UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE CIENCIAS JURÍDICAS, CONTABLES Y SOCIALES

ESCUELA PROFESIONAL DE DERECHO

Tesis

Inclusión del delito de estafa mediante el uso de billeteras digitales en el Código Penal Peruano, Cusco 2024

Asesor:

Dra. Rodríguez Ayerbe, Kathie

Autora:

Machaca Chavez, Reyna Andrea

Para optar al Título Profesional de:

Abogado(a)

Cusco – Cusco – Perú

2025

UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE CIENCIAS JURIDICAS CONTABLES Y SOCIALES

ESCUELA PROFESIONAL DE DERECHO

Acta N°: 035-2025

ACTA DE SUSTENTACIÓN DE TÍTULO PROFESIONAL

En la ciudad de Cusco, a los 14 días del mes de agosto del 2025, siendo las 10:00 horas, se reunieron los integrantes del Jurado designado por Resolución Sub Directoral N° 440-2025-UTEA-FCJCS-EPD-FC de la Escuela Profesional de Derecho, Facultad de Ciencias Jurídicas Contables y Sociales:

Presidente	:	Mgt. Kadagand Venero, Liliana
Dictaminante	:	Mgt. Caceres Caceres, Angel
Replicante	:	Mgt. Zuniga Arredondo, Yuri Sandra

Para evaluar la sustentación, en la modalidad de:

☒ Tesis ☐ Trabajo de suficiencia profesional

Titulada:

Inclusión del delito de estafa mediante el uso de billeteras digitales en el Código Penal Peruano, Cusco 2024

Desarrollado por el (los) Bachiller (es):

Br.: Machaca Chavez, Reyna Andrea
(Apellidos y Nombres)

Br.: _____
(Apellidos y Nombres)

Para optar el Título Profesional de:

Abogado(a)
(Denominación del Título)

Concluido el acto, el Jurado dictaminó que el (la) (los) mencionado(a) (s) bachiller (es) fue (ron) APROBADO (S):

Por: Unanimidad
(Unanimidad o Mayoría) (*)

Emitiéndose el calificativo final de:

Bachiller (Apellidos y Nombres)	Calificación (**)
Br. Machaca Chavez, Reyna Andrea	Aprobado

Siendo las 11:30 horas concluyó la sesión, firmando los integrantes del Jurado.

Presidente: Mgt. Kadagand Venero, Liliana
(Dr. Mg.). (Apellidos y Nombres)
(Firma)

Dictaminante: Mgt. Caceres Caceres, Angel
(Dr. Mg.). (Apellidos y Nombres)
(Firma)

Replicante: Mgt. Zuniga Arredondo, Yuri Sandra
(Dr. Mg.). (Apellidos y Nombres)
(Firma)

(*): **Mayoría**: Dos integrantes del jurado aprueban o desaprueban; **Unanimidad**: Todos los integrantes del jurado aprueban o desaprueban, Art.18 RGGAT.
(**): 0 a 10: Desaprobado, 11 a 15: Aprobado, 16 a 18: Aprobado Notable, 19 y 20: Aprobado con Distinción, Art. 18 RGGAT.

6% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 15 palabras)

Fuentes principales

5% Fuentes de Internet
1% Publicaciones
5% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Metadatos

Datos del Autor		
Apellidos y nombres	:	Machaca Chavez Reyna Andrea
Tipo de Documento de Identidad	:	DNI
Numero de Documento de Identidad	:	48111491
URL ORCID	:	https://orcid.org/0009-0000-2928-3508
Datos del Asesor		
Apellidos y nombres	:	Dra. Rodríguez Ayerbe, Kathie
Tipo de Documento de Identidad	:	D.N.I.
Numero de Documento de Identidad	:	40032400
URL ORCID	:	https://orcid.org/0000-0003-4393-5415
Datos de la Investigación		
Facultad	:	Ciencias Jurídicas, Contables y Sociales.
Escuela Profesional	:	Derecho
Línea de Investigación	:	Derecho, Privado y Público
Rango de años en que se realizó la investigación	:	Enero 2024 a enero 2025
Fuente de financiamiento	:	Autofinanciamiento
Porcentaje de similitud	:	6%
URL OCDE	:	https://purl.org/pe-repo/ocde/ford#5.05.01

Dedicatoria

La presente tesis está dedicada a mis padres Milton Machaca Mamani y Antonia Chavez Quispe por su confianza, motivación, constante apoyo, quienes creyeron en los logros de su hija, muchas gracias por ayudarme alcanzar mis metas.

A mis hermanos quienes me apoyaron en diferentes etapas de mi vida.

A mi novio por su apoyo constate y amor incondicional que me brinda día a día para alcanzar mis metas profesionales y personales.

Finalmente, y no menos importante, agradezco mi perseverancia, esfuerzo por no rendirme y persistir día a día.

Agradecimientos

A gratitud a Dios por brindarme esperanza y darme la fortaleza de terminar mi carrera de manera satisfactoria.

A la Universidad Tecnológica de los Andes, del mismo modo a la Facultad de Ciencias Jurídicas Contables y Sociales, y a la Escuela Profesional de Derecho, en especial a sus docentes por impartirnos sus conocimientos para de mi formación académica.

A mi estimada asesora, Dra. Rodríguez Ayerbe, Kathie; por su tiempo, apoyo y guía durante el proceso de investigación.

También agradezco a los validadores y entrevistados, por haberme facilitado su tiempo para poder realizar el presente trabajo de investigación, sin su apoyo no hubiese sido posible la conclusión de esta investigación.

Resumen

Esta investigación tuvo como objetivo analizar la inclusión del delito de estafa mediante billeteras digitales en el Código Penal, con el fin de mejorar la eficacia del sistema jurídico penal en el tratamiento de los fraudes digitales. Se establecieron tres objetivos específicos: identificar las modalidades de estafa mediante billeteras digitales en Cusco, determinar las billeteras más utilizadas y vulnerables, y proponer un agravante en la legislación penal.

La metodología utilizada fue cualitativa, con entrevistas a abogados y fiscales especializados en delitos informáticos en Cusco, quienes proporcionaron información clave sobre las prácticas delictivas en el contexto digital.

Los resultados mostraron que las billeteras más utilizadas en las estafas fueron Yape y Plin, siendo las principales vulnerabilidades la falta de medidas de seguridad. La mayoría de los entrevistados coincidió en que la inclusión de un agravante específico en el Código Penal era necesaria para mejorar la sanción y disuasión de este tipo de delitos.

En conclusión, se evidenció que la legislación actual no estaba suficientemente adaptada a las nuevas formas de criminalidad digital. Se recomendó a los legisladores y entidades bancarias mejorar las normativas y las medidas de seguridad en las billeteras digitales.

Palabras clave: estafa digital, billeteras electrónicas, legislación penal, ciberseguridad, fraude electrónico.

Abstract

This research aimed to analyze the inclusion of the crime of fraud through digital wallets in the Penal Code, in order to improve the effectiveness of the criminal legal system in dealing with digital fraud. Three specific objectives were established: to identify the modalities of fraud through digital wallets in Cusco, to determine the most used and vulnerable wallets, and to propose an aggravating factor in the criminal legislation.

The methodology used was qualitative, with interviews with lawyers and prosecutors specialized in computer crimes in Cusco, who provided key information on criminal practices in the digital context.

The results showed that the wallets most used in scams were Yape and Plin, with the main vulnerabilities being the lack of security measures. Most of the interviewees agreed that the inclusion of a specific aggravating factor in the Penal Code was necessary to improve the sanction and deterrence of this type of crime.

In conclusion, it was found that current legislation was not sufficiently adapted to new forms of digital crime. Legislators and banking institutions were advised to improve regulations and security measures for digital wallets.

Keywords: digital fraud, electronic wallets, criminal law, cybersecurity, electronic fraud.

Índice

Índice de tablas

Índice de anexos

I. Introducción

Este trabajo de investigación se desarrolló con el objetivo de analizar cómo la inclusión del delito de mediante billeteras digitales podría mejorar la eficacia del sistema jurídico penal en el contexto de Cusco. Dado el crecimiento de las tecnologías financieras y el uso de billeteras digitales como Yape y Plin , se identificó un aumento significativo de estafas a través de estos medios es así que la investigación se realizará en varios capítulos, cada uno abordando aspectos fundamentales para comprender y proponer soluciones a esta problemática.

El Capítulo I: introducción , establece el contexto del estudio, el propósito general de la investigación y los objetivos específicos que guiaron el trabajo describiendo las justificaciones de la investigación, en términos de su relevancia tanto jurídica como social.

En el Capítulo II: problema de investigación , se identificaron y formularon los problemas principales, con un análisis detallado de cómo las billeteras digitales han facilitado nuevas formas de fraude.

En el Capítulo III: marco teórico , se abordan los antecedentes y las bases teóricas relacionadas con el tema, incluyendo estudios previos y conceptos clave sobre el delito de estafa y su tratamiento en la legislación peruana.

El Capítulo IV: Metodología detalló el enfoque cualitativo utilizado, las entrevistas realizadas a abogados y fiscales especializados, y el tipo de muestra seleccionada para obtener datos relevantes.

Finalmente, el Capítulo V: resultados y discusión presentó los hallazgos obtenidos, discutiendo cómo los resultados se relacionan con los antecedentes previos y qué implicaciones tienen para la legislación y la práctica judicial en Cusco.

II. Problema de Investigación

2.1. Descripción y formulación del problema

En los antecedentes internacionales, estudios como el de Cornejo (2023) evidencio la importancia de la ciberseguridad y el papel de la policía en la investigación de delitos informáticos, a pesar de los avances en legislación, como la ley N° 21.459 en Chile, persisten deficiencias en la investigación y recolección de pruebas. Este planteamiento se alinea con las respuestas de los entrevistados en nuestra investigación, particularmente del Fiscal Quillahuaman , quien sugiere que un agravante específico podría mejorar las herramientas para combatir estos delitos. Sin embargo, Pallaso et al. (2022) y Ginger (2022) argumentaron que, en contextos como Ecuador, la falta de una legislación adecuada para regular los fraudes digitales genera grandes pérdidas económicas, especialmente a través de redes sociales y comercio electrónico resaltando la necesidad de actualizar la normativa legal para abordar el uso creciente de las billeteras digitales y otros medios en estos fraudes, lo cual también fue señalado por varios entrevistados como una clave de preocupación.

A pesar de que el Código Penal peruano sanciona el delito de estafa, la normativa vigente no contempla un agravante específico para las estafas cometidas mediante billeteras digitales. Esta laguna legal limita la capacidad del sistema judicial para imponer sanciones más severas y adecuadas a la gravedad de estos delitos, dejando a los usuarios desprotegidos frente a una forma de criminalidad que ha evolucionado rápidamente con el avance de la tecnología.

La necesidad de un agravante específico es evidente, ya que estas estafas no solo causan un daño económico considerable, sino que también explotan las debilidades estructurales de la normativa actual. La falta de mecanismos de rastreo efectivos y la complejidad de investigar delitos cometidos a través de plataformas digitales agravan la situación, haciendo que las autoridades locales en Cusco enfrenten grandes desafíos en la persecución y sanción de los responsables.

La pandemia de COVID-19 exacerbó esta problemática al acelerar la adopción de estas tecnologías, con más personas recurriendo a las billeteras digitales para sus transacciones diarias. Este incremento en el uso ha sido paralelo a un aumento en los casos reportados de estafas, aunque se presume que muchos más no son denunciados por diversas razones, incluyendo la desconfianza en las autoridades y el desconocimiento sobre cómo proceder.

En la provincia de Cusco, el uso de billeteras digitales como yape, plin, ágora, bim, izipayYA (antes llamado tunki) se han consolidado como una herramienta esencial para realizar transacciones económicas rápidas y accesibles. Estas aplicaciones han facilitado significativamente el intercambio de dinero entre los usuarios, eliminando barreras geográficas y simplificando procesos financieros que antes requerían más tiempo y esfuerzo. Sin embargo, junto con estas ventajas ha emergido una nueva problemática: el uso indebido de estas plataformas por parte de delincuentes para llevar a cabo estafas.

Las estafas a través de billeteras digitales se han convertido en una preocupación creciente en Cusco, donde los estafadores aprovechan la velocidad y el anonimato que ofrecen estas aplicaciones para engañar a las víctimas. El modus operandi común incluye la solicitud de transferencias bajo falsos pretextos, como la venta de productos inexistentes,

ofertas de empleo fraudulentas, y esquemas de inversión ficticios. Una vez realizada la transacción, las víctimas se enfrentan a la dificultad, si no imposibilidad, de recuperar su dinero, dado que las transacciones en estas plataformas suelen ser irreversibles.

En este contexto, resulta importante analizar la inclusión de un agravante en el delito de estafa cuando se comete mediante billeteras digitales. Este cambio en la legislación permitiría una sanción más justa y efectiva, adaptando la ley a las realidades tecnológicas actuales y fortaleciendo la protección de los usuarios en un entorno digital cada vez más vulnerable.

2.1.1. Interrogante general

¿De qué manera la inclusión del delito de estafa mediante billeteras digitales puede mejorar la eficacia del sistema jurídico penal?

2.1.2. Interrogantes especificas

¿Cuáles son las modalidades de estafa más comunes mediante billeteras digitales en Cusco?

¿Cuáles son las billeteras digitales más utilizadas en los delitos de estafa y qué características las hacen más vulnerables?

¿Qué impacto tendría la inclusión de un agravante en el delito de estafa sobre la disuasión y sanción de delitos de estafa?

2.2. Objetivos

2.2.1. Objetivo general

Analizar cómo la inclusión del delito de estafa mediante billeteras digitales podría mejorar la eficacia del sistema jurídico penal.

2.2.2. Objetivos específicos

Identificar las modalidades de estafa mediante billeteras digitales en Cusco.

Determinar cuáles son las billeteras digitales más utilizadas en los delitos de estafa y características que las hacen más vulnerables.

Proponer la inclusión de un agravante en la legislación penal para fortalecer la disuasión y sanción.

2.3. Justificación e importancia

2.3.1. Justificación jurídica

Desde una perspectiva jurídica, es fundamental analizar cómo las normativas vigentes abordan estos delitos cometidos a través de billeteras digitales y si estas normativas son realmente efectivas para sancionar a los responsables. Además, es fundamental que las leyes no solo sancionen adecuadamente estos delitos, sino que también incluyan agravantes específicos para los casos que involucran el uso de billeteras digitales, dado el impacto considerable que estas estafas tienen en las víctimas.

2.3.2. Justificación social

Socialmente, las estafas mediante billeteras digitales generan un impacto profundo en las comunidades, afectando no solo el bienestar económico de las víctimas, sino también su confianza en las transacciones digitales y en las instituciones encargadas de su protección. A medida que estas plataformas se integran cada vez más en la vida cotidiana, es esencial comprender cuáles son las más vulnerables y cómo estas estafas afectan a las víctimas. Identificar las billeteras digitales más comunes en estos delitos permitirá desarrollar estrategias de prevención más efectivas y específicas, que no solo protejan a los usuarios, sino que también fortalezcan la confianza en el ecosistema digital.

2.3.3. Justificación ética

Éticamente, esta investigación se justifica en la imperiosa necesidad de proteger a los ciudadanos de prácticas fraudulentas que vulneran su seguridad y bienestar. Garantizar un entorno digital seguro es una responsabilidad compartida entre el Estado, las plataformas tecnológicas y los usuarios. A través de esta investigación, se pretende identificar las debilidades actuales en la prevención y sanción de estafas digitales, proponiendo mejoras que contribuyan a un sistema de justicia más eficaz y equitativo.

2.3.2. Justificación practica

Científicamente, este estudio aporta al conocimiento sobre el fenómeno de las estafas digitales, proporcionando datos empíricos y análisis detallados que pueden servir como base para futuras investigaciones.

2.5. Categorías

Las categorías de análisis en esta investigación incluyen:

Como primera categoría el delito de estafa que contiene como sub categorías a a justificación legal del agravante, impacto en la legislación penal y mecanismos de denuncia y sanción.

Como segunda categoría a billeteras digitales que tiene como sub categorías a modalidades de estafas digital, tecnologías y métodos empleados e impacto en las victimas.

III. Marco teórico

3.1Antecedentes

3.1.1. Antecedentes Internacionales

Se tiene la investigacion de Cornejo (2023) en su estudio titulado “La investigación de delitos informáticos y su prueba en materia penal”, elaborado en la Universidad de Chile, en la Facultad de Derecho – Departamento de Ciencias Penales, como memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. El objetivo principal de este trabajo fue analizar el papel de la policía en la investigación de los delitos informáticos y la manera en que se valoran las pruebas dentro del proceso penal, especialmente considerando el incremento de estos delitos durante y después de la pandemia del SARS-CoV-2. La metodología utilizada fue de carácter cualitativo y jurídico–dogmático, con un enfoque en el análisis legislativo y jurisprudencial; se revisaron las normas chilenas, partiendo desde la ley N° 19.223 hasta la más reciente ley N° 21.459, que regula la ciberseguridad y actualiza la persecución de los delitos informáticos. Los resultados mostraron que, a pesar de los avances normativos, aún existen deficiencias importantes en la investigación y en la recolección de pruebas, lo que afecta la eficacia del proceso penal. En sus conclusiones, el autor señaló que la normativa chilena ha tenido avances significativos, pero todavía enfrenta limitaciones prácticas que exigen reformas para equilibrar la persecución penal con la protección de garantías constitucionales, destacando la necesidad de fortalecer las capacidades investigativas y la correcta aplicación de las leyes en materia digital.

Así mismo, Pallaso et al. (2022) titulada “Delitos de estafa a través de redes sociales en época de pandemia”, presentada en la Universidad Regional Autónoma de los Andes (UNIANDES) como requisito para optar el grado de Magíster en Derecho con mención en Derecho Penal y Criminología. El estudio tuvo como objetivo identificar las causas del incremento de estafas en la provincia de Tungurahua durante el confinamiento por la pandemia. La metodología utilizada fue de carácter cuantitativo y cualitativo, apoyada en denuncias realizadas a través de redes sociales y en la valoración de fiscales de la zona. Los resultados indicaron que las principales causas del aumento de estafas estuvieron relacionadas con el libre acceso a las redes sociales, la dificultad para identificar a los responsables y la creación de perfiles falsos, lo que facilitó la comisión de estos delitos. La investigación concluyó que el contexto de la pandemia agudizó estas debilidades, demostrando la necesidad de fortalecer los mecanismos de control y prevención frente a la vulnerabilidad de los usuarios en medios digitales.

En esa misma línea, Ginger (2022) titulada “Incidencia del delito de estafa a través del uso de redes sociales, año 2017-2020, cantón La Libertad”, presentada en la Universidad Estatal Península de Santa Elena para optar el título de abogada. El estudio tuvo como objetivo analizar la recurrencia de los delitos de estafa cometidos mediante redes sociales, tomando como referencia el artículo 186 del Código Orgánico Integral Penal. Para ello se empleó una metodología cualitativa con fundamentación jurídica, utilizando entrevistas a jueces, abogados y ciudadanos, además de la revisión normativa. Los resultados evidenciaron que el comercio electrónico impulsó un incremento notable en las estafas, generando importantes pérdidas patrimoniales, situación que se intensificó con la pandemia del COVID-19. Finalmente, la investigación concluyó que la hipótesis de que la pandemia fomentó el aumento de estafas se cumplió parcialmente y que la normativa penal debía ser

reformada para incluir de manera más amplia los medios digitales, con el fin de garantizar sanciones proporcionales al daño ocasionado.

Por su parte, Gomezjurado (2022) presentó en la Universidad Internacional del Ecuador (UIDE) su propuesta de investigación titulada “Identificación del sujeto activo en el delito de estafa a través de medios digitales y electrónicos bajo la perspectiva del COIP en el Ecuador” como requisito para optar el título de abogado de los tribunales y juzgados del Ecuador. El objetivo central de este trabajo fue determinar si el sistema normativo ecuatoriano, en particular el Código Orgánico Integral Penal (COIP), se encontraba preparado para abordar las estafas cometidas mediante medios electrónicos. La metodología empleada fue de carácter cualitativo y dogmático, con un análisis de casos y recolección documental. Los resultados mostraron que la identificación de los responsables resulta especialmente compleja debido a la naturaleza digital de los delitos; además, se evidenció que, pese al elevado número de estafas electrónicas y su creciente amenaza, la normativa ecuatoriana carece de solidez suficiente para garantizar una protección efectiva a los ciudadanos. En sus conclusiones, el autor afirmó que la evolución digital ha sobrepasado la capacidad de respuesta del sistema penal, por lo que es necesario fortalecer la legislación con normas más precisas y establecer protocolos de investigación eficaces que permitan sancionar adecuadamente a los responsables y resarcir a las víctimas.

Finalmente Paguay (2020) titulada “Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet”, realizada en la Universidad Nacional de Chimborazo para la obtención del grado de abogada de los tribunales y juzgados del Ecuador. El objetivo principal de este trabajo fue identificar las perspectivas regulatorias de los delitos informáticos en el comercio electrónico, considerando el avance de la tecnología y el desarrollo de la informática como factores que han propiciado un incremento de conductas ilícitas como la estafa electrónica, la apropiación ilícita y los daños informáticos,

todos sancionados en el Código Orgánico Integral Penal. La metodología empleada fue cualitativa de tipo analítico-sintético, basada en la revisión normativa y el análisis de casos prácticos que evidenciaban la vulneración de derechos en el ámbito digital. Los resultados señalaron que, a pesar de que el COIP contempla ciertos delitos de carácter informático, persisten vacíos importantes en la regulación, en especial respecto a los compradores que actúan con ánimo de defraudar. La conclusión principal fue que la normativa requiere ser fortalecida para garantizar la protección adecuada de los consumidores y asegurar la vigencia efectiva de sus derechos constitucionales en entornos digitales.

3.1.2. Antecedentes nacionales

Ramirez y Azabach (2024) titulada “Influencia de las redes sociales en los delitos de estafa informática y las consecuencias jurídicas Huaura - 2023” presentada en la Universidad Nacional José Faustino Sánchez Carrión para optar el título profesional de abogada. El estudio tuvo como propósito determinar el grado de influencia de las redes sociales en los delitos de estafa informática y las repercusiones legales en la provincia de Huaura. La metodología empleada fue mixta con predominancia de cualitativa, aplicando un cuestionario a una muestra de 85 abogados. Los resultados confirmaron que las redes sociales influyen directamente en la comisión de estafas informáticas. La investigación concluyó que el uso masivo y desregulado de redes sociales constituye un factor de riesgo relevante en la propagación de estos delitos, lo cual genera consecuencias jurídicas importantes que deben ser atendidas en la práctica penal.

Así mimo, Ramos (2022) presentó en la Universidad Norbert Wiener la investigación titulada “Impacto de los delitos informáticos en las investigaciones preparatorias de las fiscalías provinciales penales corporativas distrito fiscal Lima Sur 2022” como requisito para optar el título de abogada. El objetivo de este trabajo fue analizar cómo los delitos

informáticos incidían en el desarrollo de las investigaciones preliminares. Bajo un enfoque cualitativo de tipo hermenéutico y fenomenológico, se aplicó como técnica principal el análisis documental. Los resultados mostraron que la identificación de los autores y la conservación de las pruebas resultaban determinantes para el éxito de las investigaciones; sin embargo, ante la ausencia de indicios suficientes, los fiscales optaban por archivar los casos. La conclusión más relevante señaló que los operadores de justicia se encontraban en desventaja debido a la falta de herramientas adecuadas para llevar a cabo investigaciones eficaces en esta clase de delitos.

Consecuentemente, Carbajal (2022) en su tesis titulada "Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el cibercrimen" presentada en la Universidad de San Martín de Porres para obtener el grado de Magíster, examinó cómo la revolución digital, si bien ha favorecido la comunicación y el desarrollo profesional, también ha incrementado la ciberdelincuencia debilitando la capacidad del Estado para proteger a los ciudadanos. El estudio planteó como objetivo analizar la eficacia de la creación de fiscalías especializadas frente a desafíos como el anonimato de los delincuentes y la escasez de peritos capacitados. Bajo un enfoque cualitativo y sustentado en datos de la División de Investigación de Alta Tecnología y entrevistas a fiscales, se determinó que los fraudes informáticos, en particular la clonación de tarjetas y las compras fraudulentas, representan las modalidades más frecuentes. Finalmente, se concluyó que, pese a los avances legislativos, la Ley 30096 mantiene vacíos en la tipificación de estos delitos, lo cual dificulta la aplicación efectiva de sanciones y limita la capacidad de respuesta judicial..

Por su parte, Cruz (2021) desarrolló la investigación titulada "Propuestas para neutralizar la alta incidencia del delito de estafa en sus diversas modalidades", presentada en la Pontificia Universidad Católica del Perú para optar el grado académico de Magíster en Gobierno y Políticas Públicas. El estudio tuvo como finalidad analizar los casos de estafa y

otras defraudaciones investigados por la DIVIEOD-DIRINCRI PNP en Lima Metropolitana. Se empleó una metodología cualitativa basada en entrevistas a fiscales y gerentes de prevención de fraudes, además de la revisión de estadísticas oficiales del INEI y la PNP. Los resultados evidenciaron que la falta de normatividad sobre el secreto bancario representaba un obstáculo para la acción policial; en efecto, el 61% de los fiscales consultados señalaron la ausencia de un marco legal que obligue a las entidades financieras a brindar información en casos de flagrancia. Asimismo, se identificó un incremento significativo de las estafas virtuales, que alcanzaron el 82% de los casos, destacando el uso de redes sociales como Facebook e Instagram para engañar a usuarios mediante ofertas falsas y perfiles que desaparecían tras recibir los pagos. El trabajo concluyó en la necesidad de fortalecer la normativa y los mecanismos de cooperación entre bancos y autoridades para enfrentar eficazmente este fenómeno delictivo.

El estudio aboradado por Beraún (2020) titulada “El delito de estafa por medios tecnológicos en tiempos de la COVID-19, Lima, 2020”, presentada en la Universidad César Vallejo para optar el título profesional de Abogado. El estudio tuvo como objetivo analizar el incremento de estafas realizadas mediante medios tecnológicos durante la pandemia; para ello se empleó una metodología cualitativa con diseño de teoría fundamentada, utilizando entrevistas y análisis documental para la recolección de información. Los resultados evidenciaron que modalidades como las compras en línea y la denominada maleta retenida aumentaron de manera considerable debido al uso intensivo de internet en el contexto del confinamiento; finalmente, se concluyó que este fenómeno planteó la necesidad de precisar si estos ilícitos debían clasificarse como fraudes informáticos o como estafas tecnológicas, resaltando los vacíos conceptuales y jurídicos existentes en su tratamiento.

3.1.3. Antecedentes locales

Al realizar una revisión exhaustiva de repositorios y plataformas de publicación de tesis en universidades locales, no se encontraron estudios que traten específicamente la inclusión de un agravante en el delito de estafa mediante billeteras digitales en el contexto de la provincia de Cusco.

La inexistencia de investigaciones previas no solo evidencia un vacío en la literatura académica, sino que también subraya la necesidad de desarrollar un marco legal más robusto y adaptado a las nuevas realidades tecnológicas que enfrentan los ciudadanos en Cusco.

3.2. Bases teóricas

3.2.1. Delito de estafa

Carrasco (2024) enfatiza que el delito de estafa es un acto ilícito en el que una persona, mediante engaños o artimañas, logra que otra le entregue bienes, dinero u otros valores, causando así un perjuicio patrimonial a la víctima.

El Código Penal Peruano (2004), define la estafa como la acción de inducir a error a otra persona mediante engaños, para que esta realice un acto que le cause un perjuicio patrimonial.

Por su parte, Mayer (2014) Considera la estafa como una de las formas más comunes de fraude, donde el engaño es el medio principal para lograr que la víctima disponga de sus bienes de manera perjudicial. Así mismo, Cisnero y Jiménez (2021) describe la estafa como un delito de resultado, en el cual el perjuicio económico debe ser real y efectivo, y no meramente potencial.

3.2.1.1. Antecedentes histórico-conceptuales:

El delito de estafa tiene una historia jurídica que se remonta a la antigüedad, reflejando la evolución de las normas para proteger el patrimonio de las personas frente a conductas fraudulentas. En la antigua Roma, como menciono Recalde (2024) se reconocía el dolus malus, un concepto que englobaba acciones fraudulentas realizadas con la intención de inducir al error a otra persona para obtener un beneficio indebido.

Es así que durante la edad media, las leyes se centraban en castigar las ofensas contra la propiedad, aunque no existía una diferenciación clara entre el fraude y otros delitos patrimoniales, como el hurto. Textos legales como Las Siete Partidas de Alfonso (Biblioteca Juridica Digital España, 2021) establecieron precedentes al sancionar conductas que involucraban engaño para obtener bienes ajenos. Sin embargo, fue en el periodo de los códigos penales modernos del siglo XIX cuando la estafa adquirió autonomía jurídica. Influenciado por el Código Penal Francés, se definió específicamente como el uso de ardides o engaños para inducir a error a las víctimas y causarles un perjuicio patrimonial.

En américa latina, este modelo fue adoptado por los primeros códigos penales de la región, incluido el peruano, que incorporó la estafa como un delito autónomo. Con el tiempo, las normativas han evolucionado para incluir modalidades más complejas, adaptándose a los cambios tecnológicos y sociales. En la actualidad, la estafa digital plantea nuevos retos legales, como las billeteras digitales.

3.2.1.2. Elementos del delito de estafa:

En merito a la Casación N° 461-2016 se considera los siguientes elementos (Corte Suprema de Jusiticia de la Republica, 2016)

- Engaño: Consiste en la creación o aprovechamiento de un error en la víctima, que lleva a esta a realizar un acto perjudicial para su patrimonio.
- Error: La víctima debe estar bajo un error inducido por el autor, creyendo que está actuando en su propio beneficio o sin perjuicio.
- Disposición Patrimonial: Es el acto mediante el cual la víctima transfiere bienes, derechos u obligaciones, inducida por el engaño.
- Perjuicio: Debe existir un daño económico real en el patrimonio de la víctima.

3.2.1.3. Tipicidad del delito de estafa:

El Artículo 196 del Código Penal peruano (2004) establece que la persona que, con ánimo de lucro, mediante engaños o ardid, induce a otro a realizar un acto en perjuicio de su patrimonio o de un tercero, será sancionada con pena privativa de libertad no menor de uno ni mayor de seis años. Si el perjuicio es grave o se utiliza un medio tecnológico para cometer el delito, las penas pueden incrementarse.

La jurisprudencia peruana ha abordado múltiples casos de estafa, destacando la importancia del dolo (intención) y del uso de medios tecnológicos, como las redes sociales, que han incrementado la incidencia de este delito. La evolución de las modalidades de estafa, especialmente en un contexto digital, ha exigido una actualización constante de las normativas y un mayor rigor en la aplicación de la ley para proteger a las víctimas y sancionar a los infractores.

En el contexto peruano, el delito de estafa se caracteriza por una variedad de modalidades que los delincuentes utilizan para engañar a sus víctimas y obtener un beneficio patrimonial indebido. Según Ruiz (2021), un abogado especializado en derecho penal, las modalidades de estafa en Perú están detalladamente descritas en el Código Penal, específicamente en el artículo 196 y su forma agravada en el artículo 196-A. Estas

modalidades incluyen desde el uso de ardides y engaños hasta el aprovechamiento de tecnologías modernas para inducir a error a las víctimas.

Si bien el Código Penal peruano tipifica el delito de estafa, incluyendo un agravante para aquellos casos en los que se utilizan medios tecnológicos, es evidente que la legislación actual podría ser más efectiva si se estableciera una tipificación específica y objetiva para las estafas realizadas mediante billeteras digitales. Estas plataformas, como Yape, Plin, y otras, presentan características particulares que las hacen vulnerables a fraudes que resultan en la pérdida inmediata y a menudo irreparable de dinero. La dificultad de rastrear a los estafadores en estos casos, debido a la rapidez y anonimato con que operan, subraya la necesidad de una regulación más precisa que permita no solo sancionar de manera más severa, sino también prevenir de forma más eficaz este tipo de delitos.

3.2.1.4. Modalidades de estafa:

En merito a la diferenciación realizado por Rodríguez (2020) se tiene las siguientes modalidades de estafa

- Estafa clásica o tradicional: Esta modalidad implica el uso de engaños directos, como hacer creer a la víctima en la existencia de bienes, solvencia o capacidad económica que en realidad no existen. Es común que el estafador utilice documentos falsos o simule ser una persona distinta para ganarse la confianza de la víctima y así inducirla a realizar una disposición patrimonial perjudicial.
- Estafa informática: con el avance de la tecnología, las estafas a través de medios electrónicos se han vuelto cada vez más comunes. Esta modalidad incluye la clonación de tarjetas de crédito, compras fraudulentas en línea, transferencias no

autorizadas y el phishing, donde el estafador se hace pasar por una entidad legítima para obtener información confidencial de la víctima.

- Estafa contractual: En este tipo de estafa, el delincuente induce a la víctima a firmar un contrato bajo condiciones fraudulentas. Es típico en el ámbito de compraventa de bienes inmuebles o vehículos, donde se ofrecen propiedades inexistentes o se alteran las condiciones del contrato para que favorezcan al estafador.

3.2.1.5. Impacto:

El impacto de las estafas en las víctimas en Perú es significativo y se manifiesta en múltiples dimensiones, tanto económicas como psicológicas. Según diversos estudios y encuestas tal como el estudio realizado por Vigo (2020) infiere que las víctimas de estafas enfrentan no solo pérdidas financieras considerables, sino también una afectación en su confianza hacia las instituciones financieras y en el uso de tecnologías para transacciones. Según el Diario Peruano (2024) menciono que las denuncias de fraude informático van en constante crecimiento y mostró que un alto porcentaje de peruanos se siente insatisfecho con la respuesta de sus bancos tras ser víctimas de estafas, lo que los lleva a considerar cambiar de institución financiera si no reciben un reembolso adecuado.

El daño psicológico también es considerable, ya que muchas víctimas experimentan estrés, ansiedad y desconfianza, no solo hacia las plataformas que utilizaron, sino también hacia cualquier interacción digital futura.

3.2.1.6. Mecanismos de denuncia y sanción:

Los mecanismos de denuncia y sanción para los delitos de estafa en Perú están estructurados dentro del marco legal del Código Penal y las normativas procesales que guían el accionar de las autoridades. Sin embargo, la efectividad de estos mecanismos

enfrenta desafíos significativos, desde la falta de recursos hasta las dificultades inherentes a la identificación de los responsables.

En nuestro país, las víctimas de estafa pueden iniciar el proceso de denuncia acudiendo a una comisaría de la Policía Nacional del Perú (PNP), donde se recoge su declaración y se inicia una investigación preliminar. Alternativamente, las denuncias pueden presentarse directamente ante el Ministerio Público, que es el órgano encargado de dirigir la investigación penal como bien se mencionó anteriormente el artículo 196 del Código Penal, infiere que la estafa es un delito que se persigue de oficio, lo que significa que, una vez presentada la denuncia, las autoridades están obligadas a investigar el caso independientemente de la voluntad de la víctima.

El proceso de denuncia es esencial, ya que permite a las autoridades recopilar pruebas y testimonios que sustenten la acusación. No obstante, este proceso enfrenta limitaciones importantes, como la falta de denuncias formales debido al temor de las víctimas o la creencia de que las autoridades no tomarán medidas efectivas. Además, la complejidad de las estafas, especialmente aquellas que involucran medios tecnológicos, puede dificultar la identificación de los perpetradores, ya que estos suelen operar bajo un velo de anonimato y utilizando técnicas sofisticadas para evadir la detección.

3.2.1.7. Propuesta de incorporación de un agravante específico para estafas mediante billeteras digitales:

Se sugiere la adición del Artículo 196-A al Código Penal peruano bajo el siguiente supuesto:

“Artículo 196-A:

La persona que, con ánimo de lucro, mediante engaños, ardid o fraude, induzca a otro a realizar un acto en perjuicio de su patrimonio o del de un tercero, …

….7. Se empleen aplicaciones fraudulentas que simulen ser billeteras digitales oficiales, generando comprobantes de pago falsos o que aparenten realizar transacciones que no tienen respaldo financiero”

3.2.1.8. Teorías relacionadas con delito de estafa:

a. Teoría del engaño

Una teoría relevante en el ámbito del delito de estafa es la Teoría del Engaño mencionado por Lajo (2007) centrada en el elemento del engaño como el componente central que define y tipifica el delito de estafa. Según esta teoría, desarrollada en la doctrina penal, el engaño no solo implica una falsedad o mentira, sino que debe ser lo suficientemente convincente y creíble para inducir a la víctima a realizar una disposición patrimonial en perjuicio propio o de un tercero. En el contexto peruano, esta teoría es fundamental para la interpretación del Artículo 196 del Código Penal (2004), que tipifica la estafa como un delito contra el patrimonio, sancionando a quienes, mediante ardides o engaños, inducen a error a una persona con el fin de obtener un beneficio económico ilícito

b. Teoría de la asociación diferencial

Propuesta por Sutherland y analizada por Pontón (2020) , establece que el comportamiento delictivo no es innato, sino aprendido a través de la interacción social. Según esta teoría, las personas adquieren valores, actitudes, técnicas y motivos para el

comportamiento delictivo mediante su relación con otros individuos que ya participan en actividades ilícitas, este aprendizaje ocurre en un entorno donde las normas y conductas delictivas son aceptadas o justificadas, lo que facilita la adopción de estas prácticas. En el caso del delito de estafa, esta teoría es particularmente relevante, ya que explica cómo las redes criminales o los entornos sociales permisivos pueden influir en la adopción de estrategias fraudulentas. Las estafas, al ser delitos que requieren planificación y habilidades específicas, son un ejemplo claro de cómo estas conductas pueden ser transmitidas y normalizadas en ciertos contextos sociales. Este marco teórico permite comprender la importancia de desarticular redes delictivas y educar en valores contrarios al fraude para prevenir su propagación.

3.2.2. Billeteras digitales

También conocidas como monederos electrónicos, son plataformas o aplicaciones móviles que permiten a los usuarios almacenar, gestionar y transferir dinero de manera electrónica, eliminando la necesidad de llevar efectivo o usar tarjetas físicas. Estas herramientas tecnológicas han ganado popularidad en todo el mundo debido a su conveniencia, seguridad y capacidad para facilitar transacciones rápidas y sin complicaciones (Pagina oficial de gobierno, 2024).

Una de las características principales de las billeteras digitales es su capacidad para almacenar diversas formas de dinero electrónico, incluyendo saldos vinculados a cuentas bancarias, tarjetas de crédito o débito, e incluso criptomonedas en algunos casos. Los usuarios pueden acceder a sus fondos desde cualquier lugar con conexión a internet, lo que hace que las billeteras digitales sean altamente accesibles y funcionales.

La facilidad de uso es otra de las razones por las que las billeteras digitales se han vuelto tan populares. Estas plataformas suelen ofrecer interfaces intuitivas que permiten a

los usuarios realizar pagos, enviar dinero a otras personas, pagar servicios y hasta hacer compras en línea con solo unos pocos clics. En el Perú, aplicaciones como Yape, Plin, Tunki, Ágora y BIM son ejemplos prominentes de billeteras digitales que han transformado la manera en que las personas realizan transacciones cotidianas.

La seguridad es un aspecto crucial de las billeteras digitales. Estas plataformas utilizan tecnología avanzada, como la autenticación de dos factores (2FA) y la encriptación de datos, para proteger la información financiera de los usuarios. Además, algunas billeteras digitales han implementado características de seguridad adicionales, como la biometría (uso de huellas digitales o reconocimiento facial), para asegurar que solo el usuario autorizado pueda acceder a los fondos almacenados.

Además de facilitar las transacciones, las billeteras digitales están promoviendo la inclusión financiera, especialmente en regiones donde los servicios bancarios tradicionales son limitados. Estas plataformas permiten que personas que no tienen acceso a una cuenta bancaria puedan realizar y recibir pagos de manera sencilla y segura.

3.2.2.1. Antecedentes históricos de las billeteras digítales:

Su desarrollo histórico comenzó aproximadamente por los años 1990, cuando el comercio electrónico impulsó la necesidad de alternativas al efectivo y las tarjetas bancarias físicas. Plataformas como PayPal, fundada en 1998, marcaron un hito al permitir pagos en línea de manera segura y eficiente, sentando las bases para lo que posteriormente serían las billeteras digitales.

Con el avance de la tecnología móvil en los años 2000, estas herramientas evolucionaron significativamente como evidencia Garita (2013) aplicaciones como Google Wallet y Apple Pay integraron tecnologías como la comunicación de campo

cercano , lo que permitió a los usuarios realizar pagos de manera inalámbrica y segura a través de dispositivos móviles.

La situación en América Latina se fue dando progresivamente, las billeteras digitales comenzaron a ganar popularidad durante la última década, especialmente en países como Perú, donde plataformas como Yape, Plin y Tunki han sido adoptadas masivamente, permitiendo que personas sin acceso a servicios bancarios tradicionales puedan realizar transacciones digitales y especialmente durante la pandemia de COVID-19, el uso de billeteras digitales se incrementó exponencialmente debido a la necesidad de realizar pagos sin contacto físico.

Como se evidencia tiene una corta historia, pero a pesar de ello las billeteras digitales han transformado profundamente los hábitos financieros de las personas y las dinámicas del comercio consecuentemente también ha generado desafíos relacionados con la seguridad y el fraude, lo que hace necesario de una regulación específica que garantice su utilización segura y eficaz.

3.2.2.2. Yape :

Yape es una billetera digital desarrollada por el Banco de Crédito del Perú (BCP) que permite a los usuarios realizar transacciones financieras de manera rápida y segura a través de un teléfono móvil. Desde su lanzamiento en 2016, Yape se ha convertido en una de las aplicaciones de pago móvil más utilizadas en Perú, destacándose por su facilidad de uso y por su capacidad de facilitar transacciones sin necesidad de efectivo o tarjetas físicas.

Una de las principales características de Yape es su interoperabilidad. Inicialmente, la aplicación estaba dirigida a clientes del BCP, pero con el tiempo, se ha expandido para incluir a usuarios de otros bancos e incluso a personas que no tienen cuentas bancarias.

Esta expansión ha sido posible gracias a la funcionalidad que permite vincular la aplicación con un número de celular, de modo que las transferencias de dinero se realicen de manera rápida y directa entre usuarios de Yape, sin necesidad de conocer números de cuenta.

La facilidad de uso es otro aspecto clave que ha impulsado la popularidad de Yape. Los usuarios solo necesitan registrar su número de celular y asociarlo con una cuenta bancaria o una tarjeta de débito. Una vez configurada la cuenta, la aplicación permite realizar pagos y transferencias en tiempo real con solo ingresar el número de teléfono del destinatario, lo que simplifica enormemente las transacciones cotidianas.

Además de permitir transferencias de dinero, Yape ofrece funcionalidades adicionales que la convierten en una herramienta versátil para la gestión financiera diaria. Los usuarios pueden realizar pagos en comercios afiliados, recargar el saldo de teléfonos móviles, y pagar servicios básicos como agua y electricidad, todo desde la misma aplicación.

Desde su lanzamiento, Yape ha experimentado un crecimiento significativo en su base de usuarios, impulsado por su simplicidad y por la confianza que los peruanos han depositado en los pagos digitales. La aplicación ha jugado un papel importante en la promoción de la inclusión financiera en Perú, permitiendo que personas no bancarizadas accedan a servicios de pago digital. Durante la pandemia de COVID-19, Yape se convirtió en una herramienta esencial para evitar el uso de efectivo y facilitar el distanciamiento social a través de pagos electrónicos.

3.2.2.3. Plin:

Desarrollada inicialmente por el BBVA en conjunto con otras entidades bancarias, Plin ha logrado consolidarse como una herramienta clave en el ecosistema de pagos digitales del país, compitiendo directamente con aplicaciones como Yape.

Una de las características más destacadas de Plin es su interoperabilidad entre diferentes bancos. Esto significa que, a diferencia de algunas aplicaciones que limitan las transacciones a usuarios del mismo banco, Plin permite que las transferencias se realicen sin importar si los usuarios pertenecen a entidades bancarias diferentes.

La simplicidad en el uso es otro factor que ha contribuido al éxito de Plin. Al igual que otras billeteras digitales, los usuarios de Plin solo necesitan asociar su número de celular a la aplicación y vincularla a su cuenta bancaria. A partir de ahí, pueden realizar pagos y enviar dinero simplemente seleccionando el número de teléfono del destinatario, sin necesidad de ingresar complejos datos financieros. Este proceso simplificado no solo ahorra tiempo, sino que también reduce las barreras para aquellos usuarios menos familiarizados con la tecnología.

3.2.2.4. Ágora:

Es una billetera digital que ha ido ganando popularidad en Perú debido a su enfoque en la simplicidad y seguridad en las transacciones electrónicas. Diseñada para facilitar pagos y transferencias, Ágora permite a los usuarios vincular sus cuentas bancarias o tarjetas de débito para realizar transacciones de manera rápida y segura a través de sus dispositivos móviles. Una de las características distintivas de Ágora es su interfaz amigable, que está diseñada para que incluso los usuarios menos familiarizados con la tecnología puedan realizar pagos y transferencias sin complicaciones.

3.2.2.5. BIM (Billetera Móvil):

Es otra importante plataforma en el panorama de pagos digitales en Perú, especialmente conocida por su enfoque en la inclusión financiera. Lanzada con el respaldo de la Asociación de Bancos del Perú (ASBANC), BIM fue creada con el objetivo de facilitar el acceso a servicios financieros para personas no bancarizadas, especialmente en áreas rurales donde los bancos tradicionales tienen poca presencia. BIM permite a los usuarios realizar pagos, transferencias y recargas de manera sencilla desde sus teléfonos móviles, sin la necesidad de tener una cuenta bancaria tradicional. La plataforma ha sido fundamental para acercar los servicios financieros a segmentos de la población que anteriormente estaban excluidos, contribuyendo significativamente a la reducción de la brecha de inclusión financiera en el país.

3.2.2.6. IzipayYA:

Anteriormente conocido como Tunki es una billetera digital que se ha destacado en el mercado peruano por su capacidad de integrar múltiples servicios financieros en una sola aplicación. Desarrollada por el Interbank, Tunki fue renombrada a IzipayYA en un esfuerzo por expandir su alcance y funcionalidades. La aplicación permite a los usuarios realizar una amplia gama de operaciones, incluyendo transferencias de dinero, pagos en comercios, y recargas de servicios, todo desde la comodidad de su dispositivo móvil. IzipayYA se diferencia por su enfoque en la simplicidad y accesibilidad, ofreciendo una experiencia de usuario optimizada que facilita la adopción incluso para personas menos familiarizadas con la tecnología.

3.2.2.7. Tecnología y métodos :

En el reciente estudio de Acosta (2022) destaca que los estafadores emplean una variedad de tecnologías y métodos sofisticados para engañar a las víctimas y obtener sus

datos personales o financieros las técnicas más comunes utilizadas en Perú, se destacan las siguientes:

- Phishing: Es una de las tácticas más empleadas, donde los delincuentes envían correos electrónicos, mensajes de texto, o incluso hacen llamadas que parecen provenir de entidades confiables, como bancos o empresas reconocidas, solicitando información confidencial. Esta técnica se diversifica en modalidades como el smishing (vía SMS), vishing (vía llamadas telefónicas), y el phishing tradicional por correo electrónico.
- Carding: Consiste en el uso ilegal de tarjetas de crédito o débito obtenidas fraudulentamente, a menudo mediante el hackeo de bases de datos o el uso de formularios en sitios web falsos que capturan la información de las tarjetas, utilizan esta información para realizar compras sin el consentimiento de la víctima.
- Cuentas Falsas: Los delincuentes crean perfiles o páginas falsas con el fin de ganarse la confianza de las víctimas y obtener sus datos personales o financieros.
- Pharming: Conocido como phishing sin señuelo, es una técnica más avanzada donde los delincuentes manipulan el tráfico web para redirigir a los usuarios a sitios fraudulentos sin que estos lo sepan.
- SIM Swapping: Esta modalidad implica que los estafadores suplantan la identidad de la víctima para conseguir el control de su tarjeta SIM, lo que les permite acceder a su banca digital y realizar transacciones ilegales.

3.2.2.8. Teoría relacionada a billeteras digitales:

a. Teoría de la Aceptación

En relación con las billeteras digitales, una teoría aplicable es la Teoría de la Aceptación de la Tecnología de Berger y Luckman (2010), adaptada al contexto digital

es particularmente relevante para la investigación sobre el uso de billeteras digitales, como Yape, Plin, y otras, porque estas tecnologías se adoptan masivamente debido a su utilidad percibida (facilidad y rapidez en las transacciones) y facilidad de uso (interfaces intuitivas y accesibles).

Esta teoría se basa en dos categorías principales: la utilidad percibida y la facilidad de uso percibida.

- Utilidad percibida: Este concepto refiere al grado en que una persona cree que una tecnología mejorará su desempeño o hará más eficiente una actividad específica. En el caso de las billeteras digitales, los usuarios consideran que estas herramientas simplifican las transacciones financieras y ahorran tiempo, lo que incentiva su uso.
- Facilidad de uso percibida: Hace referencia a la percepción del esfuerzo necesario para utilizar una tecnología. Si un sistema es considerado intuitivo y fácil de manejar, las personas estarán más dispuestas a adoptarlo. Las interfaces simples y amigables de aplicaciones como Yape, Plin y BIM ejemplifican este principio.

b. Teoría de la difusión de innovaciones

Realizado por Rogers y republicada por Urbizagástegui (2019) analiza cómo las nuevas tecnologías e ideas se adoptan dentro de una sociedad. Según la teoría, la adopción de una innovación depende de factores como la utilidad percibida, la compatibilidad con las necesidades del usuario, la simplicidad de uso, la capacidad de ser probada antes de adoptarse por completo y la observabilidad de sus beneficios. En el contexto de las billeteras digitales, esta teoría ayuda a explicar por qué herramientas como Yape, Plin y Tunki han tenido una adopción masiva en países como Perú, ya que estas plataformas se

perciben como prácticas, seguras y accesibles, lo que las convierte en soluciones atractivas para una amplia variedad de usuarios.

3.2.3. Regulación normativa vinculante

En Perú, la regulación de las estafas, incluyendo aquellas cometidas mediante medios tecnológicos, como se fue desarrollando está principalmente enmarcada en el Código Penal Peruano Artículo 196 que tipifica el delito de estafa y establece sanciones para quienes, mediante engaños o ardid, inducen a error a una persona para obtener un beneficio patrimonial ilícito.

Además del Código Penal, Perú ha adoptado varias normativas específicas para enfrentar la ciberdelincuencia. La Ley N° 30096 (2013), conocida como la Ley de Delitos Informáticos, para abordar de manera específica los delitos cometidos a través de medios tecnológicos. Esta ley define y sanciona actos como la suplantación de identidad digital, el acceso no autorizado a sistemas informáticos, y la manipulación de datos electrónicos, proporcionando un marco legal más adecuado para la persecución de estos delitos.

A nivel internacional, uno de los más importantes es la Convención de Budapest sobre Ciberdelincuencia, a la que Perú se adhirió en 2019 que es un referente en la lucha contra los delitos informáticos, estableciendo normas sobre la cooperación internacional en la investigación de estos delitos y la armonización de las legislaciones nacionales.

Asimismo, la legislación peruana se complementa con directrices y normativas emitidas por organismos internacionales, como la Unión Internacional de Telecomunicaciones (UIT), que proporciona recomendaciones para mejorar la seguridad cibernética y la protección de datos personales.

La legislación vigente, aunque imponente en teoría, no llega a ser especifica en cuanto a las técnicas nuevas de empleo de los estafadores así mismo enfrenta dificultades en la práctica debido a la falta de recursos y capacitación específica en el área de ciberseguridad.

3.3. Definición de términos

- La estafa electrónica es un delito en el cual el perpetrador utiliza medios tecnológicos, como internet o dispositivos digitales, para engañar a la víctima y obtener un beneficio económico de manera fraudulenta.
- Las medidas de seguridad informática son un conjunto de políticas, procedimientos y tecnologías implementadas para proteger los sistemas de información y los datos contra accesos no autorizados, ciberataques, y otros tipos de delitos informáticos.
- La ingeniería social, en el contexto de la seguridad informática, se refiere a las técnicas utilizadas por los delincuentes para manipular psicológicamente a las personas, induciéndolas a realizar acciones o divulgar información confidencial.
- Delito Informático; es cualquier actividad ilegal que involucra el uso de computadoras, redes o dispositivos digitales para cometer un acto delictivo. Estos delitos pueden incluir, pero no se limitan a, el hacking, la distribución de malware, el fraude en línea y el robo de identidad (Acurio, 2016).
- El phishing es una técnica de ingeniería social utilizada por los ciberdelincuentes para engañar a las personas y hacer que revelen información confidencial, como contraseñas, números de tarjetas de crédito o detalles bancarios. Generalmente, los atacantes se hacen pasar por instituciones legítimas enviando correos electrónicos o mensajes que parecen oficiales, dirigidos a la víctima con el objetivo de inducirla a hacer clic en enlaces maliciosos o proporcionar su información personal (Aredo, 2021).

IV. Metodología

4.1. Tipo y nivel de investigación

El estudio es de enfoque cualitativo de tipo básica y descriptivo-exploratorio. La elección de este tipo se debe a lo manifestado por Henandez-Sampieri (2023) ya que es la necesidad de comprender y describir las modalidades de estafa, las herramientas tecnológicas empleadas, y las respuestas del sistema judicial frente a este delito. A través de un enfoque cualitativo, se busca no solo describir, sino también explorar las experiencias, percepciones y significados que los actores sociales asignan a los procesos relacionados con la estafa.

El diseño de la investigación fue de tipo fenomenológico y propositivo; en el punto fenomenológica, se recogieron las percepciones y experiencias de fiscales y abogados respecto a las estafas cometidas mediante billeteras digitales, permitiendo que los datos emergieran directamente del campo y reflejaran la realidad vivida por los operadores de justicia; al mismo tiempo, en su campo propositiva, la investigación no solo se limitó a describir dichas realidades, sino que también buscó plantear alternativas orientadas a la mejora del sistema jurídico penal, proponiendo la incorporación de un agravante específico en el delito de estafa contemplado en el Código Penal.

4.2. Ámbito temporal y espacial

La investigación fue realizada en la ciudad de Cusco específicamente en el transcurso del año 2024.

4.3. Población y muestra

La población estuvo conformada por abogados especializados en derecho penal, fiscales en la provincia de Cusco. La selección de la muestra en corroboración con Ñaupas (2022) se realizó mediante un muestreo intencional, seleccionando a los servidores públicos que tengan experiencia directa en la investigación y persecución de estafas tecnológicas

4.4. Instrumentos

Para la recolección de datos se utilizó entrevistas en profundidad. Valderrama (2013) menciono que las entrevistas permitirán obtener información detallada sobre las experiencias y percepciones de los servidores públicos en relación con las estafas tecnológicas.

4.5. Procedimientos

Previo a someter la recolección del instrumento se realizó la validación de los instrumentos mediante juicio de expertos quienes fueron Mgt. Anai Castro Prieto Farfán, Mgt. Hestela Rojas Enríquez, Mgt. Guido Castillo Lira; que cuentan con amplia experiencia en el derecho penal y años de función en el Ministerio Publico.

En merito a la importancia que manifestó Robles (2015) un grupo de especialistas reviso las guías de entrevista y otros instrumentos para garantizar que sean adecuados y efectivos para obtener la información necesaria para cumplir con los objetivos de la investigación.

4.6. Análisis de datos

Consecuentemente se procedió a recolección de datos y análisis mediante codificación temática permitiendo identificar patrones, categorías y relaciones dentro de los datos cualitativos, facilitando una interpretación profunda de los resultados.

Los datos se presentaron de manera descriptiva, con el fin de ilustrar las percepciones de los participantes, y se interpretaron en el contexto del marco teórico y legal previamente estuvo establecido.

4.7. Consideraciones éticas

Durante todo el proceso de recolección de datos, se asegura que los entrevistados, abogados y fiscales, estarán plenamente informados sobre el propósito de la investigación y su participación voluntaria y se cumplió con los principios de integridad y transparencia , asegurando que los datos recolectados fueron utilizados exclusivamente para los fines de la investigación, sin alteraciones ni manipulaciones.

V. Resultados y discusión

En este capítulo, se presentaron los resultados obtenidos a partir de las entrevistas a través de un enfoque cualitativo, se recolectaron opiniones y perspectivas que permiten comprender mejor las modalidades de estafa mediante billeteras digitales, las billeteras más utilizadas y las características que las hacen vulnerables y se exploraron las propuestas sobre la inclusión de un agravante en la legislación penal, con el objetivo de fortalecer la disuasión y sanción de este tipo de delitos.

5.1. Resultados

Tabla 1

Respuestas del primer ítem

Ítem	Entrevistado	Respuesta
¿Cuáles son las modalidades más frecuentes de estafa que ha observado en su práctica profesional, relacionadas con el uso de billeteras digitales en Cusco?	Fiscal. Roman Fiscal. Quillahuaman	La utilización de billeteras digitales sin autorización del titular Pagos realizados a billeteras o números telefónicos falsos y suplantación de identidad de los números telefónicos usados al pago por billetera virtual
	Abg. Vidarte	Considero que los frecuentes son el Yape
	Abg, Chujutalli	El pago por alguna venta de productos supuestamente por la conductiva del producto pero que en realidad no se llega a concretar
	Abg. Cardenas	El uso de baucher y Yapeos falsos
	Abg. Valdivia	Clonación de datos personales creación de accesos directos (link) para descargar la aplicación y a través de ellos obtener los datos del titular
	Abg. Zanabria	Cuando mediante un acceso ilícito a un celular se solicita préstamos de dinero a los contactos del titular en algunos casos media el hurto del celular y en otros no

Codificación cualitativa

- Yape : Mencionado por Abg. Vidarte y Abg. Cárdenas como uno de los fraudes más frecuentes.
- Billeteras digitales sin autorización : Mencionado por Fiscal Román y Abg. Quillahuamán como modalidad común de fraude.

- Fraude en productos no entregados : Mencionado por Abg. Chihuallhuaman en su respuesta sobre la venta fraudulenta de productos.
- Clonación de datos personales : Mencionado por Abg. Valdivia .
- Acceso ilícito a celulares : Mencionado por Abg. Zanabria relacionado con el fraude y préstamos solicitados a contactos del titular.

Las respuestas obtenidas en las entrevistas revelaron que las principales modalidades de estafa mediante billeteras digitales en Cusco incluyen el uso no autorizado de plataformas como Yape , la suplantación de identidad , y el fraude en ventas de productos no entregados así como, la clonación de datos personales y el acceso ilícito a celulares , prácticas que permiten a los delincuentes obtener información para realizar fraudes lo que plantea desafíos para la legalidad y la protección de los usuarios.

Tabla 2

Respuestas del segundo ítem

Ítem	Entrevistado	Respuesta
¿Qué billeteras digitales considera usted como las más utilizadas en los delitos de estafa, y qué características específicas las hacen más vulnerables?	Fiscal. Roman	Yape por ser de uso masivo a nivel nacional
	Fiscal. Quillahuaman	Yape y Plin
	Abg. Vidarte	Lo más utilizado es el Yape y Plin
	Abg, Chujutalli	Yape y respecto a las características sugiero que se debería tener una opción de reportar a los números desde los cuales se podría realizar el depósito falso
	Abg. Cardenas	Yape por ser utilizado de manera virtual
	Abg. Valdivia	Lo más utilizado Yape y justamente lo hace más vulnerable pues al tener que estuvo r en la generalidad vinculada a una cuenta BCP son lo más utilizado por los delincuentes para acceder a la cuenta por la misma aplicación a la web o por datos del equipo móvil
	Abg. Zanabria	Yape y Plim se hacen más vulnerables cuando el usuario no protege su acceso con claves y contengan números u otros pero también es cierto que para los hackers esto no es un obstáculo

Codificación cualitativa

- Yape se mencionó como la billetera digital más utilizada para fraudes debido a su uso masivo a nivel nacional . Esto es indicado por el Fiscal Román , quien destaca su

prevalencia, y el Abg. Cárdenas , quien menciono que se utiliza principalmente de forma virtual.

- Plin , por su parte, es mencionado junto con Yape por el Fiscal Quillahuaman y el Abg. Vidarte como una de las más comunes en estos fraudes.
- En cuanto a las vulnerabilidades , el Abg. Chihuallhuamán señalo que Yape debería permitir reportar números fraudulentos, ya que la falta de estuvo opción facilita los depósitos falsos. El Abg. Valdivia menciono que Yape está vinculado a cuentas bancarias, como las del BCP , lo que la hace más vulnerable a los delincuentes que pueden acceder a la cuenta de los usuarios. Además, el Abg. Zanabria menciono que tanto Yape como Plin son vulnerables cuando no se protegen adecuadamente con claves, lo que facilita su explotación por hackers.

Los entrevistados indicaron que Yape y Plin son las billeteras más utilizadas en estafas en Cusco, principalmente por su uso masivo. Sin embargo, ambas presentan vulnerabilidades como la falta de opciones para reportar números fraudulentos y su vinculación con cuentas bancarias las hace susceptibles a fraudes lo que aumenta el riesgo con las estafas digitales.

Tabla 3

Respuestas del tercer ítem

Ítem	Entrevistado	Respuesta
¿Cree que el sistema jurídico penal actual está preparado para sancionar de manera efectiva las estafas realizadas mediante billeteras digitales?	Fiscal. Roman	Aún no, porque no hay personal especializado en el conocimiento de herramientas digitales
	Fiscal. Quillahuaman	La sanción para este tipo de ilícito penal no está prevista en el código penal
	Abg. Vidarte	No porque durante la investigación que realiza Fiscalía y coordinación no puede identificar el presunto autor
	Abg, Chujutalli	Sí
	Abg. Cardenas	No por ser delitos nuevos que a la fecha no se encuentra incorporado en el sistema jurídico penal
	Abg. Valdivia	No, si bien el derecho como ciencia se encuentra en constante evolución sin embargo muchos de ellos no prevenían como conductas típicas las ejecutadas a través de billeteras digitales además nuestro sistema no cuenta con las herramientas electrónicas adecuadas para el manejo identificación y logística de estos delitos
	Abg. Zanabria	No la unidad De La PNP para delitos informáticos no tiene el implementación ni logística para ser oposición y una investigación exitosa

Codificación cualitativa

- Falta de personal especializado: El Fiscal Román menciono que el sistema no está preparado, ya que no hay personal especializado en herramientas digitales. El Abg. Vidarte indico que, durante las investigaciones, la fiscalía no puede identificar al presunto autor de estos delitos. El Abg. Zanabria resalto que la PNP no cuenta con la logística ni herramientas necesarias para investigar delitos informáticos con éxito.
- No hay sanción prevista: El Fiscal Quillahuamán destacó que la sanción para este tipo de delitos no está específicamente prevista en el Código Penal.
- Reconocimiento del problema: El Abg. Chihuallhuamán considero que sí existe un problema, pero no proporciona detalles adicionales.
- Evolución del derecho: El Abg. Valdivia menciono que el derecho está en constante evolución, pero el sistema no tiene herramientas adecuadas para manejar los delitos cometidos mediante billeteras digitales. El Abg. Cárdenas señalo que, aunque los

delitos no son nuevos, aún no están completamente incorporados al sistema jurídico penal.

Las respuestas indican que, en general, el sistema jurídico penal actual no está completamente preparado para sancionar las estafas realizadas mediante billeteras digitales. Los principales obstáculos incluyen la falta de personal especializado , la ausencia de una sanción específica en el Código Penal y la dificultad para identificar a los autores de estos delitos así como la necesidad de adaptación del derecho a la evolución tecnológica , ya que muchas de las herramientas necesarias para investigar y procesar estos delitos aún no están disponibles en el sistema judicial y policial.

Tabla 4

Respuestas del cuarto ítem

Ítem	Entrevistado	Respuesta
¿Cree usted que sería adecuado incorporar un agravante específico en el artículo 196-A del Código Penal para las estafas cometidas mediante billeteras digitales?	Fiscal. Roman	No
	Fiscal. Quillahuaman	Sí creo que sería óptimo agregar ese hecho como un tipo penal independiente o como un agravante
	Abg. Vidarte	Sí con el fin de poder sancionar este tipo de conducta que se realiza con este tipo de aplicativos como Yape
	Abg, Chujutalli	No
	Abg. Cardenas	Sí
	Abg. Valdivia	A mi consideración sería adecuado puesto estando en la Modernización y propagación de estuvo s billeteras digitales existen mayor cantidad de población vulnerable
	Abg. Zanabria	Como agravante no pero así como una de sus modalidades

Codificación Cualitativa:

- Agravante específico propuesto: Fiscal Quillahuamán, Abg. Cardenas y Abg. Vidarte estuvieron de acuerdo con la idea de agregar un agravante específico en el Código Penal para las estafas realizadas mediante billeteras digitales, referenciando la necesidad de sancionar este tipo de conductas, así mismo el Abg. Valdivia considero

que, dada la modernización de las billeteras digitales y el incremento de usuarios vulnerables, es adecuado

- En desacuerdo: El Abg. Chujutalli y el Fiscal Roman no estuvieron de acuerdo con la incorporación de un agravante.
- No como agravante, sino modalidad: Abg. Zanabria no está de acuerdo con considerarlo un agravante, pero sugiere que podría ser considerado como una modalidad más dentro de los delitos.

En general, la mayoría de los entrevistados estuvo de acuerdo con la necesidad de incluir un agravante específico para las estos casos, argumentando que el crecimiento de estas herramientas y su impacto en una población vulnerable hacen necesaria una sanción más fuerte. Sin embargo, hay diferencias en el enfoque: mientras algunos sugieren un agravante específico , como Fiscal Quillahuaman , Abg. Vidarte y Abg. Cárdenas , otros, como Abg. Zanabria , propone que no sea un agravante, sino una modalidad más.

Tabla 5

Respuestas del quinto ítem

Ítem	Entrevistado	Respuesta
¿Cree que la inclusión de un agravante en el Código Penal para las estafas mediante billeteras digitales ayudaría a reducir el aumento de estos delitos?	Fiscal. Roman	No
	Fiscal. Quillahuaman	Creo que ayudaría a reducir un poco pero no es el mecanismo más adecuado para combatir este tipo de delitos se debería exigir Seguridad a las entidades bancarias
	Abg. Vidarte	Considero que si disminuiría este tipo de delitos
	Abg, Chujutalli	No
	Abg. Cardenas	Sí
	Abg. Valdivia	Si bien la sobre criminalización no es la mejor alternativa para reducir la comisión de delitos en pero es una forma disuasiva en tanto se fortalece el sistema penal como tal
	Abg. Zanabria	No lo que ayudaría es que la PNP tenga las herramientas para descubrir quienes cometen en este delito y así dejar de ser una conducta ilícita atractiva para los delincuentes

Codificación cualitativa:

- Reducción de delitos mediante un agravante:

  Fiscal Quillahuaman consideró que la inclusión de un agravante podría ayudar a reducir un poco los delitos , pero no es el mecanismo más adecuado para combatir

este tipo de estafas, y opina que se debería exigir seguridad a las entidades bancarias como medida preventiva.

Por su parte el Abg. Vidarte estuvo de acuerdo con que la inclusión de un agravante disminuiría este tipo de delitos , ya que daría herramientas legales para enfrentar las estafas digitales.

- Mejorar el sistema penal y fortalecer la disuasión:

  Abg. Cárdenas y el Abg, Valdivia está de acuerdo con que un agravante ayudaría a reducir el problema, pero también subraya la necesidad de fortalecer el sistema penal y establecer mecanismos de disuasión , para que los delincuentes se sientan menos atraídos por este tipo de delitos.

- Herramientas de la PNP y enfoque preventivo:
- Abg. Zanabria opina que lo más importante es que la PNP tenga las herramientas necesarias para descubrir a los delincuentes, además de reducir la atractividad de este tipo de delitos, haciendo que dejaran de ser conductas ilícitas atractivas

Las respuestas muestran que la inclusión de un agravante específico en el Código Penal podría tener un impacto positivo en la reducción de los delitos , aunque no se considera la solución definitiva.

Tabla 6

Respuestas del sexto ítem

Ítem	Entrevistado	Respuesta
¿Qué medidas adicionales o alternativas propondría para evitar que los delincuentes utilicen las billeteras digitales como herramientas para cometer estafas?	Fiscal. Roman	Mejor protección y actualización constante de los aplicativos
	Fiscal. Quillahuaman	Que las entidades bancarias creen mayores mecanismos de seguridad en sus aplicativos de billetera virtual
	Abg. Vidarte	Sanciones penales y que se implementen equipos tecnológicos que se pueda rastrear de donde se habría realizado la transferencia
	Abg, Chujutalli	Siendo que las billeteras virtuales es un medio utilizado por clientes de bancos estas empresas deberían tener un control para poder asegurar el monto transferido o un listado de las cuentas vinculadas a clientes con denuncias por estafa lo que podría alertar a la agraviado de un posible perjuicio económico
	Abg. Cardenas	Mayores medidas de seguridad en el uso de billeteras digitales para que no sean vulnerables fácilmente
	Abg. Valdivia	Que las entidades puedan otorgar mayores mecanismos de seguridad en la u obligatoriedad de la obtención de seguridad para el uso de billeteras digitales
	Abg. Zanabria	Que la aplicación tenga más cuidado y recelo al momento de crear sus contraseñas así como no utilizar redes de Wi-Fi públicas

Codificación Cualitativa Sintetizada:

- Mejoras en seguridad y control:

  El Fiscal Román , Fiscal Quillahuaman , y Abg. Cárdenas coincidió en que es necesario fortalecer la seguridad en los aplicativos de billeteras digitales, exigiendo medidas de actualización constante y mayor protección en las plataformas. Abg. Chihuallhuamán sugiero que las entidades bancarias deben tener un control riguroso de las cuentas vinculadas a denuncias por estafas.

- Uso de tecnología para rastreo:

  Abg. Vidarte propuso utilizar tecnología de rastreo para identificar las transferencias fraudulentas y aplicar sanciones penales .

- Precauciones para los usuarios:

  Por su parte el Abg. Zanabria destacó que los usuarios deben ser más cuidadosos al crear contraseñas seguras y evitar el uso de redes Wi-Fi públicas para proteger sus datos.

La mayoría de los entrevistados coincidieron en que es importante mejorar las medidas de seguridad en el uso de billeteras digitales, tanto a nivel de las entidades bancarias como de los usuarios reflejando la necesidad de fortalecer la protección y monitorear las transferencias para prevenir fraudes, mientras que también se destaca ca la importancia de que los usuarios tomen precauciones para proteger sus datos.

5.2. Discusión

En estudios como la de Ramírez y Azabach (2024) mostraron una fuerte aceleración entre el uso de redes sociales y el aumento de estos delitos hallazgo que es congruente con las respuestas obtenidas de Abg. Cárdenas y Abg. Zanabria, quienes enfatizaron la importancia de que las entidades bancarias y la PNP cuenten con mejores herramientas tecnológicas para investigar y prevenir estos delitos. Sin embargo, el estudio de Ramos (2022) definió como dificultad significativa en la identificación de los responsables de estos fraudes debido a la falta de pruebas y la carencia de tecnología especializada, lo que coincide con las respuestas de los entrevistados que mencionaron la insuficiencia de recursos y la falta de capacitación en investigación digital .

Por otro lado, la investigación de Carbajal (2022) sobre la revolución digital y el aumento de la ciberdelincuencia también resalta la necesidad de fiscalías especializadas , lo cual se refleja en las respuestas de Abg. Vidarte.

Desde mi posición como investigadora, resulta evidente que la problemática de las estafas digitales mediante billeteras virtuales ha superado la capacidad de respuesta del marco normativo vigente. Si bien los estudios internacionales han resaltado la importancia de la ciberseguridad y la especialización en la persecución de delitos informáticos, en el contexto peruano se advierte una brecha significativa entre la evolución del crimen digital y la respuesta del sistema de justicia. La falta de herramientas tecnológicas adecuadas para la

identificación y rastreo de los autores de estos fraudes, mencionados en diversos antecedentes y confirmada por mis entrevistados, refuerza la idea de que la efectividad del sistema penal es aún insuficiente para abordar esta modalidad delictiva.

Considero que la inclusión de un agravante específico para las estafas mediante billeteras digitales en el Código Penal representaría un avance necesario para fortalecer la disuasión y sanción de estos delitos. Sin embargo, como señalaron algunos entrevistados, esta medida no sería suficiente si no se complementa con capacitación especializada para los operadores de justicia y la implementación de mecanismos tecnológicos avanzados para la investigación criminal. En países como Ecuador y Chile, la necesidad de actualización normativa ya ha sido identificada, lo que refuerza la pertinencia de esta propuesta en el contexto peruano.

Asimismo, la responsabilidad del sector bancario y de las plataformas digitales en la prevención de fraudes sigue siendo un tema crítico. A lo largo de la investigación, quedó en evidencia que la falta de controles efectivos en las billeteras digitales facilita la comisión de estafas, generando un vacío de responsabilidad que debe ser abordado con regulaciones más estrictas. Además de la tipificación específica en el Código Penal, considera fundamental establecer protocolos de seguridad más eficientes para las entidades financieras y exigir la implementación de sistemas de alerta más efectivos ante transacciones sospechosas.

VI. Conclusiones

PRIMERO: La incorporación del delito de estafa mediante billeteras digitales en el Código Penal constituye un paso esencial para fortalecer la eficacia del sistema jurídico penal frente a los fraudes digitales; ello porque la legislación vigente aún presenta limitaciones para enfrentar estas conductas, y su inclusión permitiría brindar una respuesta más clara y adecuada frente a un fenómeno que afecta a un número cada vez mayor de ciudadanos.

SEGUNDO: En la ciudad del Cusco se identificó que las modalidades de estafa vinculadas al uso de billeteras digitales, especialmente Yape y Plin, son las más frecuentes; esta situación refleja la vulnerabilidad de los usuarios, quienes carecen de mecanismos de protección efectivos frente a la amplia accesibilidad y uso de estas tecnología.

TERCERO: Las características que incrementan la vulnerabilidad de estas plataformas incluyen la ausencia de sistemas de autenticación en varios niveles, la falta de alertas inmediatas ante transacciones sospechosas y la facilidad con la que los delincuentes pueden suplantar información de contacto, lo cual facilita la comisión de fraudes.

CUARTA: La propuesta de establecer un agravante específico para los delitos de estafa cometidos mediante billeteras digitales representa un avance significativo en el fortalecimiento de la disuasión y sanción; esta medida proporcionaría a los tribunales una herramienta más efectiva para imponer sanciones proporcionales al daño causado y contribuiría a reducir la reincidencia en este tipo de conductas delictivas.

VII. Recomendaciones

PRIMERO: Se recomienda a los legisladores y responsables de la reforma penal incluir expresamente el fraude cometido mediante billeteras digitales dentro de los delitos específicos del Código Penal; esta medida permitiría que el sistema jurídico se adecúe a los avances tecnológicos y brinde una protección más efectiva a los ciudadanos frente a estas nuevas modalidades delictivas.

SEGUNDO: Se recomienda a las autoridades locales y organismos de seguridad implementar campañas de sensibilización orientadas a la población para informar sobre los riesgos de estafas a través de billeteras electrónicas; dichas campañas deberían fomentar el uso de herramientas de seguridad complementarias, como la autenticación en dos factores, a fin de prevenir la victimización.

TERCERO: Se recomienda a las empresas desarrolladoras de billeteras digitales y a las entidades financieras fortalecer sus protocolos de seguridad mediante la incorporación de mecanismos más rigurosos, como la autenticación biométrica y la emisión de alertas inmediatas ante operaciones sospechosas; ello contribuiría a reducir la exposición de los usuarios a transacciones fraudulentas.

CUARTA: Se recomienda a los legisladores y autoridades judiciales valorar la inclusión de un agravante específico para este tipo de estafa, de modo que los responsables reciban sanciones más severas y proporcionales al daño causado; esta medida no solo reforzaría la disuasión, sino que también contribuiría a prevenir la reincidencia en fraudes digitales vinculados al uso de billeteras electrónicas.

VIII. Referencias

Acosta, J. (2022). *Efectos de la insuficiente legislación persecutoria del delito de estafascibernética en el distrito fiscal del Santa.* https://repositorio.ucv.edu.pe/handle/20.500.12692/138107

Acurio, S. (2016). *Delitos informaricos: Generalidades.* https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Aredo, L. (2021). *El phishing y su vulneración a la protección de datos personales en los delitos informáticos.* Repositorio Institucional de la Universidad Cesar Vallejo: https://repositorio.ucv.edu.pe/handle/20.500.12692/80920

Beraún, C. (2020). *El delito de estafaspor medios tecnoloicos en tiempos de la COVID-19 Lima.* https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/81913/Bera%C3%BAn_LCJ-SD.pdf?sequence=1

Berger, L., & Luckmann, T. (2010). *La construcción social de la realidad.* https://dialnet.unirioja.es/servlet/articulo?codigo=3262960

Biblioteca Juridica Digital España. (2021). *Las siete partidas.* https://www.boe.es/biblioteca_juridica/publicacion.php?id=PUB-LH-2021-217

Carbajal, M. (2022). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha conra el cibrecrimen.* https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/11398/carbajal_cm.pdf?sequence=1&isAllowed=y

Carrasco, C. (2024). *Analisi fáctico- objetivo al elemento engaño dentro de la estafa.* https://repositorio.uisek.edu.ec/bitstream/123456789/934/1/Tesis%20Carlos%20Carrasco%20Y%c3%a9pez.pdf

Cisneros, C., & Jimenez, R. (2021). *El delito de estafa: naturaleza, elementos y consumación.* https://www.scielo.org.mx/scielo.php?pid=S2007-78902021000600042&script=sci_arttext_plus&tlng=es

Congreso de la Republica del Perú. (2013). *Ley N° 30096.* Ley de Delitos Informaticos y sus modificatorias: https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

Cornejo, A. (2023). *La investigación de delitos informáticos y su prueba en materia penal.* https://repositorio.uchile.cl/bitstream/handle/2250/196235/La-investigacion-de-delitos-informaticos-y-su-prueba-en-materia-penal.pdf?sequence=1&isAllowed=y

Corte Suprema de Jusiticia de la Republica. (2016). *Sala Transitoria* . Casación N° 461-2016: https://actualidadpenal.pe/jurisprudencia/delito-de-estafa-tipicidad-objetiva-y-consumacion-cas-n0-461-2016-arequipa/1

Cruz, J. (2021). *Propuestuvo s para neutralizar la alta incidencia del delito e estafasen sus diversas modalidades.* https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/24197/CRUZ_CHAMBA_JOSE_MANUEL_MG.pdf?sequence=1&isAllowed=y

Diario el Peruano. (2024). *¡Cuidado! Crecen denuncias de fraude informático en el Perú.* https://elperuano.pe/noticia/241353-cuidado-crecen-denuncias-de-fraude-informatico-en-el-peru

Diario Oficial el Peruano. (2004). *Codigo Penal Peruano.*

El Peruano. (2023). *Poder Judicial: estafaspor redes sociales se castigan hasta con ocho años de cárcel.* https://www.elperuano.pe/noticia/232161-poder-judicial-estafas-por-redes-sociales-se-castigan-hasta-con-ocho-anos-de-carcel

Eolo comunicación. (2023). *Redes Sociales: Cómo aprovechar al máximo su impacto en la comunicación.* https://eolocomunicacion.com/que-son-las-redes-sociales/

Garita, R. (2013). *Desarrollo de sistemas y aplicaciones para las Unidades de Información.* https://www.redalyc.org/pdf/4768/476848738003.pdf

Ginger, M. (2022). *Incidencia del delito de estafasa través del uso de redes Sociales, año 2017-2020, cantón La Libertad.* https://repositorio.upse.edu.ec/bitstream/46000/8820/1/UPSE-TDR-2022-0064.pdf

Giraldo, C. (2023). *Casi 800 casos de estafaspor redes sociales han sido denunciados en lo que va del 2023.* https://www.infobae.com/peru/2023/07/19/casi-800-casos-de-estafa-por-redes-sociales-han-sido-denunciados-en-lo-que-va-del-2023/

Gomezjurado, J. (2022). *Identificacion del sujeto activo en el delito de estafasa travez de medios digitales y electronicos bajo la perspectiva del COIP en el Ecuador.* https://repositorio.uide.edu.ec/bitstream/37000/5790/1/UIDE-Q-TDR-2023-5.pdf

Goncalves, W. (2024). *Facebook: ¡todo sobre la red social más usada en el mundo!* https://rockcontent.com/es/blog/facebook/#google_vignette

Hernandez Sampieri, R., & Mendoza, C. (2023). *Metodologia de la Investigacion- Las rutas cuantitativa, cualitativa y mixta* (Vol. segunda edición). Mexico: Mc graw Hill.

Lajo, B. (2007). *La teoría del engaño.* https://www.levante-emv.com/opinion/2007/03/06/teoria-engano-13606609.html

Mayer, L. (2014). *El engaño concluyente en el delito de estafa*. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372014000300010

Ñaupas, H., E., M., & Novoa, E. &. (2022). *Metodología de lainvestigación: Cuantitativa - cualitativa y redacción de la tesis.* Ediciones de la U.

Pagina oficial de gobierno. (2024). *Conocer más sobre las billeteras digitales disponibles en el Perú.* https://www.gob.pe/14930-conocer-mas-sobre-las-billeteras-digitales-disponibles-en-el-peru

Paguay, V. (2020). *Las nuevas perspectivas regulatorias de delitos informaticos en ñas compras a traves de internet.* http://dspace.unach.edu.ec/bitstream/51000/7607/1/8.-TESIS%20VER%C3%93NICA%20LILIANA%20PAGUAY%20CALDER%C3%93N-DER.pdf

Pallasco, O., Proaño, G., & Romero, A. (2022). *Delitos de estafasa través de redes sociales en época de pandemia.* https://dspace.uniandes.edu.ec/bitstream/123456789/14802/1/UA-MMP-EAC-037-2022.pdf

Pontón , D. (2020). *El aporte de Edwin Sutherland al análisis del crimen económico global.* https://www.redalyc.org/journal/5526/552663274006/html/

Ramirez, K., & Azabache, S. (2024). *Influencia de las redes sociales en los delitos de estafasinformática y las consecuencias jurídicas Huaura -.* https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/9530/TESIS.pdf?sequence=1&isAllowed=y

Ramos, M. (2022). *Impacto de los delitos informaticos en las investigaciones preparatorias de las fiscalías provinciales penales corporativas distrito fiscal Lima S ur.* https://repositorio.uwiener.edu.pe/bitstream/handle/20.500.13053/8051/T061_73813479_TSP.pdf?sequence=1&isAllowed=y

Recalde, J. (2024). *Analasis de los delitos privados en el derecho romano.* https://repositorio.puce.edu.ec/server/api/core/bitstreams/82ebd313-4c88-4dc8-8482-20c4d1f8a7cd/content

Robles, P. (2015). *La validación por juicio de expertos; dos investigaciones cualitativas en lingüística aplicada.* Revista Nebrija de lingüística aplicada.: https://www.nebrija.com/revistalinguistica/files/articulosPDF/articulo_55002aca89c37

Rodriguez, J. (2020). *Una aproximación al delito de estafasen sus modalidades clásica e informática:De la estafastradicional a las nuevasmodalidades como el Phishing.* https://ruc.udc.es/dspace/bitstream/handle/2183/27015/Rodr%C3%ADguezGarc%C3%ADaJos%C3%A9David_TFM_2020.pdf

Ruiz, H. (2021). *El delito de estafasy sus elementos constitutivos ¿Cuál es el más importante?* https://iuslatin.pe/el-delito-de-estafa-y-sus-elementos-constitutivos-cual-es-el-mas-importante/

Urbizagástegui, R. (2019). *El modelo de difusión de innovaciones de Rogers en la bibliometría mexicana.* https://www.redalyc.org/journal/3505/350560860001/html/

Valderrama, S. (2013). *Pasos para elaborar proyectos de investigación científica, Cuantitativa, cualitativa y mixta* (Vol. Segunda Edición). Peru: San Marcos.

Vega, L. (2020). *Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima* . https://repositorio.ucv.edu.pe/handle/20.500.12692/83325

Los anexos, panel fotográfico y otros documentos están resguardados en la oficina de repositorio digital institucional en la Biblioteca Central de la Universidad Tecnológica de los Andes