las circunstancias del hecho delictivo. Estados de Cuenta: Muestran transacciones no autorizadas. Constancia de Bloqueo: Indica el bloqueo de la tarjeta el 28 de julio de 2023. Fundamentos: El Ministerio Público evaluó la relevancia jurídica de los hechos denunciados y la suficiencia de los indicios delictivos. Se requiere sospecha razonable para formalizar la investigación preparatoria. El principio de "última ratio" del Derecho Penal sugiere usarlo solo cuando otros medios no penales no pueden resolver el conflicto.

	Materialidad del Delito: El acto podría tipificarse como Fraude Informático, pero se considera que puede resolverse por vías ajenas a lo penal, como Indecopi o la Defensoría del Consumidor Financiero. Insuficiencia de Elementos de Convicción: No hay suficiente información para identificar al presunto autor. La falta de individualización del imputado impide formalizar la investigación.
Conclusión	El Ministerio Público decidió no formalizar la investigación preparatoria por la presunta comisión del delito de Fraude Informático debido a la falta de elementos de convicción suficientes para identificar al responsable y porque el conflicto puede resolverse mediante procedimientos alternos más idóneos. La disposición se archiva, con la salvedad de que puede reabrirse si se aportan nuevos elementos de convicción.

Nota: *Creación propia*

Análisis: El análisis del Caso 01 revela que, a pesar de que el hecho de fraude informático está claramente establecido por la denuncia de la víctima, el Ministerio Público decidió no formalizar la investigación preparatoria. Este caso implicaba la sustracción no autorizada de dinero mediante una tarjeta de débito, con un monto significativo de S/. 6,697.00 soles. La denuncia incluyó una declaración detallada de la agraviada, estados de cuenta que confirmaban las transacciones no autorizadas, y una constancia de bloqueo de la tarjeta. Sin embargo, el Ministerio Público encontró que, aunque el acto podía tipificarse como fraude informático, la falta de identificación del imputado y la insuficiencia de elementos de convicción dificultaban la formalización de la investigación. Además, se evaluó que el conflicto podría ser resuelto por vías alternativas como Indecopi o la Defensoría del Consumidor Financiero, lo cual se alinea con el principio de "última ratio" del Derecho Penal, que sugiere utilizar el proceso penal solo cuando otros medios no sean efectivos.

Interpretación: La decisión del Ministerio Público de no formalizar la investigación refleja un enfoque pragmático en la gestión de casos de fraude informático. La falta de identificación del imputado y de elementos de convicción sólidos impide avanzar con el proceso penal, lo que destaca una de las limitaciones actuales en la persecución de delitos cibernéticos: la dificultad para recopilar pruebas concretas y rastrear a los responsables en un contexto tecnológico complejo. Además, la consideración de vías alternativas para resolver el conflicto subraya la necesidad de mecanismos de resolución de disputas más accesibles y eficientes para casos que pueden no cumplir con los requisitos penales estrictos. La decisión de archivar el caso, con la posibilidad de reabrirlo si surgen nuevos elementos, refleja una estrategia que busca equilibrar la aplicación del derecho penal con la eficacia en la resolución de conflictos, sugiriendo una revisión continua de las prácticas y procedimientos en el ámbito de los delitos cibernéticos.

Tabla 13

Caso 02

Datos del caso	Caso Fiscal: 02
	Fecha de la Disposición: 10 de julio de 2023 Agraviado: 02 Imputado: 02 Delito: Fraude Informático Hecho: Transferencia no autorizada desde la cuenta bancaria del agraviado. Monto sustraído: S/. 1,980.00
Resumen	El agraviado 02, recibió un mensaje de texto en su teléfono móvil el 11 de abril de 2020, supuestamente del Banco Continental - BBVA, solicitando la actualización de sus datos mediante un enlace. Al ingresar sus datos en el enlace, no pudo acceder posteriormente a su aplicación bancaria debido a un supuesto mantenimiento. El 14 de abril de 2020, al contactar al banco, se enteró de una transferencia no autorizada de S/.1,980.00 realizada el 11 de abril a otro número de teléfono. La tarjeta del

agraviado fue bloqueada por seguridad, y denunció el hecho ante la policía.

Análisis

Hechos Investigados:

El agraviado 02 recibió un mensaje fraudulento solicitando la actualización de sus datos bancarios.

Al ingresar los datos en el enlace proporcionado, no pudo acceder a su cuenta bancaria.

Posteriormente, se enteró de una transferencia no autorizada de S/.1,980.00 desde su cuenta.

Función del Ministerio Público:

Evaluar si los hechos tienen trascendencia jurídica para proceder con la investigación.

Reunir pruebas suficientes para formalizar la acción penal o archivarla si no se encuentra evidencia suficiente.

Diligencias Preliminares:

La investigación preliminar no logró reunir pruebas suficientes para proceder con la formalización de la investigación preparatoria.

Tipo Penal y Pena:

Delito de Fraude Informático, tipificado en el artículo 8° de la Ley 30096, con una pena de 3 a 8 años de prisión y 60 a 120 días-multa.

Análisis Fáctico y Jurídico:

No se encontraron pruebas suficientes que demuestren la responsabilidad de la imputada 2 en el delito de fraude informático.

La víctima voluntariamente proporcionó sus datos bancarios, lo que implica una autopuesta en peligro.

Elementos de Convicción:

La denuncia verbal, la consulta de movimientos bancarios y la declaración del agraviado no fueron suficientes para vincular a la imputada con el delito.

No se logró identificar al titular o beneficiario del número de teléfono al que se transfirió el dinero.

Conclusión	Debido a la falta de pruebas suficientes para demostrar la responsabilidad de la denunciada 02 en el delito de fraude informático y considerando que el agraviado voluntariamente proporcionó sus datos bancarios, se decidió no formalizar ni continuar con la investigación preparatoria. Se dispuso el archivo del caso, dado que no existen indicios reveladores de la existencia del delito ni elementos que justifiquen una persecución penal formal.

Nota: *Creación propia*

Análisis: El análisis del Caso 02 revela que el agraviado fue víctima de un fraude informático tras recibir un mensaje de texto fraudulento que solicitaba la actualización de sus datos bancarios. Aunque el agraviado bloqueó su tarjeta y denunció la transferencia no autorizada, la investigación preliminar no pudo reunir suficientes pruebas para relacionar a los imputados con el delito. La falta de elementos de convicción, como la identificación del beneficiario de la transferencia y pruebas directas sobre la responsabilidad de la imputada, dificultó la formalización de la investigación. Además, la autopuesta en peligro por parte del agraviado, al proporcionar sus datos a un enlace fraudulento, complicó aún más la persecución penal.

Interpretación: La interpretación de estos resultados subraya las limitaciones en la capacidad del sistema judicial para manejar casos de fraude informático debido a la falta de pruebas concretas y la complejidad en el rastreo de actividades fraudulentas en línea. La decisión de archivar el caso refleja una brecha significativa en la capacidad de la ley para abordar eficazmente los delitos cibernéticos. Esto indica una necesidad urgente de mejorar las estrategias de recolección de pruebas, fortalecer la educación preventiva y actualizar los mecanismos legales y tecnológicos para enfrentar los desafíos del fraude informático de manera más eficaz. La dificultad para probar la responsabilidad directa de los imputados y la falta de evidencia sólida muestran cómo la naturaleza del fraude informático puede obstaculizar la justicia y resaltar la importancia de reformas y adaptaciones en el sistema judicial.

Tabla 14

Caso 03

Datos del caso	Caso Fiscal: 03 Fecha de la disposición: 11 de abril de 2023 Delito: Fraude Informático Imputado: L.Q.R.R. Agraviado: 03 Hecho: Uso no autorizado de tarjeta de crédito para realizar una apuesta. Monto Sustraído: S/1,000.00 soles
Resumen	El agraviado 03, recibió un mensaje de texto del número 52244 el 29 de marzo de 2023, informando que se había realizado un consumo de S/1,000.00 soles en Apuesta Total con su tarjeta de crédito terminada en 6284. Posteriormente, llamó al Banco Falabella para bloquear su tarjeta y se acercó al banco el 30 de marzo de 2023 para realizar el reclamo correspondiente.
Análisis	Hechos Investigados: El agraviado 03 recibió un mensaje de texto el 29 de marzo de 2023 informando sobre un consumo no autorizado de S/1,000.00 soles con su tarjeta de crédito. Llamó al Banco Falabella para bloquear su tarjeta y presentó un reclamo el 30 de marzo de 2023. Función del Ministerio Público: Evaluar si los hechos tienen trascendencia jurídica para proceder con la investigación. Reunir pruebas suficientes para formalizar la acción penal o archivarla si no se encuentra evidencia suficiente. Diligencias Preliminares: La investigación preliminar no logró reunir pruebas suficientes para proceder con la formalización de la investigación preparatoria. Tipo Penal y Pena:

	Delito de Fraude Informático, tipificado en el artículo 8° de la Ley 30096, con una pena de 3 a 8 años de prisión y 60 a 120 días-multa. Análisis Fáctico y Jurídico: No se encontraron pruebas suficientes que demuestren la responsabilidad del imputado L.Q.R.R. en el delito de fraude informático. Las tarjetas de crédito requieren una clave personal para realizar transacciones, y se asume que el titular debe proteger dicha clave. Elementos de Convicción: Denuncia verbal y declaración en sede policial de la agraviada 03, no fueron suficientes para identificar al presunto autor del delito.
Conclusión	Debido a la falta de pruebas suficientes para demostrar la responsabilidad del imputado L.Q.R.R. en el delito de fraude informático y considerando que las tarjetas de crédito requieren una clave personal para realizar transacciones, se decidió no formalizar ni continuar con la investigación preparatoria. Se dispuso el archivo del caso, dado que no existen indicios reveladores de la existencia del delito ni elementos que justifiquen una persecución penal formal.

Nota: *Creación propia*

Análisis: El análisis del Caso 03 muestra que el agraviado 03 reportó un uso no autorizado de su tarjeta de crédito para una apuesta por S/1,000.00 soles tras recibir una notificación el 29 de marzo de 2023. A pesar de la rápida reacción del agraviado al bloquear su tarjeta y presentar un reclamo, la investigación preliminar no logró reunir pruebas suficientes para vincular al imputado L.Q.R.R. con el delito. La principal dificultad radica en la falta de evidencia concreta sobre cómo el imputado obtuvo y utilizó la tarjeta de crédito, dado que estas requieren una clave personal para completar las transacciones. La ausencia de pruebas directas y la falta de identificación del autor complicaron la formalización de la investigación.

Interpretación: La interpretación de estos resultados revela una debilidad significativa en el proceso investigativo para casos de fraude informático, especialmente en relación con el uso no autorizado de tarjetas de crédito. La falta de evidencia directa y la dificultad para rastrear el uso indebido de una tarjeta, que requiere una clave

personal para transacciones, indican que las investigaciones sobre delitos cibernéticos enfrentan grandes desafíos en términos de recolección de pruebas y atribución de responsabilidad. Esto pone de manifiesto la necesidad de mejorar las técnicas de investigación y fortalecer los mecanismos legales para abordar eficazmente los delitos informáticos, así como la importancia de adoptar medidas de prevención y protección más robustas para los titulares de tarjetas.

Tabla 15

Caso 04

Datos del caso	Caso Fiscal: 04 Delito: Fraude Informático Imputado: Los que resulten responsables Agraviado: 04 Fecha de la Disposición: 25 de agosto de 2023 Hecho: Uso no autorizado de tarjeta de débito extraviada para realizar compras. Monto Sustraído: $148 dólares americanos
Resumen	El agraviado 04, perdió su tarjeta de débito del banco Scotiabank el 27 de julio de 2023. Posteriormente, se realizaron ocho transacciones no autorizadas el 31 de julio de 2023, por un total de $148 dólares americanos.
Análisis	Hechos Investigados: La agraviada 04 perdió su tarjeta de débito el 27 de julio de 2023. Se realizaron ocho transacciones no autorizadas el 31 de julio de 2023, por un total de $148 dólares americanos. Función del Ministerio Público: Evaluar si los hechos tienen trascendencia jurídica para proceder con la investigación. Reunir pruebas suficientes para formalizar la acción penal o archivarla si no se encuentra evidencia suficiente. Diligencias Preliminares:

	La investigación preliminar no logró reunir pruebas suficientes para proceder con la formalización de la investigación preparatoria. Tipo Penal y Pena: Delito de Fraude Informático, tipificado en el artículo 8° de la Ley 30096, con una pena de 3 a 8 años de prisión y 60 a 120 días-multa. Análisis Fáctico y Jurídico: No se encontraron pruebas suficientes que demuestren la responsabilidad de un individuo específico en el delito de fraude informático. Las circunstancias del caso sugieren que el agraviado pudo haber evitado el fraude reportando la pérdida de la tarjeta a tiempo. Elementos de Convicción: Denuncia verbal y declaración en sede policial de la agraviada 04a no fueron suficientes para identificar al presunto autor del delito. No se logró individualizar a los responsables de las transacciones no autorizadas.
Conclusión	Debido a la falta de pruebas suficientes para demostrar la responsabilidad de algún individuo específico en el delito de fraude informático y considerando que el agraviado no reportó la pérdida de su tarjeta de manera oportuna, se decidió no formalizar ni continuar con la investigación preparatoria. Se dispuso el archivo del caso, dado que no existen indicios reveladores de la existencia del delito ni elementos que justifiquen una persecución penal formal. Además, el caso puede ser tratado por vías alternativas como Indecopi o la Defensoría del Consumidor Financiero.

Nota: *Creación propia*

Análisis: El análisis del Caso 04 revela que la agraviada 04 perdió su tarjeta de débito el 27 de julio de 2023 y, a partir de esa fecha, se realizaron ocho transacciones no autorizadas el 31 de julio de 2023, totalizando $148 dólares americanos. La investigación preliminar no encontró pruebas suficientes para vincular a un individuo

específico con las transacciones fraudulentas. La falta de una denuncia oportuna por la pérdida de la tarjeta complicó la recolección de pruebas y la identificación de los responsables. La denuncia verbal y la declaración policial no aportaron datos concretos para seguir con la investigación.

Interpretación: La interpretación de estos resultados sugiere que la demora en la denuncia de la pérdida de la tarjeta contribuyó a la falta de evidencia en el caso. Este retraso en la notificación redujo las posibilidades de rastrear e identificar al autor de las transacciones no autorizadas. Además, el caso subraya una deficiencia en la capacidad del sistema para manejar estos fraudes cuando no se reportan rápidamente. La falta de pruebas y la imposibilidad de identificar a un responsable específico llevaron a archivar el caso, reflejando una necesidad urgente de fortalecer los procesos de denuncia y protección para prevenir y gestionar eficazmente el fraude informático. La posibilidad de resolver el conflicto a través de vías alternativas como Indecopi o la Defensoría del Consumidor Financiero también destaca la importancia de tener mecanismos adicionales para abordar tales problemas fuera del ámbito penal.

Tabla de Resultados de Casos y Relación con Objetivos

Tabla 16

Resultado de Casos General

Categoría	***Caso 1***	***Caso 2***	***Caso 3***	***Caso 4***
Fecha de Disposición	28 de agosto de 2023	10 de julio de 2023	11 de abril de 2023	25 de agosto de 2023
Agraviado	01	02	03	04
Imputado	LQRR	02	L.Q.R.R.	Los que resulten responsables
Monto Sustraído	S/. 6,697.00	S/. 1,980.00	S/1,000.00	$148 dólares americanos
Hecho	Retiro no autorizado y compra con tarjeta de débito	Transferencia no autorizada desde cuenta bancaria	Uso no autorizado de tarjeta de crédito para apuesta	Uso no autorizado de tarjeta de débito extraviada
Conclusión	Archivo por falta de elementos de convicción y solución alterna	Archivo por falta de pruebas y autopuesta en peligro	Archivo por falta de pruebas y posible negligencia en la protección de la tarjeta	Archivo por falta de pruebas y reporte tardío de pérdida

Nota: *Creación propia*

En primer lugar, el objetivo de determinar los factores que contribuyen a que las fiscalías penales en Perú archiven las denuncias por fraude informático se relaciona con varias categorías emergentes. Una categoría clave es la insuficiencia de elementos de convicción, identificada en todos los casos, lo que implica la falta de pruebas suficientes para identificar al responsable del delito. Otra categoría es la opción de resolver el conflicto por vías no penales, como Indecopi o la Defensoría del Consumidor. Además, la autopuesta en peligro del agraviado, como en el Caso 2, donde la víctima proporcionó voluntariamente sus datos, también contribuye al

archivo de la denuncia. Los casos relevantes incluyen el Caso 1, donde no se identificó al responsable y se sugirió resolver el caso por medios alternos; el Caso 2, donde la falta de identificación del imputado y la autopuesta en peligro llevaron al archivo; el Caso 3, marcado por la falta de pruebas suficientes y posible negligencia en la protección de la tarjeta; y el Caso 4, caracterizado por un reporte tardío de la pérdida y la falta de pruebas identificativas. El segundo objetivo, evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos, se asocia con la categoría de protección y reacción de las entidades bancarias. En los casos analizados, se evidencia la importancia de la rapidez en la notificación y bloqueo de tarjetas por parte de las entidades bancarias. La falta de medidas inmediatas para evitar el uso no autorizado también contribuye al archivo de los casos. En el Caso 1, la retención de la tarjeta y la revisión del estado de cuenta fueron cruciales para la denuncia. En el Caso 2, la falta de acceso a la cuenta debido a un enlace fraudulento indica una deficiencia en la protección ofrecida por el banco. En el Caso 3, aunque la víctima contactó al banco para bloquear la tarjeta, la protección preventiva es clave. En el Caso 4, la pérdida de la tarjeta y la tardía notificación al banco indican una brecha en la gestión de seguridad. El tercer objetivo, valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos, se vincula con la necesidad de reformas en el procedimiento y la mejora en la recopilación de evidencias. Los casos destacan la falta de un marco efectivo para abordar y probar los fraudes informáticos, lo que sugiere una necesidad de reformas para mejorar la eficacia de la persecución penal. También se requiere un fortalecimiento en la forma en que se recopilan y validan las pruebas relacionadas con el fraude informático. El Caso 1 indica la necesidad de procedimientos más claros debido a la falta de pruebas para identificar al imputado y la posibilidad de resolución alterna. En el Caso 2, la falta de pruebas y la responsabilidad del agraviado sugieren que se deben mejorar las medidas preventivas y las reformas en la legislación para abordar la autopuesta en peligro. El Caso 3 resalta la necesidad de protocolos más rigurosos debido a la falta de pruebas y la posible negligencia en la protección de tarjetas. El Caso 4, con su tardía notificación de la pérdida de la tarjeta y la falta de individualización de los responsables, indica que se necesitan procesos más eficientes y reformas legislativas para mejorar la persecución de delitos cibernéticos.

Tabla 17

Cuadro de Resultados y relación con los Objetivos

Caso	Resumen del Caso	Conclusión	Relación con los Objetivos
Caso 1	Retiro no autorizado y compra con tarjeta de débito retenida por el cajero. Monto sustraído: S/. 6,697.00.	Archivo por falta de elementos de convicción y solución alterna.	Objetivo a) Insuficiencia de elementos de convicción y la posibilidad de resolver mediante medios alternos contribuyen al archivo. Objetivo b) Relevancia de la rapidez en la notificación y bloqueo de la tarjeta por el banco. Objetivo c) Necesidad de mejorar el marco para la identificación y resolución de casos.
Caso 2	Transferencia no autorizada tras ingresar datos en un enlace fraudulento. Monto sustraído: S/. 1,980.00.	Archivo por falta de pruebas y autopuesta en peligro.	Objetivo a) La autopuesta en peligro y la falta de identificación del imputado afectan el archivo del caso. Objetivo b) Deficiencia en la protección de datos por el banco Objetivo c) Necesidad de medidas preventivas más robustas y reformas para abordar la autopuesta en peligro.
Caso 3	Uso no autorizado de tarjeta de crédito para una apuesta. Monto sustraído: S/1,000.00.	Archivo por falta de pruebas y posible negligencia en la protección de la tarjeta.	Objetivo a) Falta de pruebas suficientes y posible negligencia en la protección de la tarjeta contribuyen al archivo. Objetivo b) Importancia de medidas preventivas y gestión de seguridad por parte del banco. Objetivo c) Recomendación para protocolos más rigurosos en la protección de tarjetas y recopilación de pruebas.
Caso 4	Uso no autorizado de tarjeta de débito extraviada. Monto sustraído: $148 dólares americanos.	Archivo por falta de pruebas y reporte tardío de pérdida.	Objetivo a) Falta de pruebas identificativas y reporte tardío de la pérdida de la tarjeta llevan al archivo. Objetivo b) Necesidad de notificación oportuna y gestión efectiva por parte del banco. Objetivo c) Necesidad de reformas para mejorar la respuesta y procedimientos en casos de pérdida de tarjetas.

Fuente: Creación propia

Comentario:

Objetivo a: En todos los casos, la insuficiencia de elementos de convicción y el uso de vías alternas para la resolución de conflictos contribuyen al archivo de las denuncias. La falta de pruebas y la dificultad para identificar a los responsables son factores recurrentes.

Objetivo b: La protección y gestión por parte de las entidades bancarias juegan un papel crucial en la prevención y resolución de fraudes. En varios casos, la deficiencia en la protección de datos y la falta de medidas preventivas son evidentes.

Objetivo c: Los casos analizados sugieren la necesidad de reformas legislativas y mejoras en los procedimientos judiciales. La falta de protocolos efectivos para la identificación de fraudes y la recopilación de pruebas, así como la necesidad de una respuesta más eficiente en la gestión de fraudes, son aspectos destacados.

III. DISCUSIÓN

Discusión del Primer Resultado: Causas del Archivo de Denuncias

El análisis de las causas principales del archivo de denuncias por fraude informático en las fiscalías penales, en relación con el objetivo específico de identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023, mostró que la falta de un marco legal actualizado y la falta de recursos y capacitación en las fiscalías son factores críticos. Este hallazgo coincide con la Teoría de Tipicidad en Cibercrimen de Posada (2010), que señala que la rápida evolución y complejidad técnica de los delitos cibernéticos a menudo generan vacíos legales, complicando la tipificación y sanción de estos delitos. Además, el antecedente de Morales (2016) resalta las deficiencias en la legislación peruana frente a los delitos informáticos, lo que refuerza la conexión con la teoría al evidenciar cómo la falta de un marco legal adecuado contribuye al archivo de las denuncias. La metodología cualitativa utilizada permite un análisis profundo de estas deficiencias, pero futuros estudios podrían beneficiarse de un enfoque cuantitativo para medir de manera más precisa el impacto de estas lagunas legales en el archivo de las denuncias.

Discusión del Segundo Resultado: Rol y Responsabilidad de las Entidades Bancarias

El análisis del rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos, en relación con el objetivo específico de evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos, reveló que la falta de medidas de seguridad adecuadas y de educación para los clientes son deficiencias clave. Este resultado está en línea con la Teoría de las Obligaciones de Resultado de Perez (2018), que sostiene que las entidades bancarias tienen una responsabilidad casi objetiva para proteger los fondos y datos de sus clientes. El antecedente de Quiroz (2019), que examina la dependencia tecnológica en la banca y su impacto en la criminalidad, también respalda esta perspectiva, destacando la necesidad de una mayor responsabilidad de las

instituciones financieras en la prevención de delitos informáticos. La investigación cualitativa proporciona una visión detallada de estas deficiencias, pero un enfoque cuantitativo podría ofrecer una evaluación más exhaustiva de las medidas de seguridad implementadas por los bancos.

Discusión del Tercer Resultado: Reformas Legislativas y Mejora en Procesos Judiciales

El análisis de las propuestas de reformas legislativas y mejoras en los procesos judiciales para aumentar la eficacia en la persecución y resolución de delitos cibernéticos, en relación con el objetivo específico de Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos, evidenció la necesidad de actualizar las leyes y procedimientos para enfrentar adecuadamente los delitos cibernéticos. Este hallazgo coincide con la Teoría de Tipicidad en Cibercrimen de Posada (2010), que destaca la importancia de adaptar las leyes para abordar los vacíos legales que dificultan la persecución de estos delitos. El antecedente de Nuñez (2022), que discute la necesidad de adaptarse a la evolución de la ciberdelincuencia, apoya esta perspectiva al subrayar la urgencia de reformas legislativas. La metodología cualitativa proporciona una comprensión detallada de las deficiencias actuales, pero integrar un enfoque cuantitativo podría ofrecer una visión más clara sobre la efectividad de las reformas propuestas y su impacto en la eficacia del sistema judicial.

Discusión del Cuarto Resultado: Factores que Contribuyen a la Impunidad en Fraude Informático

El análisis de los factores que contribuyen a la impunidad en los casos de fraude informático, en relación con el objetivo específico de identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023, mostró que la insuficiencia en la evidencia digital y la falta de capacidad técnica en las fiscalías son factores clave. Estos hallazgos están en consonancia con la Teoría de Tipicidad en Cibercrimen de Posada (2010), que enfatiza cómo la falta de un marco legal adaptado a la complejidad técnica de los delitos cibernéticos puede contribuir

a la impunidad. El antecedente de Riofrío (2012), que destaca la falta de disposiciones penales específicas en Ecuador, refuerza esta conexión, subrayando la necesidad de capacitación y recursos adecuados para enfrentar la ciberdelincuencia. La metodología cualitativa permitió un análisis detallado de estos factores, pero un enfoque cuantitativo podría proporcionar una visión más amplia sobre cómo la insuficiencia en la evidencia y la capacidad técnica afectan la persecución de estos delitos.

Discusión del Quinto Resultado: Eficiencia en la Gestión de Fraudes Informáticos por parte de los Bancos

El análisis de la eficiencia en la gestión de fraudes informáticos por parte de los bancos, en relación con el objetivo específico de evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos, reveló que la falta de protocolos estandarizados y la inadecuada respuesta a incidentes son deficiencias importantes. Este resultado está alineado con la Teoría de las Obligaciones de Resultado de Perez (2018), que sostiene que las entidades bancarias deben implementar medidas de seguridad proactivas y eficaces. El antecedente de Quiroz (2019), que examina cómo la dependencia tecnológica impacta en la criminalidad y la necesidad de mejorar la investigación de delitos informáticos, también apoya esta perspectiva, destacando la importancia de protocolos robustos. La investigación cualitativa ofreció una visión profunda de estas deficiencias, pero la aplicación de un enfoque cuantitativo podría proporcionar una evaluación más completa de la eficacia de las medidas de seguridad y gestión en los bancos.

Discusión del Sexto Resultado: Impacto de Reformas Legislativas en la Eficacia del Sistema Judicial

El análisis del impacto de las reformas legislativas propuestas en la eficacia del sistema judicial para la persecución de delitos cibernéticos, en relación con el objetivo específico de Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos, evidenció que la implementación de reformas podría mejorar la capacidad del sistema judicial

para manejar estos casos. Este hallazgo está en sintonía con la Teoría de Tipicidad en Cibercrimen de Posada (2010), que destaca la necesidad de actualizar las leyes para abordar los vacíos que afectan la persecución de delitos cibernéticos. El antecedente de Nuñez (2022), que resalta la necesidad de adaptación a la evolución de la ciberdelincuencia, apoya la necesidad de reformas para mejorar la eficacia judicial. La metodología cualitativa proporcionó una comprensión detallada de cómo las reformas podrían influir en la eficacia del sistema judicial, pero un enfoque cuantitativo podría ofrecer una evaluación más precisa del impacto real de estas reformas en la práctica.

Discusión del Séptimo Resultado: Recomendaciones para la Prevención de Fraudes Informáticos

El análisis de las recomendaciones para la prevención de fraudes informáticos, en relación con el objetivo específico de Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos, mostró que las reformas legislativas y la implementación de tecnologías avanzadas son cruciales. Este hallazgo está en concordancia con la Teoría de la Tipicidad en Cibercrimen de Posada (2010), que aboga por una actualización continua del marco legal para enfrentar la evolución de los delitos cibernéticos. El antecedente de Morales (2016), que critica las deficiencias en la legislación peruana frente a delitos informáticos, respalda la necesidad de reformas que se adapten a la complejidad de los crímenes digitales. La metodología cualitativa permitió explorar detalladamente las recomendaciones, pero un análisis cuantitativo podría ofrecer una visión más clara de la eficacia potencial de estas reformas en la práctica.

Discusión del Octavo Resultado: Educación y Concienciación sobre Seguridad en Línea

El análisis sobre la educación y concienciación en seguridad en línea, en relación con el objetivo específico de evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos, reveló que una mayor inversión en programas educativos para clientes puede reducir significativamente los incidentes de fraude. Este resultado coincide con

la Teoría de las Obligaciones de Resultado de Perez (2018), que enfatiza la responsabilidad de las entidades bancarias en educar a sus clientes para proteger sus datos y fondos. El antecedente de Quiroz (2019), que aborda la necesidad de mejorar la investigación y la educación sobre delitos informáticos, también apoya la idea de que una mayor concienciación puede tener un impacto positivo en la reducción de fraudes. La metodología cualitativa ofreció una visión profunda de las iniciativas educativas, pero un enfoque cuantitativo podría proporcionar datos más precisos sobre la efectividad de estos programas de formación.

Discusión del Noveno Resultado: Capacitación y Recursos para las Fiscalías

El análisis de la capacitación y los recursos disponibles para las fiscalías, en relación con el objetivo específico de identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023, demostró que una mayor inversión en capacitación técnica y en tecnología avanzada puede mejorar significativamente la capacidad de las fiscalías para manejar casos de fraude informático. Este hallazgo está en línea con la Teoría de Tipicidad en Cibercrimen de Posada (2010), que resalta la necesidad de un marco legal y técnico actualizado para abordar los delitos cibernéticos. El antecedente de Riofrío (2012), que señala la falta de recursos y capacitación en Ecuador, refuerza la importancia de estas inversiones para mejorar la efectividad en la persecución de delitos informáticos. La metodología cualitativa permitió una comprensión detallada de las deficiencias en recursos y capacitación, pero un enfoque cuantitativo podría proporcionar una evaluación más amplia de cómo estos factores impactan la resolución de casos.

Discusión del Décimo Resultado: Propuestas de Reformas Legislativas y Mejoras Procesales

La evaluación de las propuestas de reformas legislativas y mejoras en los procesos judiciales para una mayor eficacia en la persecución y resolución de delitos cibernéticos reveló una necesidad urgente de actualización y

adaptación de las leyes y procedimientos existentes. Este hallazgo se relaciona con el objetivo específico de valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos. La Teoría de la Tipicidad en Cibercrimen de Posada (2010) destaca que la rápida evolución de los delitos cibernéticos y su complejidad técnica a menudo superan los marcos legales existentes, lo que deja vacíos legales que los delincuentes pueden explotar. Este problema es consistente con el análisis de Morales (2016), quien criticó la legislación peruana por no captar adecuadamente la complejidad de los crímenes modernos. La metodología cualitativa permitió identificar áreas específicas donde las reformas son necesarias, como la actualización de leyes y la creación de unidades especializadas. Sin embargo, un enfoque cuantitativo podría ayudar a evaluar la viabilidad y el impacto potencial de las reformas propuestas de manera más sistemática.

Discusión del Primer Caso

El primer caso, relacionado con el fraude informático sufrido por la victima 01, ilustra la falta de responsabilidad bancaria y la impunidad en el sistema financiero, coincidiendo con el objetivo específico de evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos. La Teoría de las Obligaciones de Resultado (Perez, 2018) sostiene que las entidades bancarias tienen una obligación objetiva de asegurar la seguridad de los fondos y datos financieros. El caso revela una deficiencia en las medidas de seguridad y en la respuesta de la entidad bancaria, confirmando que la responsabilidad de los bancos no ha sido adecuadamente cumplida. Esto concuerda con Quiroz (2019), quien propuso que una mayor responsabilidad y mejores prácticas por parte de las instituciones financieras son necesarias para combatir los fraudes informáticos. La falta de acción efectiva por parte del banco en este caso subraya la necesidad de que las entidades adopten un enfoque más proactivo para prevenir y gestionar fraudes, alineándose con la teoría que sugiere que la falta de responsabilidad activa facilita la comisión de delitos cibernéticos.

Discusión del Segundo Caso:

En el segundo caso, relacionado con la incapacidad de la fiscalía para avanzar en la denuncia presentada por el agraviado 2, se destaca la falta de recursos y capacitación en la fiscalía, alineándose con el objetivo específico de identificar las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023. La Teoría de la Tipicidad en Cibercrimen (Posada, 2010) destaca cómo los delitos cibernéticos a menudo caen en vacíos legales debido a su complejidad y rápida evolución. La falta de recursos y capacitación en la fiscalía contribuye a la ineficacia en el procesamiento de casos, lo que coincide con los hallazgos de Nuñez (2022), quien enfatizó la necesidad de una adaptación continua del marco legal y de recursos en las instituciones encargadas de la justicia. La metodología cualitativa revela que la escasez de recursos y la falta de formación específica impiden a las fiscalías abordar adecuadamente los casos de fraude, reflejando la teoría que sugiere que la falta de recursos y actualización legal es una causa significativa para el archivo de denuncias.

Discusión del Tercer Caso.

El tercer caso, que involucra la denuncia de la víctima 3 y la falta de respuesta efectiva por parte de las autoridades, refleja las deficiencias en el proceso judicial y la falta de reformas legislativas. Esto se relaciona con el objetivo específico de Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos. La Teoría del Delito de Rutina (Felson, 1979) sugiere que una mayor presencia de guardianes capaces puede reducir la incidencia de delitos cibernéticos. La falta de reformas adecuadas en el sistema judicial y la ineficacia en la persecución de casos reflejan una ausencia de "guardianes" efectivos. Esto coincide con los hallazgos de Morales (2016), quien criticó la falta de legislación adecuada en Perú y propuso que las reformas podrían mejorar la eficacia en la persecución de delitos informáticos. Los datos cualitativos muestran que la implementación de reformas y mejoras en los procesos judiciales podría aumentar la efectividad en la resolución de casos, confirmando la teoría que plantea que un marco legal robusto y bien aplicado puede disminuir la incidencia de fraudes informáticos.

Discusión del Cuarto Caso:

En el cuarto caso, relacionado con la denuncia presentada la victima 04 sobre la falta de adecuadas medidas de seguridad y protección en su banco, se evidencia un problema persistente en la responsabilidad de las entidades bancarias. Este caso se vincula estrechamente con el objetivo específico de evaluar el rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos.

La Teoría de las Obligaciones de Resultado (Perez, 2018) es particularmente relevante aquí, ya que esta teoría establece que las entidades bancarias tienen una responsabilidad objetiva para asegurar la seguridad de las transacciones financieras y la protección de los datos de sus clientes. El caso revela que la falta de medidas adecuadas por parte del banco facilitó la comisión del fraude, corroborando la teoría que postula que los bancos deben adoptar medidas proactivas y robustas para prevenir delitos cibernéticos. Este hallazgo se alinea con los argumentos presentados por Quiroz (2019), quien enfatizó que la responsabilidad bancaria debe ser una prioridad para reducir la incidencia de fraudes informáticos.

La coincidencia entre la teoría y el caso resalta que, a pesar de la importancia de la teoría en la responsabilización de las entidades bancarias, en la práctica muchas instituciones aún no han implementado medidas de seguridad efectivas. Los datos cualitativos del caso de Luis Alberto Gómez subrayan la necesidad urgente de que los bancos fortalezcan sus políticas de seguridad y prácticas preventivas para proteger a los clientes y evitar que se repitan incidentes similares. Esto confirma que la falta de medidas adecuadas sigue siendo un problema central en la gestión de fraudes informáticos, reflejando la teoría y las recomendaciones previas sobre la necesidad de una mayor responsabilidad bancaria.

IV. CONCLUSIONES

Identificación de las causas principales del archivo de denuncias por fraude informático en las fiscalías penales de Perú durante 2023:

La investigación evidenció que las principales causas del archivo de denuncias por fraude informático en las fiscalías penales de Perú se relacionan con la falta de recursos tecnológicos y la insuficiencia en la capacitación del personal judicial. La ausencia de herramientas tecnológicas adecuadas y la falta de formación especializada en ciberseguridad limitan la capacidad de las fiscalías para llevar a cabo investigaciones exhaustivas. Los fiscales enfrentan dificultades para recolectar y analizar pruebas digitales debido a estas deficiencias. Además, se observó que el marco legal vigente no se ajustaba adecuadamente a la complejidad de los delitos cibernéticos, lo que contribuye a la dificultad para tipificar y procesar estos delitos de manera efectiva. La falta de actualización en la legislación y los procedimientos judiciales impide una respuesta eficaz frente a la creciente incidencia de fraudes cibernéticos.

Evaluación del rol y la responsabilidad de las entidades bancarias en la prevención y gestión de fraudes informáticos:

El estudio subrayó que las entidades bancarias en Perú desempeñan un papel crucial en la prevención y gestión de fraudes informáticos. Sin embargo, se observó una carencia significativa en la implementación de medidas de seguridad adecuadas. Las prácticas de seguridad en las entidades financieras resultaron ser insuficientes para proteger adecuadamente los fondos y datos de los clientes. La falta de responsabilidad de las entidades bancarias en la protección contra fraudes cibernéticos contribuyó a una mayor vulnerabilidad de los clientes. Además, el estudio reveló que, a pesar de las regulaciones existentes, muchas instituciones financieras no cumplen con las normas de seguridad requeridas, lo que incrementa el riesgo de fraudes. La investigación concluyó que es esencial que las entidades bancarias asuman una mayor responsabilidad en la implementación de medidas de seguridad robustas y en la formación de su personal para enfrentar los desafíos de la ciberseguridad.

Propuesta de reformas legislativas y mejoras en los procesos judiciales para asegurar una mayor eficacia en la persecución y resolución de delitos cibernéticos.

Se concluyó que es necesaria una reforma legislativa integral para abordar de manera efectiva los delitos cibernéticos en Perú. La legislación existente no cubría adecuadamente la complejidad de los delitos informáticos, creando vacíos legales que dificultaban la persecución y sanción de estos delitos. La propuesta de reformas incluyó la actualización del marco legal para incluir disposiciones específicas para los delitos cibernéticos y la introducción de procedimientos judiciales especializados en la materia. Además, se sugirió la necesidad de fortalecer los recursos tecnológicos y de capacitación para el personal judicial y policial. La investigación destacó que una reforma legislativa y una mejora en los procesos judiciales podrían aumentar significativamente la eficacia en la persecución y resolución de fraudes cibernéticos, contribuyendo a una mayor seguridad financiera para los clientes y una reducción en la incidencia de estos delitos.

V. RECOMENDACIONES

1. Mejora de recursos tecnológicos y capacitación del personal judicial

La investigación revela que las fiscalías penales en Perú enfrentan deficiencias en recursos tecnológicos y capacitación, lo que contribuye al archivo de denuncias por fraude informático. Se recomienda al Ministerio Público del Perú invertir en tecnología avanzada y en la formación continua del personal judicial y policial, incluyendo el desarrollo de unidades especializadas en ciberdelincuencia. La implementación de estos recursos y capacitación mejorará la capacidad de respuesta en la investigación de delitos cibernéticos, alineándose con estudios que destacan la importancia de la actualización tecnológica y la formación especializada para enfrentar estos delitos de manera más efectiva.

2. Implementación de medidas de seguridad robustas por parte de las entidades bancarias

El estudio señala la carencia de medidas de seguridad adecuadas por parte de las entidades bancarias en Perú, lo que facilita el fraude informático. Se recomienda a la Superintendencia de Banca, Seguros y AFP (SBS) que refuerce la regulación y supervisión de las medidas de seguridad, estableciendo estándares rigurosos como encriptación de datos y autenticación multifactor. Además, se deben realizar campañas educativas para clientes sobre prácticas seguras en línea. Esta recomendación está respaldada por la necesidad de que las instituciones financieras asuman una responsabilidad activa en la protección de datos, como se evidencia en investigaciones previas sobre las obligaciones de resultado.

3. Reforma legislativa integral para abordar los delitos cibernéticos

La legislación peruana actual no cubre adecuadamente la complejidad de los delitos cibernéticos, según el estudio. Se recomienda al Congreso de la República del Perú promover una reforma legislativa integral que incluya disposiciones específicas para delitos informáticos y procedimientos judiciales

especializados. Esta reforma debe reflejar los avances tecnológicos y seguir ejemplos internacionales de actualización legislativa. La creación de un marco legal actualizado fortalecerá la capacidad del sistema judicial para perseguir y sancionar a los perpetradores, como se evidencia en la necesidad de una legislación adecuada observada en estudios anteriores.

4. Uso de herramientas analíticas avanzadas

Para mejorar el entendimiento de los delitos cibernéticos, se recomienda a futuros investigadores utilizar herramientas analíticas avanzadas, como software de análisis de redes y algoritmos de aprendizaje automático. Estos enfoques proporcionarán una visión más detallada sobre las operaciones de los delincuentes y la prevención de delitos. La investigación debe combinar métodos cuantitativos y cualitativos y realizar estudios comparativos internacionales. Estas recomendaciones están alineadas con la necesidad de utilizar enfoques metodológicos diversos para enfrentar los desafíos de la ciberdelincuencia, como se observa en estudios previos sobre la eficacia de métodos analíticos avanzados.

5. Evaluación de la efectividad de las reformas propuestas

Se recomienda que las instituciones académicas y centros de investigación lleven a cabo estudios longitudinales para evaluar el impacto de las reformas legislativas y las medidas de seguridad implementadas en las entidades bancarias. Estos estudios deben medir cómo las reformas afectan la incidencia de delitos cibernéticos y la seguridad financiera. La colaboración con entidades gubernamentales y privadas será crucial para obtener datos precisos. La evaluación continua de políticas y prácticas es esencial para adaptarlas a nuevas amenazas, como se sugiere en investigaciones sobre la importancia de la evaluación constante en el ámbito de la ciberseguridad.

6. Fomento de la cooperación internacional en ciberseguridad

Se recomienda al Gobierno de Perú fomentar la cooperación internacional en ciberseguridad mediante la participación en tratados y acuerdos multilaterales. La colaboración global permitirá compartir conocimientos y mejores prácticas para enfrentar los delitos cibernéticos de manera más efectiva. La ciberdelincuencia es un problema global que requiere una respuesta coordinada, como destacan investigaciones sobre la importancia de la cooperación entre distintas entidades responsables de la seguridad. Establecer alianzas internacionales fortalecerá la capacidad de Perú para protegerse contra amenazas cibernéticas y mejorar la efectividad de su respuesta.

REFERENCIAS

Bermúdez, T. (2021). Aplicaciones de aprendizaje automático en el cibercrimen. *Trabajos de Tecnología y Crimen*.

Clark, J. (2021). Marcos de ciberseguridad: una visión general. Seguridad y privacidad de clientes.

Código Penal Peruano (1991) Lp. Pasión por el Derecho. https://lpderecho.pe/codigo-penal-peruano-actualizado/

Corales, L. (2022). Amenazas persistentes avanzadas y técnicas de mitigación. Sistema de cibernético y delitos criminales.

Donolo, D. (2018). Perspectivas y experiencias creativas. *Cuadernos de la Facultad de Humanidades y Ciencias Sociales - UNJ*. Jujuy, Argentina.

El peruano. (2024, 15 de abril). ¡Cuidado! Crecen denuncias de fraude informático en el Perú. *El peruano*. Recuperado de https://elperuano.pe/noticia/241353-cuidado-crecen-denuncias-de-fraude-informatico-en-el-peru#:~:text=El%20uso%20de%20celulares%20robados,58%25%20respecto%20al%20a%C3%B1o%20previo.

Elson, M., & Cohen, L. E. (1979). Social change and crime rate trends: A routine activity approach. *JSTOR*.

Felson, M., & Cohen, L. E. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*.

Gamarra. A. (2020) Penal Teoría de La Tipicidad. Obtenido de Scribd. https://es.scribd.com/document/263155235/Penal-Teoria-de-la-tipicidad

González, A. L. (2021). La autopuesta en peligro en el derecho penal. *Noticias Jurídicas*.

Harris, K. (2020). Sistemas de detección de amenazas impulsados por inteligencia artificial. *Journal of Cyber Intelligence*.

Hernández Sampieri, R. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (7a ed.). *McGraw-Hill Education*.

Jenkins, L. (2019). Desarrollos recientes en la legislación sobre cibercrimen. *International Law and Policy Review*.

Johnson, H. (2022). Avances en la prevención de delitos digitales. *Cyber Security Review*.

Ley 30096- Ley de delitos informáticos. *Lp Pasion por el Derecho*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://img.lpderecho.pe/wp-content/uploads/2023/08/LEY-30096-LPDerecho_.pdf

Martínez, J. (2019). Teoría de la imputación objetiva: Autoexposición al peligro. *Revista Jurídica de Derecho Penal*.

Maya, R. (2019). La tipicidad en cibercrimen: Perspectiva de la autopuesta en peligro. *Revista Latinoamericana de Derecho Penal*.

Ministerio público (2024) Ministerio Público Fiscalía de la Nación- Distrito Fiscal de Santa https://www.gob.pe/35870-ministerio-publico-fiscalia-de-la-nacion-distrito-fiscal-de-santa

Mitnick, L. C. (2017). La historia de John Draper, el primer "hacker malo" que engañó a los poderosos con un silbato de juguete. *Vocero Cívico*.

Morales, D. (2016). La Inseguridad al Utilizar los Servicios de Redes Sociales y la Problemática Judicial para Regular los Delitos Informáticos en el Perú-2015. [Tesis de Pregrado, Universidad Señor de Sipán]. *Repositorio Institucional USS*. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/3161/MORALES_DELGADO_DEIVID_1%20YULY-1.%20turnitin.pdf?sequence=6&isAllowed=y

Morris, P. (2023). Paisajes de amenazas cibernéticas: Tendencias y tecnologías emergentes. International Journal of Cyber Security.

Muñante, E (2016) Delitos informáticos en Perú. Scribd. https://es.scribd.com/document/503083909/334154783-Delitos-Informaticos-Peru

Navarro, A. L. (2022). La autopuesta en peligro en el derecho penal. Noticias Jurídicas. La Mancha TH: Madrid. España

Nuñez, M. (2022). Tesis Delitos electrónicos procedentes del lavado de activos. [Tesis de Maestría, Universidad de la República Dominicana]. *Scribd*. https://es.scribd.com/document/561251343/Tesis-Delitos-electonicos-procedentes-del-lavado-de-activos-Clairet

Organización para la Cooperación y el Desarrollo Económicos. (2018). Manual de Oslo: Guía para la recogida e interpretación de datos sobre innovación (4ª ed.). *OCDE*.

Peña, G. (2019). Responsabilidad bancaria en la prevención del fraude informático. *Revista de Derecho Financiero*.

Pérez, L. (2018). La teoría de las obligaciones de resultado en el derecho bancario. *Editorial Jurídica Nacional CBA. Mar de Plata Argentina*

Pernias, S. (2020). Responsabilidad de las Entidades Bancarias ante el Consumidor. *Repositorio Dialnet*: https://dialnet.unirioja.es/servlet/tesis?codigo=71671)

Poder Judicial (2023). Portal de Revista del Poder Judicial. Perú. https://revistas.pj.gob.pe/revista/index.php/iusVocatio/article/download/928/1261/

Porthé, L. (2007) Responsabilidad de las Entidades Bancarias ante el Consumidor" (año 2007). *Repositorio Uva: Argentina*. Obtenido de http://www.derecho.uba.ar/publicaciones/lye/revistas/84/09-winitzky-porthe.pdf.

Posada R. (2019). La tipicidad en cibercrimen: Un desafío contemporáneo. *Revista Latinoamericana de Derecho Penal*.

Quiroz, F. (2019). Los Delitos Informáticos y la Protección Penal de la Intimidad en el Distrito Judicial de Lima, Periodo 2008 al 2012. [Tesis de Maestría, Universidad Nacional Federico Villarreal]. Repositorio Institucional UNFV. https://unfv.edu.pe/repositorio

Ramos, M. (2022). Impacto de los delitos informáticos en las investigaciones preparatorias de las fiscalías provinciales penales corporativas del distrito fiscal Lima Sur 2022: Repositorio. *Norvert Wiener*. Lima, Perú.

Riofrío Tacuri, J. F. (2012). Los Delitos Informáticos y su Tipificación en la Legislación Ecuatoriana. [Tesis de Maestría, Universidad Nacional de Loja]. *Repositorio Digital - Universidad Nacional de Loja*. https://unl.edu.ec

Roxin, C. (2006). Derecho penal parte general: Fundamentos y teoría de la imputación (6th *ed.). Editorial Temis.*

Sampieri, R. (2018). Teoría de la autopuesta de Claux Roxin, perspectiva de oro: Investigaciones Jurídicas. Bogotá: Colombia.

San Martin, P. (2012). Derecho Penal: Parte General. *Jurista editores. Lima. Perú.*

Smith, G. (2020). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.

Tellez, J. (2021) Delitos cibernéticos 2021. *Dialent*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=248139

Vera, M. (2011). Delitos informáticos en las organizaciones. [Tesis de Maestría, Universidad Nacional Autónoma de Honduras]. *Repositorio Institucional UNAH*. *Scribd*. https://es.scribd.com/document/337222608/Proyecto-de-Investigacion-derecho-informatico

ANEXOS

Anexo 1. Tabla de categorización.

Categorías de estudio	Definición conceptual	subcategoría	Indicadores
Naturaleza y Alcance de los Delitos Cibernéticos	Los delitos cibernéticos se definen como conductas ilícitas perpetradas a través de sistemas informáticos, redes y dispositivos digitales, que pueden involucrar la manipulación, destrucción o acceso no autorizado a datos y sistemas. Estos delitos abarcan una amplia gama de actividades delictivas, desde el fraude y la estafa hasta el espionaje y el sabotaje informático (Tellez, 2021).	Tipos de Delitos Cibernéticos	• Clasificación de delitos cibernéticos (fraude informático, robo de identidad, etc.). • Frecuencia de cada tipo de delito reportado en el periodo de estudio.
		Tendencias y Estadísticas	• Incidencia anual de delitos cibernéticos. • Tendencias de crecimiento o disminución. • Estadísticas relacionadas con casos reportados y resueltos.

Legislación y Marco Normativo en Perú	La legislación y el marco normativo en Perú sobre delitos cibernéticos abordan las leyes y regulaciones diseñadas para prevenir, sancionar y controlar los delitos cometidos en el entorno digital. San Martin (2012) indica que el marco normativo peruano ha evolucionado lentamente para adaptarse a los nuevos desafíos que presentan los delitos cibernéticos, con una legislación que todavía enfrenta dificultades para abarcar todas las formas de ciberdelincuencia emergentes.	Leyes Específicas	• Identificación de leyes y regulaciones relevantes (Ley de Protección de Datos Personales, Ley de Delitos Informáticos, etc.). • Evaluación de la aplicabilidad y eficacia de estas leyes.
		Revision de Reformas	• Propuestas de reformas legislativas. • Impacto esperado de las reformas en la seguridad cibernética. • Estado actual de la implementación de reformas.

Medidas Preventivas y Estrategias de Manejo por Parte de Instituciones Bancarias	Las medidas preventivas y estrategias de manejo por parte de instituciones bancarias incluyen prácticas y políticas destinadas a proteger los sistemas financieros y la información de los clientes contra los ataques cibernéticos. Según Pernias (2020), estas medidas pueden incluir la implementación de tecnologías de seguridad avanzadas, procedimientos internos de monitoreo y auditoría, así como la formación continua del personal para detectar y responder a amenazas cibernéticas.	Medidas de Seguridad Implementadas	• Tecnologías de seguridad implementadas (firewalls, sistemas de detección de intrusos). • Procedimientos de seguridad (autenticación multifactor, cifrado de datos). • Efectividad de las medidas de seguridad.
		Educación y Capacitación	• Programas de capacitación para empleados y clientes • Materiales educativos utilizados (guías, talleres). • Evaluación de la efectividad de los programas de formación.
Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías	La gestión de casos de delitos cibernéticos por parte de las fiscalías implica la investigación, procesamiento y resolución de casos relacionados con la	Causas del Archivo de Casos	• Razones documentadas para el archivo de casos (falta de evidencia, falta de cooperación, etc.) • Número de casos archivados por año. • Causas recurrentes para el archivo de casos.

	ciberdelincuencia. Según Ramos (2022), esta gestión requiere de habilidades especializadas y recursos adecuados para manejar la complejidad técnica de los delitos cibernéticos, además de una colaboración efectiva con entidades tecnológicas y de seguridad.	Barreras en la Investigación	• Dificultades encontradas durante la investigación (identificación de responsables, falta de cooperación). • Medidas tomadas para superar estas barreras. • Efectividad de las acciones correctivas
Responsabilidad y Rol de las Entidades Bancarias	La responsabilidad y el rol de las entidades bancarias en el contexto de delitos cibernéticos implican garantizar la seguridad de las transacciones y la protección de la información del cliente. Porthé (2007) sostiene	Obligaciones de Resultado Evaluación de Responsabilidad	• Políticas de seguridad de los bancos en relación con la protección de datos. • Evaluación de la responsabilidad objetiva de los bancos. • Casos documentados de incumplimiento y sus consecuencias. • Cumplimiento de las obligaciones de

	que las entidades bancarias tienen la obligación de implementar medidas de seguridad robustas y responder de manera adecuada a los incidentes de fraude, para evitar daños financieros y preservar la confianza del cliente.		seguridad por parte de los bancos. • Casos de fallos en la seguridad y sus impactos. • Medidas correctivas implementadas por los bancos.
Perspectivas y Experiencias de Profesionales	Las perspectivas y experiencias de profesionales en el ámbito de los delitos cibernéticos se refieren a la visión y vivencias de expertos que trabajan en la prevención, investigación y resolución de estos delitos. Donolo (2018) señala que las experiencias de estos profesionales son	Percepciones de Abogados y Fiscales	• Opiniones sobre los desafíos y dificultades en la gestión de delitos cibernéticos. • Experiencias y casos relevantes. • Recomendaciones para mejorar la gestión de delitos.
		Fundamentación de Decisiones	• Criterios utilizados para tomar decisiones en casos de fraude informático. • Justificaciones para el archivo o

	fundamentales para comprender las dificultades prácticas y las brechas existentes en la lucha contra la ciberdelincuencia, así como para desarrollar estrategias más efectivas.	prosecución de casos. • Evaluación de la consistencia en la toma de decisiones.

Fuente: Creación propia

Anexo 02. Instrumento de recolección de datos

Universidad Cesar Vallejo

Instrumento de recolección de datos

Guía de entrevista

Reciba mí cordial saludo y a la vez le informo que su participación es muy valiosa en la investigación titulada: Delitos Cibernéticos en Perú 2024: Análisis y propuesta de prevención para una mayor responsabilidad Bancaria Chimbote – 2024. Las respuestas son absolutamente anónimas y confidenciales las mismas que serán respondidas desde su experiencia; y que serán empleados únicamente para fines de investigación.

A continuación, se procederá a dar inicio a la entrevista:

Declaro que acepto de manera voluntaria responder a las siguientes preguntas. A continuación, se procederá a dar inicio a la entrevista:

Categoría: Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías
Subcategoría: Causas del Archivo de Casos

1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?

Categoría: Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías
Subcategoría: Barreras en la Investigación

2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?

---

3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?

Categoría: Responsabilidad y Rol de las Entidades Bancarias Subcategoría: Obligaciones de Resultado

4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?

Categoría: Legislación y Marco Normativo en Perú

Subcategoría: Revisión de Reformas

5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?

Categoría: Legislación y Marco Normativo en Perú

Subcategoría: Leyes especificas

6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?

Categoría: Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías

Subcategoría: Barreras en la Investigación

7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?

Categoría: Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías
Subcategoría: Causas del Archivo de Casos

8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?

Categoría: Responsabilidad y Rol de las Entidades Bancarias

Subcategoría: Evaluación de Responsabilidad

9. Pregunta 9: ¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?

Categoría: Perspectivas y Experiencias de Profesionales
Subcategoría: Fundamentación de Decisiones

10. ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?

Universidad Cesar Vallejo

FICHA PARA EL ANALISIS DE LA CASOS FISCALES

A continuación, se presenta una guía detallada sobre cómo estructurara y presentar una ficha de registro de datos, asegurando que sea clara y funcional.

• Descripción del caso:	
• Disposición:	
• Motivos del archivo de las denuncias por fraude informático.	
• Conclusión:	

Anexo 3. Fichas de validación de instrumentos para la recolección de datos

Ficha de validación de juicio de experto

Experto N°01	
Nombre del instrumento	Encuesta
Objetivo del instrumento	Recoger opiniones de magistrados, con el fin de evidenciar que los casos de fraude informático se archivan frecuentemente debido a la imposibilidad de identificar a los presuntos responsables.
Nombres y apellidos del experto	Mg. Carmen Nelly Macuado Arroyo.
Documento de identidad	32966345
Años de experiencia en el área	16 años
Máximo Grado Académico	Magister en Gestión Pública.
Nacionalidad	Peruana
Institución	Ministerio Público
Cargo	Fiscal Provincial Penal de la Segunda Fiscalía Provincial Penal Corporativa del Santa.
Número telefónico	943 911 343
Firma	Carmen Nelly Macuado Arroyo FISCAL PROVINCIAL (T) SEGUNDA FISCALIA PROVINCIAL PENAL CORPORATIVA DEL SANTA DISTRITO FISCAL DEL SANTA
Fecha	22 de Mayo del 2024

Matriz de validación de la guía de entrevista de las categorías

Categoría	**Indicador**	**Ítem**	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	Observación
Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías	Causas del Archivo de Casos	¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?	1	1	1	1	
	Barreras en la Investigación	¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?	1	1	1	1	
		¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?	1	1	1	1	
		¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?	1	1	1	1	
	Causas del Archivo de Casos	¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?	1	1	1	1	
Responsabilidad y Rol de las Entidades Bancarias	Obligaciones de Resultado	¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?	1	1	1	1	
	Evaluación de Responsabilidad	¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?	1	1	1	1	
Legislación y Marco Normativo en Perú	Revisión de Reformas	¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?	1	1	1	1	
	Leyes Específicas	¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?	1	1	1	1	
Perspectivas y Experiencias de	Fundamentación de	¿Qué recomendaciones tiene para	1	1	1	1	

Profesionales	Decisiones	mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?					

Explicación de los Criterios:

- Suficiencia: Evalúa si el ítem cubre de manera adecuada el indicador dentro de la categoría.
- Claridad: Evalúa si el ítem está redactado de manera comprensible y fácil de interpretar.
- Coherencia: Evalúa si el ítem se alinea con los objetivos generales de la investigación y mantiene una relación lógica con las demás preguntas.
- Relevancia: Evalúa la importancia del ítem en relación con la obtención de datos significativos para la investigación.
- Observaciones: Espacio para anotar cualquier comentario adicional que los evaluadores deseen realizar.

Experto N°02	
Nombre del instrumento	Encuesta
Objetivo del instrumento	Recoger opiniones de magistrados, con el fin de evidenciar que los casos de fraude informático se archivan frecuentemente debido a la imposibilidad de identificar a los presuntos responsables.
Nombres y apellidos del experto	Mg. Donald Esteban Quilcate Galicia.
Documento de identidad	32960938
Años de experiencia en el área	12 años
Máximo Grado Académico	Magister en Derecho Civil y Procesal Civil.
Nacionalidad	Peruana
Institución	Ministerio Público
Cargo	Fiscal Adjunto Provincial.
Número telefónico	980089675
Firma	Donald Esteban Quilcate Galicia FISCAL ADJUNTO PROVINCIAL (T) SEGUNDA FISCALÍA PROVINCIAL PENAL CORPORATIVA DISTRITO FISCAL [illegible] SANTA
Fecha	22 de Mayo del 2024.

Matriz de validación de la guía de entrevista de las categorías

Categoría	**Indicador**	**Ítem**	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	Observación
Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías	Causas del Archivo de Casos	¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?	1	1	1	1	
	Barreras en la Investigación	¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?	1	1	1	1	
		¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?	1	1	1	1	
		¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?	1	1	1	1	
	Causas del Archivo de Casos	¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?	1	1	1	1	
Responsabilidad y Rol de las Entidades Bancarias	Obligaciones de Resultado	¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?	1	1	1	1	
	Evaluación de Responsabilidad	¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?	1	1	1	1	
Legislación y Marco Normativo en Perú	Revisión de Reformas	¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?	1	1	1	1	
	Leyes Específicas	¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?	1	1	1	1	

Perspectivas y Experiencias de Profesionales	Fundamentación de Decisiones	¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?	1	1	1	1	

Explicación de los Criterios:

- Suficiencia: Evalúa si el ítem cubre de manera adecuada el indicador dentro de la categoría.
- Claridad: Evalúa si el ítem está redactado de manera comprensible y fácil de interpretar.
- Coherencia: Evalúa si el ítem se alinea con los objetivos generales de la investigación y mantiene una relación lógica con las demás preguntas.
- Relevancia: Evalúa la importancia del ítem en relación con la obtención de datos significativos para la investigación.
- Observaciones: Espacio para anotar cualquier comentario adicional que los evaluadores deseen realizar.

Experto N°03	
Nombre del instrumento	**Encuesta**
Objetivo del instrumento	Recoger opiniones de magistrados, con el fin de evidenciar que los casos de fraude informático se archivan frecuentemente debido a la imposibilidad de identificar a los presuntos responsables.
Nombres y apellidos del experto	Mg. Jorge Luis Ricser Flores
Documento de identidad	32816235
Años de experiencia en el área	19 años
Máximo Grado Académico	Magister en Derecho Penal y Procesal Penal.
Nacionalidad	Peruano
Institución	Ministerio Público
Cargo	Fiscal Adjunto Provincial Penal
Número telefónico	972953862
Firma	 Jorge L. Ricser Flores FISCAL ADJUNTO PROVINCIAL(T) SEGUNDA FISCALIA PROVINCIAL PENAL CORPORATIVA DEL SANTA DISTRITO FISCAL DEL SANTA
Fecha	22 de mayo del 2024

Matriz de validación de la guía de entrevista de las categorías

Categoría	**Indicador**	**Ítem**	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	Observación
Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías	Causas del Archivo de Casos	¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?	1	1	1	1	
	Barreras en la Investigación	¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?	1	1	1	1	
		¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?	1	1	1	1	
		¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?	1	1	1	1	
	Causas del Archivo de Casos	¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?	1	1	1	1	
Responsabilidad y Rol de las Entidades Bancarias	Obligaciones de Resultado	¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?	1	1	1	1	
	Evaluación de Responsabilidad	¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?	1	1	1	1	
Legislación y Marco Normativo en Perú	Revisión de Reformas	¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?	1	1	1	1	
	Leyes Específicas	¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?	1	1	1	1	
Perspectivas y Experiencias de	Fundamentación de	¿Qué recomendaciones tiene para	1	1	1	1	

Profesionales	Decisiones	mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?					

Explicación de los Criterios:

- Suficiencia: Evalúa si el ítem cubre de manera adecuada el indicador dentro de la categoría.
- Claridad: Evalúa si el ítem está redactado de manera comprensible y fácil de interpretar.
- Coherencia: Evalúa si el ítem se alinea con los objetivos generales de la investigación y mantiene una relación lógica con las demás preguntas.
- Relevancia: Evalúa la importancia del ítem en relación con la obtención de datos significativos para la investigación.

Observaciones: Espacio para anotar cualquier comentario adicional que los evaluadores deseen realizar

Experto N°04	
Nombre del instrumento	**Encuesta**
Objetivo del instrumento	Recoger opiniones de magistrados, con el fin de evidenciar que los casos de fraude informático se archivan frecuentemente debido a la imposibilidad de identificar a los presuntos responsables.
Nombres y apellidos del experto	Mg. Maguin Arévalo Minchola
Documento de identidad	44992024
Años de experiencia en el área	14 años
Máximo Grado Académico	Magister en Derecho Penal
Nacionalidad	Peruano
Institución	Ministerio Público
Cargo	Fiscal Provincial(T) del DF. Santa.
Número telefónico	996353664
Firma	
Fecha	23 de mayo del 2024.

MAGUIN ARÉVALO MINCHOLA
FISCAL PROVINCIAL
TERCERA FISCALÍA PROVINCIAL PENAL
CORPORATIVA DEL SANTA

Matriz de validación de la guía de entrevista de las categorías

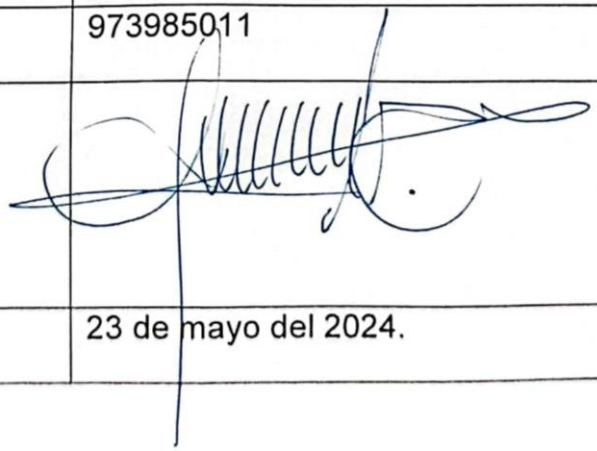
Categoría	**Indicador**	**Ítem**	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	Observación
Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías	Causas del Archivo de Casos	¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?	1	1	1	1	
	Barreras en la Investigación	¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?	1	1	1	1	
		¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?	1	1	1	1	
		¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?	1	1	1	1	
	Causas del Archivo de Casos	¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?	1	1	1	1	
Responsabilidad y Rol de las Entidades Bancarias	Obligaciones de Resultado	¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?	1	1	1	1	
	Evaluación de Responsabilidad	¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?	1	1	1	1	
Legislación y Marco Normativo en Perú	Revisión de Reformas	¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?	1	1	1	1	
	Leyes Específicas	¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?	1	1	1	1	
Perspectivas y Experiencias de	Fundamentación de	¿Qué recomendaciones tiene para	1	1	1	1	

Profesionales	Decisiones	mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?					

Explicación de los Criterios:

- Suficiencia: Evalúa si el ítem cubre de manera adecuada el indicador dentro de la categoría.
- Claridad: Evalúa si el ítem está redactado de manera comprensible y fácil de interpretar.
- Coherencia: Evalúa si el ítem se alinea con los objetivos generales de la investigación y mantiene una relación lógica con las demás preguntas.
- Relevancia: Evalúa la importancia del ítem en relación con la obtención de datos significativos para la investigación.

Observaciones: Espacio para anotar cualquier comentario adicional que los evaluadores deseen realizar

Experto N°05	
Nombre del instrumento	**Encuesta**
Objetivo del instrumento	Recoger opiniones de magistrados, con el fin de evidenciar que los casos de fraude informático se archivan frecuentemente debido a la imposibilidad de identificar a los presuntos responsables.
Nombres y apellidos del experto	Dr. Jaime Li García
Documento de identidad	18198363
Años de experiencia en el área	9 años
Máximo Grado Académico	Doctor
Nacionalidad	Peruano
Institución	Ministerio Público
Cargo	Fiscal Adjunto Provincial(T) del DF Santa.
Número telefónico	973985011
Firma	
Fecha	23 de mayo del 2024.

Matriz de validación de la guía de entrevista de las categorías

Categoría	**Indicador**	**Ítem**	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	Observación
Gestión de Casos de Delitos Cibernéticos por Parte de las Fiscalías	Causas del Archivo de Casos	¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?	1	1	1	1	
	Barreras en la Investigación	¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?	1	1	1	1	
		¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?	1	1	1	1	
		¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?	1	1	1	1	
	Causas del Archivo de Casos	¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?	1	1	1	1	
Responsabilidad y Rol de las Entidades Bancarias	Obligaciones de Resultado	¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?	1	1	1	1	
	Evaluación de Responsabilidad	¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?	1	1	1	1	
Legislación y Marco Normativo en Perú	Revisión de Reformas	¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?	1	1	1	1	
	Leyes Específicas	¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?	1	1	1	1	
Perspectivas y Experiencias de	Fundamentación de	¿Qué recomendaciones tiene para	1	1	1	1	

Profesionales	Decisiones	mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?					

Explicación de los Criterios:

- Suficiencia: Evalúa si el ítem cubre de manera adecuada el indicador dentro de la categoría.
- Claridad: Evalúa si el ítem está redactado de manera comprensible y fácil de interpretar.
- Coherencia: Evalúa si el ítem se alinea con los objetivos generales de la investigación y mantiene una relación lógica con las demás preguntas.
- Relevancia: Evalúa la importancia del ítem en relación con la obtención de datos significativos para la investigación.
- Observaciones: Espacio para anotar cualquier comentario adicional que los evaluadores deseen realizar.

Anexo 5. Consentimiento informado UCV

Universidad Cesar Vallejo

Título de la investigación: Delitos cibernéticos en Perú 2023: Análisis y propuesta de prevención para una mayor responsabilidad bancaria

Investigadora **:** Carlin Ruiz Licencia Esmith

Le invitamos a participar en la investigación titulada “Delitos cibernéticos en Perú 2023: Análisis y propuesta de prevención para una mayor responsabilidad bancaria”, cuyo objetivo es analizar las tendencias actuales y Valorar la pertinencia de implementar nuevas reformas legislativas sobre delitos cibernéticos. Esta investigación es desarrollada por estudiantes del programa de Derecho y Tecnología de la Información, de la Universidad César Vallejo del campus Trujillo, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución financiera Banco de Perú.

La ciberdelincuencia ha mostrado un crecimiento alarmante en Perú, afectando la confianza en el sistema bancario y causando pérdidas económicas significativas. Este estudio busca comprender mejor este fenómeno para contribuir a la creación de un entorno bancario más seguro.

Si usted decide participar en la investigación se realizará lo siguiente:

1. Se realizará una encuesta o entrevista donde se recogerán datos personales y algunas preguntas relacionadas con su experiencia y percepción sobre la ciberdelincuencia.
2. Esta encuesta o entrevista tendrá un tiempo aproximado de 30 minutos y se realizará en el ambiente de la sala de conferencias de la institución Banco de Perú. Las respuestas al cuestionario o guía de entrevista serán codificadas usando un número de identificación y, por lo tanto, serán anónimas.

Su participación es completamente voluntaria. Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Puede dejar de participar en cualquier momento sin ningún problema.

La participación en la investigación no implica riesgo o daño. Sin embargo, si alguna pregunta le genera incomodidad, tiene la libertad de no responderla.

Los resultados de la investigación se compartirán con la institución al término de la misma. No recibirá ningún beneficio económico ni de ninguna otra índole. Los resultados del estudio podrán convertirse en beneficio de la salud pública.

Los datos recolectados serán anónimos y no tendrán ninguna forma de identificar al participante. La información recogida es totalmente confidencial y no será usada para

ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y serán eliminados convenientemente después de un tiempo determinado.

Si tiene preguntas sobre la investigación puede contactar con el Investigador carlinruizlicenia1@gmail.com.

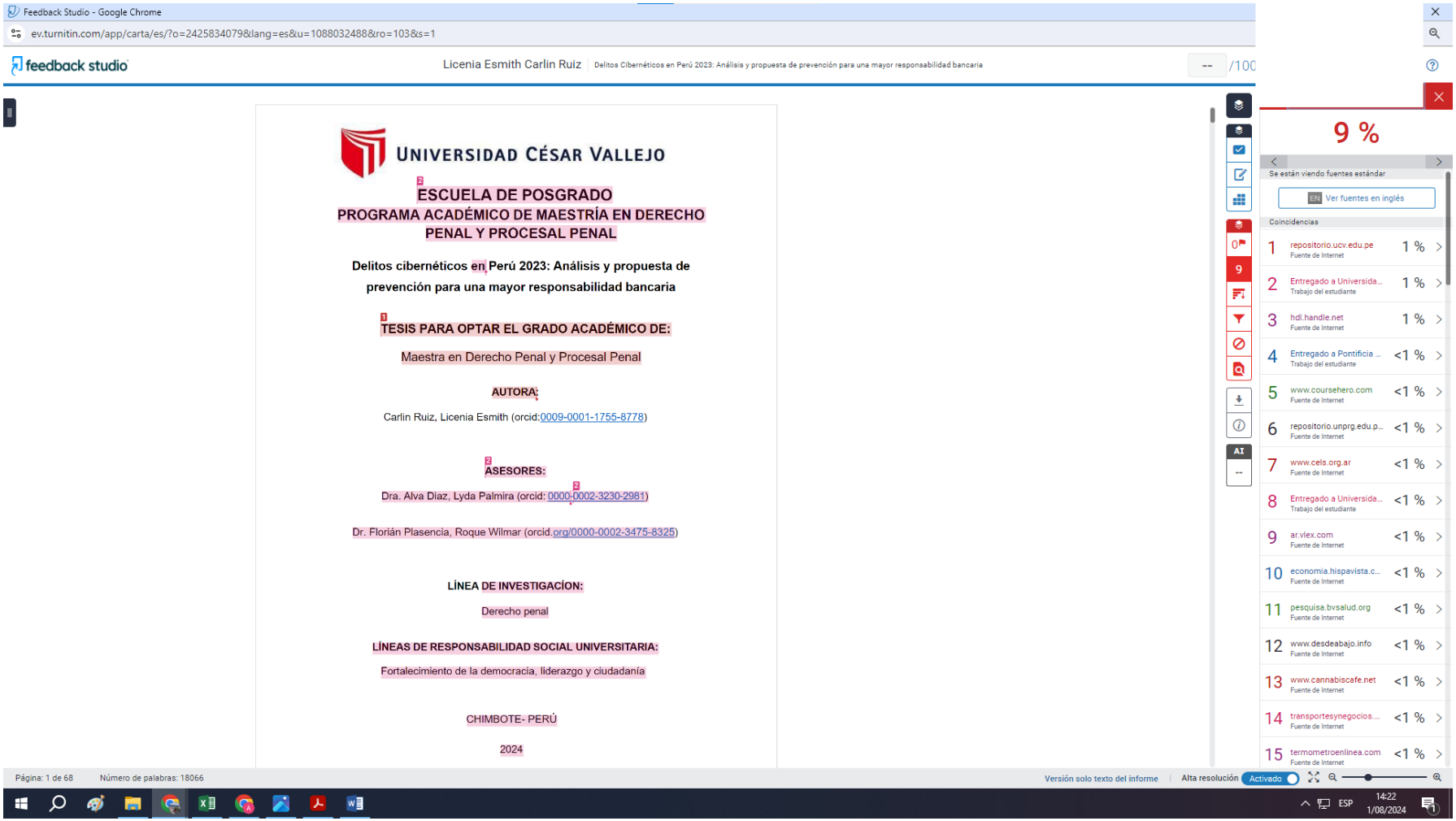
Después de haber leído los propósitos de la investigación autorizo mi participación en la investigación.

Nombre y apellidos:_____

Firma(s): _____

Fecha y Hora: _____

Anexo 6. Reporte de similitud en software Turnitin



Anexo 7. Análisis complementario

Tabla 18 Relación de participantes entrevistados

N°	Nombres y Apellidos	Edad	Sexo	Profesión
1	Xxxxxxx, xxxxxxxxxx	55	Femenino	Abogado
2	Xxxxxxx, xxxxxxxxxx	60	Masculino	Abogado
3	Xxxxxxx, xxxxxxxxxx	45	Femenino	Abogado
4	Xxxxxxx, xxxxxxxxxx	48	Femenino	Abogado
5	Xxxxxxx, xxxxxxxxxx	53	Masculino	Abogado
6	Xxxxxxx, xxxxxxxxxx	43	Femenino	Abogado
7	Xxxxxxx, xxxxxxxxxx	54	Masculino	Abogado
8	Xxxxxxx, xxxxxxxxxx	59	Femenino	Abogado

Fuente: Creación propia, extraída del aplicativo Excel

Anexo 8. Autorizaciones para el desarrollo del proyecto de investigación

MINISTERIO PÚBLICO
DISTRITO FISCAL DEL SANTA
PRESIDENCIA DE LA JUNTA DE FISCALES SUPERIORES
06 JUN 2024
RECIBIDO
HORA: 9:10 FIRMA

UNIVERSIDAD CÉSAR VALLEJO

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

Chimbote, 30 de mayo del 2024.

Doctora:

MIRIAM LUCERO TAMAYO

PRESIDENTA DE LA JUNTA DE FISCALES DEL MINISTERIO PÚBLICO DF. SANTA

Presente. -

Es grato dirigirme a vuestro superior despacho para saludarla, y a la vez manifestarle que dentro de mi formación académica en la experiencia curricular de investigación del III ciclo del Programa de MAESTRIA EN DERECHO PENAL Y PROCESAL PENAL, se contempla la realización de una investigación (Tesis) con fines netamente académicos para la obtención de mi respectivo grado.

En tal sentido, considerando la relevancia de su organización, solicito su colaboración, y tenga a bien autorizar para que la suscrita pueda aplicar su guía de entrevista en las áreas correspondientes, así como se le facilite la información pertinente para el respectivo análisis documental, lo cual es de vital importancia para el desarrollo de la investigación titulada:Delitos cibernéticos en Perú 2023: "Análisis y propuesta de prevención para una mayor responsabilidad bancaria".

Asimismo, me comprometo en el desarrollo de la investigación a mantener en reserva el nombre o cualquier distintivo de la institución.

Agradeciéndole anticipadamente por vuestro apoyo en favor de mi formación profesional, hago propicia la oportunidad para expresar las muestras de mi especial consideración.

Atentamente,

LICENIA ESMITH CARLIN RUIZ

DNI Nª 42265964

Anexo 9. Otras evidencias

Universidad Cesar Vallejo

Instrumento de recolección de datos

Guía de entrevista

Reciba mí cordial saludo y a la vez le informo que su participación es muy valiosa en la investigación titulada: Delitos Cibernéticos en Perú 2024: Análisis y propuesta de prevención para una mayor responsabilidad Bancaria Chimbote – 2024. Las respuestas son absolutamente anónimas y confidenciales las mismas que serán respondidas desde su experiencia; y que serán empleados únicamente para fines de investigación.

A continuación, se procederá a dar inicio a la entrevista:

Declaro que acepto de manera voluntaria responder a las siguientes preguntas ☐

A continuación, se procederá a dar inicio a la entrevista:

PREGUNTAS

1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?.

   Falta de colaboración efectiva con las entidades bancarias

2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?.

Resistencia de las entidades bancarias a compartir información crucial.

3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?

La colaboración es crucial pero generalmente no se da de manera efectiva.

4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?.

Deben ser más proactivos en la prevención y gestión de fraudes

5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?

Fortalecer la ley para mejorar la cooperación internacional y tecnológica

6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley N° 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?.

Requiere revisión para incluir cooperación y tecnología avanzada

7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?.

Dificultades al rastrear delincuentes internacionales

8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?.

La falta de evidencia es una barrera importante para la prosecución de casos

9. Pregunta 9: ¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?

Debe mejorar para cubrir adecuadamente los perdidos de los víctimas.

10. ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?.

Implementar un enfoque más coordinado y aumentar la inversión en tecnología y formación

Universidad Cesar Vallejo

Instrumento de recolección de datos

Guía de entrevista

Reciba mí cordial saludo y a la vez le informo que su participación es muy valiosa en la investigación titulada: Delitos Cibernéticos en Perú 2024: Análisis y propuesta de prevención para una mayor responsabilidad Bancaria Chimbote – 2024. Las respuestas son absolutamente anónimas y confidenciales las mismas que serán respondidas desde su experiencia; y que serán empleados únicamente para fines de investigación.

A continuación, se procederá a dar inicio a la entrevista:

Declaro que acepto de manera voluntaria responder a las siguientes preguntas [X]

A continuación, se procederá a dar inicio a la entrevista:

PREGUNTAS

1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?.

   Carencia de procedimientos estandarizados para el seguimiento de casos

2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?.

Carencia de personal capacitado en ciberataques

3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?

La cooperación entre las partes es insuficiente

4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?.

Implementar medidas de seguridad avanzadas y mantener una comunicación efectiva

5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?

Necesidad de ajustes para enfrentar la evolución del cibercrimen

6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?.

Es una base, pero carece de elementos, para enfrentar el cibercrimen

7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?.

Insuficiente capacitación y recursos, y complejidad de los delitos.

8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?.

Muchos casos se archivan debido a la falta de pruebas concretas

9. Pregunta 9: ¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?

Las Compensaciones Suelen ser parciales y no siempre cubren el daño total.

10. ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?.

Reforzar la colaboración y modernizar los herramientas investigativos.

Universidad Cesar Vallejo

Instrumento de recolección de datos

Guía de entrevista

Reciba mí cordial saludo y a la vez le informo que su participación es muy valiosa en la investigación titulada: Delitos Cibernéticos en Perú 2024: Análisis y propuesta de prevención para una mayor responsabilidad Bancaria Chimbote – 2024. Las respuestas son absolutamente anónimas y confidenciales las mismas que serán respondidas desde su experiencia; y que serán empleados únicamente para fines de investigación.

A continuación, se procederá a dar inicio a la entrevista:

Declaro que acepto de manera voluntaria responder a las siguientes preguntas [X]

A continuación, se procederá a dar inicio a la entrevista:

PREGUNTAS

1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?.

   Limitaciones en recursos tecnológicos y falta de personal capacitado.

2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?.

Falta de recursos y falta de comunicación efectiva entre las partes.

3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?

Falta de acuerdos claros entre fiscales y entidades bancarios

4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?.

Las entidades Bancarios deben cumplir con estándares de seguridad mas estrictos.

5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?

Incorporar medidas para enfrentar nuevas amenazas y técnicas utilizadas por los ciberdelincuentes

6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?.

La ley se queda corta frente a la deducción del ciberarimen.

7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?.

Falta de herramientas adecuadas y rápida evolución del ciberarimen

8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?.

La insuficiencia de evidencia suele ser un motivo principal para el archivo de casos

9. Pregunta 9: ¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?

No siempre es adecuada ni suficiente para el perjuicio sufrido

10. ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?.

Proporcionar recursos tecnológicos y capacitación adecuada

Universidad Cesar Vallejo

Instrumento de recolección de datos

Guía de entrevista

Reciba mí cordial saludo y a la vez le informo que su participación es muy valiosa en la investigación titulada: Delitos Cibernéticos en Perú 2024: Análisis y propuesta de prevención para una mayor responsabilidad Bancaria Chimbote – 2024. Las respuestas son absolutamente anónimas y confidenciales las mismas que serán respondidas desde su experiencia; y que serán empleados únicamente para fines de investigación.

A continuación, se procederá a dar inicio a la entrevista:

Declaro que acepto de manera voluntaria responder a las siguientes preguntas [X]

A continuación, se procederá a dar inicio a la entrevista:

PREGUNTAS

1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?.

   Falta de evidencia suficiente y dificultades en la recolección de datos.

2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?.

Falta de herramientas para el análisis de datos.

3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?

La colaboración no siempre se establece adecuadamente.

4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?.

Responsabilidad clave en la protección de datos y en la respuesta a incidentes de fraude

5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?

Reformas que incluyan mejor cooperación y herramientas tecnológicas

6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley N° 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?.

Necesita abordar tecnología y cooperación internacional

7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?.

Insuficiente capacitación y recursos y complejidad de los delitos

8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?.

La falta de pruebas adecuados dificulta la prosecución efectiva de los casos

9. Pregunta 9: ¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?

Frecuentemente las compensaciones no cubren el impacto total del Fraude

10. ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?.

Mejorar la cooperación y actualización tecnológica en las investigaciones

Universidad Cesar Vallejo

Instrumento de recolección de datos

Guía de entrevista

Reciba mí cordial saludo y a la vez le informo que su participación es muy valiosa en la investigación titulada: Delitos Cibernéticos en Perú 2024: Análisis y propuesta de prevención para una mayor responsabilidad Bancaria Chimbote – 2024. Las respuestas son absolutamente anónimas y confidenciales las mismas que serán respondidas desde su experiencia; y que serán empleados únicamente para fines de investigación.

A continuación, se procederá a dar inicio a la entrevista:

Declaro que acepto de manera voluntaria responder a las siguientes preguntas [X]

A continuación, se procederá a dar inicio a la entrevista:

PREGUNTAS

1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?.

   Inadecuada coordinación interinstitucional y falta de herramientas especializadas.

2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?.

Deficiencia en la integración de tecnologías en el proceso investigativo.

3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?

La falta de integración y comunicación entre las entidades es un problema.

4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?.

Necesitan reforzar sus políticas de seguridad y educación para prevenir fraudes

5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?

Enfoque integral con reformas legislativas y mejoras en la tecnología y cooperación

6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?.

Requiere ajustes para modernizar herramientas y mejorar la coordinación internacional.

7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?.

Falta de cooperación internacional y necesidad de tecnología avanzada.

8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?.

Sin evidencia solida, los casos de fraude suelen ser archivados.

9. Pregunta 9: ¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?

Las compensaciones deben ser mas integrales y justas para las victimas

10. ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?.

Adoptar un enfoque integral con reformas legislativas y mejorar tecnológicas.

Universidad Cesar Vallejo

Instrumento de recolección de datos

Guía de entrevista

Reciba mí cordial saludo y a la vez le informo que su participación es muy valiosa en la investigación titulada: Delitos Cibernéticos en Perú 2024: Análisis y propuesta de prevención para una mayor responsabilidad Bancaria Chimbote – 2024. Las respuestas son absolutamente anónimas y confidenciales las mismas que serán respondidas desde su experiencia; y que serán empleados únicamente para fines de investigación.

A continuación, se procederá a dar inicio a la entrevista:

Declaro que acepto de manera voluntaria responder a las siguientes preguntas ☑

A continuación, se procederá a dar inicio a la entrevista:

PREGUNTAS

1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?.

   Falta de evidencia concreta.

2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?.

Falta de colaboración con las entidades bancarias

3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?

La colaboración es deficiente, Falta de comunicación efectiva.

4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?.

Implementar Sistemas de Seguridad robustos y capacitar al personal

5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?

Actualizar las leyes para abordar nuevas formas de cibercrimen

6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?.

Es un buen inicio pero no es suficiente para la complejidad actual

7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?.

Falta de herramientas tecnológicos adecuados

8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?.

La falta de evidencia concreta a menudo lleva al archivo de los casos.

9. Pregunta 9: ¿Cómo percibe la compensación para las víctimas de fraude informático en Perú?

La compensación es a menudo insuficiente y no satisface completamente a los víctimas

10. ¿Qué recomendaciones tiene para mejorar el proceso de investigación y procesamiento de delitos cibernéticos en Perú?.

Mejorar la tecnología utilizada y fortalecer la colaboración interinstitucional

Universidad Cesar Vallejo

Instrumento de recolección de datos

Guía de entrevista

Reciba mí cordial saludo y a la vez le informo que su participación es muy valiosa en la investigación titulada: Delitos Cibernéticos en Perú 2024: Análisis y propuesta de prevención para una mayor responsabilidad Bancaria Chimbote – 2024. Las respuestas son absolutamente anónimas y confidenciales las mismas que serán respondidas desde su experiencia; y que serán empleados únicamente para fines de investigación.

A continuación, se procederá a dar inicio a la entrevista:

Declaro que acepto de manera voluntaria responder a las siguientes preguntas [A]

A continuación, se procederá a dar inicio a la entrevista:

PREGUNTAS

1. ¿Cuáles son los principales motivos por los que las fiscalías penales en Perú archivan denuncias por fraude informático?.

   Dificultad para identificar a los responsables debido a falta de tecnología avanzada

2. ¿Qué factores contribuyen a la falta de seguimiento de las denuncias por fraude informático en las fiscalías penales?.

Insuficiencia de recursos tecnologicos adecuados

3. ¿Cómo afecta la colaboración entre fiscalías y entidades bancarias en la resolución de casos de fraude informático?

Hay resistencia por parte de los bancos para compartir información.

4. ¿Qué responsabilidad tienen las entidades bancarias en la prevención y gestión de fraudes informáticos según su experiencia?.

Deberían tomar un papel mas activo en la Prevención de fraudes

5. ¿Qué cambios legislativos cree que serían necesarios para mejorar la efectividad en la persecución de delitos cibernéticos?

Incoporar tecnologías avanzados y mejorar la aplicación de la ley

6. ¿Cómo evalúa la Ley de Delitos Informáticos (Ley Nº 30096) en su capacidad para enfrentar el aumento de delitos cibernéticos?.

Tiene lagunas, importants que limitan su velocidad. o efectividad

7. ¿Qué dificultades enfrenta al investigar y procesar casos de fraude informático?.

Rápida evolución de los tecnicas de los delincuentes y Falta de capacitación

8. ¿Qué impacto tiene la falta de evidencia en el archivo de casos de fraude informático?.

Sin evidencias suficientes, es dificil Proceder con los casos