UNIVERSIDAD NACIONAL DE TUMBES

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

La estafa informática y su relación con las criptomonedas en el Perú, 2023

Tesis para optar el título profesional de Abogado

Autor: Br. Acuña Estrada, Bryan Jhair

Tumbes, 2026

UNIVERSIDAD NACIONAL DE TUMBES

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

La estafa informática y su relación con las criptomonedas en el Perú, 2023

Tesis aprobada en forma y estilo por:

Mg. Frank Alexander Díaz Valiente
Código ORCID: 0000-0001-6750-4527
Presidente

Mg. Hugo Chanduvi Vargas
Código ORCID: 0000-0002-7655-8487
Secretario

Mg. Cinthia Milagros Córdova Rivera
Código ORCID: 0000-0001-6831-2295
Vocal

Mg. Carlos Alberto Vargas Vilela
Código ORCID: 0009-0001-7090-9477
Accesitario

Tumbes, 2026

UNIVERSIDAD NACIONAL DE TUMBES

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

La estafa informática y su relación con las criptomonedas en el Perú, 2023

Los suscritos declaramos que la tesis es original en su contenido y forma:

Br. Acuña Estrada, Bryan Jhair
Cod. ORCID 0009-0000-0670-4760

Autor

Mg. Córdova Rivera, Cinthia Milagros
Cod. ORCID: 0000-0001-6831-2295

Asesora

Tumbes, 2026

CERTIFICACIÓN

Yo, Mg. Córdova Rivera, Cinthia Milagros, docente ordinario de la Universidad Nacional de Tumbes, adscrito a la Escuela Profesional de Derecho, Facultad de Derecho y Ciencias Políticas.

CERTIFICA:

Que el proyecto de tesis denominado "La estafa informática y su relación con las criptomonedas en el Perú, 2023", presentado por el tesista Bach. Acuña Estrada Bryan Jhair, ha sido asesorado por mi persona, por tanto, queda autorizado para su presentación e inscripción en la Escuela Profesional de Derecho de la Universidad Nacional de Tumbes para su revisión y aprobación correspondiente.

Tumbes, 31 de marzo de 2026

Mg. Córdova Rivera, Cinthia Milagros
Código ORCID: 0000-0001-6831-2295
Asesor

UNIVERSIDAD NACIONAL DE TUMBES
FACULTAD DE DERECHO Y CIENCIA POLÍTICA
ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACIÓN DE TESIS

En la ciudad de Tumbes, a los cuatro días del mes de mayo del dos mil veintiséis, a las 18:00 horas, los integrantes del jurado, designado mediante **Resolución Decanal N° 215-2024/UNTUMBES-FDCP-D(e): 09 de julio de 2024, integrado** por el **Mg. Frank Alexander Díaz Valiente,** en su condición de Presidente, con DNI N° 46378953; **Mg. Carlos Alberto Vargas Vilela**, con DNI N° 42798179, en su condición de Secretario; y la **Mg. Cinthia Milagros Córdova Rivera**, con DNI N° 41581317, en su condición de Asesora - Vocal, con la finalidad de realizar la evaluación del informe final de tesis, titulado: "La estafa informática y su relación con las criptomonedas en el Perú, 2023", para optar el Título Profesional de Abogado, del bachiller: Bryan Jhair Acuña Estrada, la que se realiza en FORMA PRESENCIAL.

En conformidad con el artículo 71 y siguientes del Reglamento de Tesis de la Universidad Nacional de Tumbes, la sustentación de tesis es un acto púbico de exposición y defensa, amparado en las normas reglamentarias invocadas. El presidente del jurado dio por iniciado el acto de sustentación, concediendo el uso de la palabra al tesista,: Bryan Jhair Acuña Estrada, para que procedan a la sustentación de la Tesis.

Luego de la sustentación, se procedió a la formulación de preguntas y finalmente a la deliberación del jurado, en conformidad con el artículo 75 del Reglamento Tesis de la Universidad Nacional de Tumbes. Declaran aprobado por unanimidad con el calificativo de Regular ( ) Buena ( ) Muy Buena (X) y Sobresaliente ( ).

Por tanto, el Bachiller, queda **APTO** para iniciar los trámites administrativos, y el Consejo Universitario de la Universidad Nacional de Tumbes, expida el Título Profesional de Abogado, en conformidad con lo estipulado en el Artículo N° 90 del Estatuto de la Universidad Nacional de Tumbes y lo normado en el Reglamento de Grados y Títulos.

Siendo las 18... horas con 59 minutos, del mismo día, el presidente del jurado dio por concluido el presente acto académico, de sustentación de tesis, para mayor constancia de lo actuado firmaron en señal de conformidad todos los integrantes del jurado.

Mg. Frank Alexander Díaz Valiente
DNI N° 46378953
Código ORCID 0000- 0001- 6750- 4527
Presidente

Mg. Carlos Alberto Vargas Vilela
DNI N° 80453434
Código ORCID :0009- 0001- 7090- 9477
Secretario

Mg. Cinthia Milagros Cordova Rivera
DNI N°41581317
Código ORCID: 0000-0001-6831-2295
Asesora - Vocal

RESUMEN DE TURNITIN

BRYAN JHAIR ACUÑA ESTRADA

La estafa informática y su relación con las criptomonedas en el Perú, 2023

PROYECTOS DE TESIS 2025

Detalles del documento

Identificador de la entrega
trn:oid:::3117:573442186

Fecha de entrega
31 mar 2026, 10:14 GMT-5

Fecha de descarga
31 mar 2026, 10:18 GMT-5

Nombre del archivo
TESIS ESTAFA Y CRIPTOMONEDAS - ACUÑA.docx

Tamaño del archivo
265.3 KB

74 páginas

15.935 palabras

96.281 caracteres

turnitin Página 1 de 80 - Portada Identificador de la entrega trn:oid:::3117:573442186

Mg. Cinthia Milagros Cordova Rivera
DNI N° 41581317
Código ORCID: 0000-0001-6831-2295
Asesora - Vocal

9% Similitud general

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

Filtrado desde el informe

- Bibliografía
- Coincidencias menores (menos de 15 palabras)

Fuentes principales

8% Fuentes de Internet
3% Publicaciones
7% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° 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.

Mg. Cinthia Milagros Cordova Rivera
DNI N° 41581317
Código ORCID: 0000-0001-6831-2295
Asesora - Vocal

turnitin Página 2 de 80 - Descripción general de integridad Identificador de la entrega trn:oid:::3117:573442186

Fuentes principales

8% Fuentes de Internet
3% Publicaciones
7% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1 Internet
repositorio.untumbes.edu.pe <1%

2 Internet
hdl.handle.net <1%

3 Internet
alicia.concytec.gob.pe <1%

4 Trabajos del estudiante
uncedu on 2025-03-28 <1%

5 Internet
repositorio.unjfsc.edu.pe <1%

6 Internet
core.ac.uk <1%

7 Internet
repositorio.uch.edu.pe <1%

8 Trabajos del estudiante
Universidad Continental on 2024-11-09 <1%

9 Trabajos del estudiante
Universidad Continental on 2026-03-19 <1%

10 Trabajos del estudiante
Universidad Nacional Federico Villarreal on 2025-11-13 <1%

11 Trabajos del estudiante
Universidad Privada del Norte on 2026-02-27 <1%

Mg. Cinthia Milagros Cordova Rivera
DNI N° 41581317
Código ORCID: 0000-0001-6831-2295
Asesora - Vocal

turnitin Página 3 de 80 - Descripción general de integridad Identificador de la entrega trn:oid:::3117:573442186

12	Internet	
apirepositorio.unu.edu.pe		<1%
13	Internet	
repositorio.ucv.edu.pe		<1%
14	Trabajos del estudiante	
Universidad Andina Nestor Caceres Velasquez on 2025-11-25		<1%
15	Trabajos del estudiante	
Universidad TecMilenio on 2025-01-28		<1%
16	Trabajos del estudiante	
Universidad Cesar Vallejo on 2025-07-25		<1%
17	Internet	
dokumen.pub		<1%
18	Internet	
repositorio.unap.edu.pe		<1%
19	Trabajos del estudiante	
Integración Blackboard on 2025-08-12		<1%
20	Internet	
repositorio.autonoma.edu.pe		<1%
21	Internet	
dspace-uh-tmp.igniteonline.la		<1%
22	Internet	
cdn.nestjs.wipolex.wji.prd.web1.wipo.int		<1%
23	Internet	
repositorio.undac.edu.pe		<1%
24	Trabajos del estudiante	
Universidad Nacional del Centro del Peru on 2025-08-23		<1%
25	Internet	
larepublica.pe		<1%

Mg. Cinthia Milagros Cordova Rivera
DNI N° 41581317
Código ORCID: 0000-0001-6831-2295
Asesora - Vocal

turnitin Página 4 de 80 - Descripción general de integridad Identificador de la entrega trn:oid:::3117:573442186

26	Trabajos del estudiante	
Uniminuto Virtual on 2025-11-04		<1%
27	Trabajos del estudiante	
Universidad Cesar Vallejo on 2025-07-23		<1%
28	Trabajos del estudiante	
Universidad San Ignacio de Loyola on 2025-02-28		<1%
29	Internet	
repositorio.upsjb.edu.pe		<1%
30	Publicación	
CONSULTORIA INTERNACIONAL EN INGENIERIA Y GESTION PARA EL DESARROLLO...		<1%
31	Trabajos del estudiante	
Universidad Cesar Vallejo on 2025-09-10		<1%
32	Trabajos del estudiante	
Universidad Nacional de Tumbes on 2025-10-24		<1%
33	Trabajos del estudiante	
Universidad Privada del Norte on 2024-05-19		<1%
34	Trabajos del estudiante	
University of La Guajira on 2025-08-24		<1%
35	Trabajos del estudiante	
Instituto Superior de Artes, Ciencias y Comunicación IACC on 2025-11-23		<1%
36	Trabajos del estudiante	
Universidad Tecnológica Indoamerica on 2024-05-02		<1%
37	Trabajos del estudiante	
Universitat Oberta de Catalunya on 2026-03-08		<1%
38	Trabajos del estudiante	
University of Essex on 2026-02-13		<1%
39	Internet	
laccei.org		<1%

Mg. Cinthia Milagros Cordova Rivera
DNI N° 41581317
Código ORCID: 0000-0001-6831-2295
Asesora - Vocal

40 Internet

www.congreso.gob.pe <1%

Mg. Cinthia Milagros Cordova Rivera
DNI N° 41581317
Código ORCID: 0000-0001-6831-2295
Asesora - Vocal

turnitin Página 6 de 80 - Descripción general de integridad Identificador de la entrega trn:oid:::3117:573442186

DEDICATORIA

A mi madre, Cecilia, por ser raíz, techo y camino. A mi abuelita Nelly, por enseñarme que la ternura también es una forma de valentía. Dedico esta obra al Bryan que sobrevivió a sus propias tormentas y aprendió a caminar con el viento en contra. A mi versión del pasado, que soñó con este momento sin saber cuánto costaría.

AGRADECIMIENTO

A mis docentes, que moldearon mis dudas en certezas. A quienes me tendieron una mano sin pedir nada a cambio. A quienes se alejaron, porque me recordaron que el camino es para quienes quieren andar conmigo. A Dios, por darme fuerza cuando mis fuerzas ya no alcanzaban. A la vida, por forjar carácter donde otros verían obstáculos.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

La presente investigación tuvo como objetivo determinar la relación entre el delito de estafa informática y las criptomonedas en el Perú, 2023. El estudio se desarrolló bajo un enfoque cuantitativo, de tipo básica, nivel correlacional y diseño no experimental de corte transversal. La población estuvo conformada por operadores del derecho con conocimientos en la materia, a quienes se les aplicó un cuestionario estructurado. La validez del instrumento se estableció mediante juicio de expertos y la confiabilidad se determinó con el coeficiente Alfa de Cronbach, obteniéndose un valor de 0.81, considerado de muy alta confiabilidad. Para el procesamiento de la información se utilizó el programa estadístico SPSS y, en el análisis inferencial, se aplicó el coeficiente Tau-b de Kendall. Los resultados evidenciaron una relación positiva débil y estadísticamente significativa entre el delito de estafa informática y las criptomonedas ($\tau b = 0.309$; $p = 0.003$). Asimismo, se identificó relación significativa entre los sistemas de inversión online y las criptomonedas ($\tau b = 0.308$; $p = 0.001$), entre el phishing y las criptomonedas ($\tau b = 0.201$; $p = 0.001$), entre las transferencias falsas y las criptomonedas ($\tau b = 0.304$; $p = 0.003$), y entre el comercio electrónico fraudulento y las criptomonedas ($\tau b = 0.305$; $p = 0.008$). Se concluye que las criptomonedas se relacionan de manera significativa con diversas modalidades de estafa informática, favorecidas por el anonimato relativo, la limitada trazabilidad y la insuficiente regulación en el contexto peruano.

Palabras claves: criptomonedas, estafa informática, fraude digital, phishing, seguridad tecnológica.

ABSTRACT

This research aimed to determine the relationship between online fraud and cryptocurrencies in Peru in 2023. The study employed a quantitative, basic, correlational, and non-experimental cross-sectional design. The population consisted of legal professionals with expertise in the subject, who were administered a structured questionnaire. The instrument's validity was established through expert review, and its reliability was determined using Cronbach's alpha coefficient, yielding a value of 0.81, considered highly reliable. The SPSS statistical software was used for data processing, and Kendall's Tau-b coefficient was applied for inferential analysis. The results showed a weak but statistically significant positive relationship between online fraud and cryptocurrencies ($\tau b = 0.309$; $p = 0.003$). Furthermore, a significant relationship was identified between online investment systems and cryptocurrencies ($\tau b = 0.308$; $p = 0.001$), between phishing and cryptocurrencies ($\tau b = 0.201$; $p = 0.001$), between fraudulent transfers and cryptocurrencies ($\tau b = 0.304$; $p = 0.003$), and between fraudulent e-commerce and cryptocurrencies ($\tau b = 0.305$; $p = 0.008$). It is concluded that cryptocurrencies are significantly related to various forms of online fraud, facilitated by relative anonymity, limited traceability, and insufficient regulation in the Peruvian context.

Keywords: cryptocurrencies, computer fraud, digital fraud, phishing, technological security.

I. INTRODUCCIÓN

En la actualidad, el panorama digital está marcado por un incremento en la adopción de criptomonedas como mecanismo para el intercambio y resguardo de valor, lo cual ha transformado significativamente la dinámica de las transacciones económicas a nivel global. Sin embargo, este vertiginoso avance también ha generado nuevos desafíos tanto legales y sociales, entre los cuales destaca la "*proliferación de delitos informáticos"*, particularmente la estafa informática, que se ha visto fortalecida por el uso de entornos digitales descentralizados (Bank for International Settlements, 2023). Asimismo, este fenómeno se vincula con los riesgos emergentes asociados a los criptoactivos en el sistema financiero global (European Central Bank, 2023). En ese sentido, ambas variables adquieren relevancia debido a su interacción directa dentro de un ecosistema digital en constante evolución.

A nivel internacional, la problemática de la estafa informática vinculada al uso de criptomonedas ha experimentado un crecimiento sostenido, debido a las características propias de estos activos digitales, como el anonimato, la irreversibilidad de las transacciones y la ausencia de regulación uniforme en diversos países. Estas condiciones han permitido que organizaciones criminales adapten sus métodos delictivos tradicionales hacia nuevas modalidades digitales, utilizando criptomonedas para ejecutar fraudes, estafas de inversión y otras actividades ilícitas a gran escala, generando pérdidas económicas significativas (United Nations Office on Drugs and Crime, 2024). De igual manera, se ha evidenciado que el uso criminal de criptomonedas se ha expandido en distintas regiones, consolidándose como un problema transnacional (COPOLAD, 2025). En este contexto, la importancia de las variables radica en que la estafa informática ha evolucionado en complejidad y alcance, encontrando en las criptomonedas un medio que potencia su ejecución.

Asimismo, diversos reportes internacionales evidencian que el uso de criptomonedas en delitos informáticos continúa en aumento, consolidándose como un mecanismo recurrente para la comisión de fraudes digitales, especialmente en esquemas como phishing, plataformas falsas de inversión y transferencias

engañosas, donde la dificultad para rastrear operaciones representa un desafío para las autoridades (Chainalysis, 2026).

En esa misma línea, estudios recientes advierten que la trazabilidad limitada de las transacciones favorece la expansión de estafas digitales en entornos descentralizados (TRM Labs, 2026). Esta situación pone en evidencia la necesidad de fortalecer los sistemas de control y supervisión a nivel global, así como de comprender la relación existente entre ambas variables.

En el contexto peruano, la estafa básica se encuentra regulada en el artículo 196 del Código Penal; sin embargo, no se hace una mención específica a la estafa informática, lo cual evidencia una limitación normativa frente a las nuevas modalidades delictivas que surgen en entornos digitales. Esta situación guarda similitud con experiencias internacionales como la de Alemania, donde fue necesario adecuar el tipo penal para responder a los desafíos del delito informático, mientras que en países como España ya existen disposiciones específicas que regulan esta figura en el ámbito digital (European Criminal Law Review, 2024). Asimismo, diversos estudios jurídicos destacan la necesidad de modernizar los marcos normativos frente a los delitos informáticos emergentes (Carrizosa, 2024). En ese sentido, la importancia de las variables a nivel nacional radica en la necesidad de adecuar el marco jurídico peruano para enfrentar eficazmente estos delitos.

Del mismo modo, en el Perú se ha evidenciado un incremento de casos vinculados a fraudes digitales mediante el uso de plataformas virtuales y criptomonedas, lo cual se ve agravado por las dificultades en la obtención y valoración de pruebas digitales, así como en la identificación de los responsables, lo que limita la eficacia del sistema de justicia (Arce, 2026). A ello se suma que la individualización del ciberdelincuente representa un desafío constante en el ámbito penal, dificultando la persecución efectiva de estos delitos (Gómez, 2026). En consecuencia, la relación entre la estafa informática y las criptomonedas adquiere especial relevancia en el ámbito nacional, debido a la necesidad de fortalecer tanto la normativa como los mecanismos de investigación.

Por lo tanto, se fijó como objetivo general determinar la relación que existe entre el delito de estafa informática y las criptomonedas en el Perú, 2023 y de manera específica: Evaluar la relación que existe entre los sistemas de inversión online y las criptomonedas en el Perú, 2023., Establecer la relación que existe entre el Phishing y las criptomonedas en el Perú, 2023., Identificar la conexión que existe entre las transferencias falsas y las criptomonedas en el Perú, 2023. , Analizar la asociación que existe entre el Comercio Electrónico Fraudulento y las criptomonedas en el Perú, 2023.

A nivel local, esta problemática se manifiesta de manera más cercana a la realidad de los ciudadanos, donde se observa el incremento de estafas a través de redes sociales, plataformas digitales y aplicaciones de pago, incluyendo medios como Yape y Plin, los cuales, a pesar de estar respaldados por entidades financieras, también son utilizados para la comisión de fraudes. Asimismo, se han identificado casos de plataformas falsas, esquemas piramidales y suplantación de identidad digital, donde los usuarios, muchas veces por desconocimiento en ciberseguridad, resultan afectados (Ayala, 2024). De igual manera, estudios recientes evidencian la creciente incidencia del fraude digital en entornos virtuales y redes sociales (Federal Bureau of Investigation, 2023). En este nivel, la importancia de las variables radica en su impacto directo en la población, generando pérdidas económicas y afectando la confianza en el uso de herramientas digitales.

En relación con lo anterior, se observa que modalidades como el phishing han evolucionado hacia el ecosistema de las criptomonedas, donde los ciberdelincuentes crean sitios web fraudulentos que simulan ser plataformas legítimas, logrando obtener datos personales y financieros de los usuarios, lo que conlleva a la pérdida irreversible de sus fondos. Asimismo, las transferencias falsas y el comercio electrónico fraudulento se han incrementado, aprovechando las características propias de las criptomonedas, como su anonimato y descentralización, lo que dificulta la recuperación del dinero y la identificación de los responsables (Carrizosa, 2024). En esa misma línea, investigaciones sobre delitos en entornos Web3 confirman la sofisticación creciente de estas modalidades fraudulentas (Wu et al., 2022).

Estas prácticas delictivas no solo generan pérdidas económicas significativas, sino que también afectan la confianza de los usuarios en las tecnologías financieras digitales, limitando su adopción y desarrollo. En ese sentido, la presente investigación se justifica desde el punto de vista metodológico, ya que permitirá analizar la relación entre la estafa informática y el uso de criptomonedas mediante un enfoque sistemático que contribuya al desarrollo del conocimiento en el ámbito jurídico (Arias et al., 2022). Asimismo, estudios sobre riesgos en criptomonedas evidencian que la percepción de inseguridad influye en su adopción y uso (Rojas Rincón, 2023).

Desde el punto de vista práctico, el estudio permitirá proponer mejoras en los mecanismos de prevención, investigación y sanción de estos delitos en el Perú, contribuyendo al fortalecimiento del sistema de justicia. En el ámbito social, la investigación resulta relevante debido a que estas conductas delictivas afectan directamente a los ciudadanos, generando inseguridad y vulnerabilidad en el uso de tecnologías digitales (Federal Trade Commission, 2023). A su vez, organismos internacionales advierten que la protección del consumidor financiero es clave frente al crecimiento de los criptoactivos (World Bank, 2023). Finalmente, desde el enfoque económico, el estudio adquiere importancia al evidenciar cómo estas estafas impactan negativamente en el desarrollo de la economía digital y en la confianza de los inversionistas.

En ese orden de ideas, se establece como problema de estudio: ¿Cuál es la relación que existe entre el delito de estafa informática y las criptomonedas en el Perú, 2023?, ¿De qué manera están relacionados los sistemas de inversión online y las criptomonedas en el Perú, 2023?, ¿Qué vínculo existe entre el Phishing y las criptomonedas en el Perú, 2023?, ¿Cómo se conectan las transferencias falsas con las criptomonedas en el Perú, 2023?, ¿Qué asociación hay entre el Comercio Electrónico Fraudulento y las criptomonedas en el Perú, 2023?

II. REVISIÓN DE LA LITERATURA

2.1 BASES TEÓRICAS

2.1.1 ANTECEDENTES

A nivel internacional

Wang y Deng (2026) tuvieron como objetivo general:

> Explorar los factores determinantes y los mecanismos de acción que influyen en la intención de participación de las víctimas en fraudes de inversión con criptomonedas desde la perspectiva de la Teoría del Comportamiento Planificado; metodológicamente, desarrollaron una investigación de enfoque cuantitativo, diseño no experimental y corte transversal, aplicando la técnica de encuesta mediante un cuestionario estructurado con escala Likert de cinco puntos dirigido a víctimas de fraude de inversión con criptomonedas en China, obteniendo 322 cuestionarios, de los cuales 287 fueron válidos, con una tasa de respuesta efectiva del 89 %; respecto de los resultados generales, reportaron que el modelo presentó adecuada validez y confiabilidad, con cargas factoriales superiores a 0.73, valores de AVE entre 0.609 y 0.760, fiabilidad compuesta entre 0.884 y 0.941, alfa de Cronbach en niveles excelentes, un KMO de 0.920 y prueba de esfericidad de Bartlett significativa ($\chi^2 = 7310.113$; $gl = 496$; $p < .001$), además de una varianza acumulada explicada de 78.169 %, mientras que, en los resultados específicos, hallaron que la actitud de participación y el control conductual percibido tuvieron un efecto positivo significativo sobre la intención de participar en este tipo de inversiones fraudulentas, y que los rasgos de personalidad, las leyes y regulaciones, la educación en inversión y la exposición a casos de fraude incidieron de manera directa e indirecta sobre dicha intención; asimismo, se observó que la correlación más alta se dio entre actitud de participación y control conductual percibido ($r = 0.559$), una correlación positiva entre regulación y educación en inversión ($r = 0.500$), y una correlación negativa más fuerte entre casos típicos y educación en inversión ($r = -0.522$), mientras que las normas subjetivas mostraron baja asociación con las demás variables; en conclusión, los autores sostuvieron que la intención de participación de las víctimas en fraudes de inversión con

criptomonedas depende principalmente de factores cognitivos y actitudinales individuales más que de la presión social, por lo que la naturaleza descentralizada de las criptomonedas favorece que las víctimas confíen más en su propio juicio.

Dulisse et al. (2025) tuvieron como objetivo general:

> Examinar los patrones utilizados por los estafadores que cometen fraude financiero mediante criptomonedas, centrándose en los tipos de estafa, las pérdidas económicas y los métodos de contacto empleados con las víctimas; metodológicamente, desarrollaron un estudio de enfoque cuantitativo, de nivel descriptivo-exploratorio, basado en análisis documental y de contenido de denuncias de consumidores registradas en dos bases estatales públicas de rastreo de estafas de criptomonedas de California y Wisconsin, utilizando como fuente de información los reportes narrativos completos de las quejas presentadas ante dichas agencias, con una muestra total de 291 casos, de los cuales 260 correspondieron a California y 31 a Wisconsin; en cuanto a los resultados generales, encontraron que las estafas con criptomonedas comparten rasgos con otros fraudes financieros en línea, aunque conservan características particulares ligadas a plataformas digitales, anonimato y comunicación remota, observándose además que las víctimas fueron predominantemente hombres y que casi todas las interacciones iniciales ocurrieron por medios digitales, pues solo 1 de 291 contactos se produjo de manera presencial, mientras que 18.9 % de los casos parecían haber sido iniciados por la propia víctima al ingresar a sitios de inversión o plataformas de trading; de forma específica, las modalidades más frecuentes fueron el uso de plataformas de trading fraudulentas, con 41.1 % del total, y las estafas tipo pig butchering, con 27 %, de modo que más de dos tercios de los fraudes se concentraron en estos dos esquemas, caracterizados por la construcción de una apariencia de legitimidad y el abuso de la confianza; asimismo, los autores identificaron que los estafadores solían presentarse con títulos de “figuras de autoridad”, “expertos financieros” o “conocidos” para reforzar credibilidad, y que las pérdidas económicas más elevadas se registraron cuando el contacto inicial provenía de vínculos personales o identidades románticas o familiares, lo que evidencia que la manipulación relacional

incrementa el impacto patrimonial del fraude; en conclusión, el estudio determinó que el fraude financiero con criptomonedas representa una evolución de las técnicas tradicionales de estafa, ahora potenciadas por redes sociales, mensajería digital, plataformas falsas y la opacidad de las criptomonedas, por lo que su prevención requiere fortalecer la educación pública, la detección temprana de patrones de contacto y la comprensión criminológica de cómo estas tecnologías crean nuevas oportunidades delictivas más costosas y difíciles de rastrear.

Yan et al. (2023) tuvieron como objetivo general:

Comprender y detectar los comportamientos de estafa en Ethereum a nivel de interacción entre nodos, a partir de la identificación de su ciclo de vida y de puntos de riesgo, para proponer un modelo automático de detección denominado Aparecium; metodológicamente, desarrollaron una investigación de enfoque cuantitativo, de carácter aplicado y nivel explicativo-tecnológico, basada en análisis de grafos, aprendizaje automático y experimentación con datos reales del ecosistema Ethereum, utilizando como fuente de información conjuntos de datos abiertos de transacciones y direcciones maliciosas extraídas de Etherscan, Cryptoscamdb y Ethplorer, modelando la red como un grafo transaccional y empleando caminatas aleatorias sesgadas, extracción de características, clasificación por random forest y evaluación mediante métricas de precisión, recall y F1-score; en los resultados generales encontraron que la capa de negocio de blockchain concentraba el 51.31 % de las pérdidas económicas globales y que los fraudes constituían el principal factor de dichas pérdidas, además de que, según el reporte de cripto-crimen 2022, las estafas ocasionaron pérdidas por 14 mil millones de dólares en 2021, duplicando los 7.8 mil millones de 2020, mientras que, de manera específica, el modelo Aparecium alcanzó una precisión de 0.977, un recall de 0.957 y un F1-score de 0.967, superando a otros métodos comparados, y adicionalmente permitió identificar un ciclo de conducta fraudulenta compuesto por cuatro etapas: recolección de cebo, explotación de la trampa, transferencia lateral y acciones para obtener ganancias, así como distinguir puntos de identificación de riesgo entre direcciones normales y direcciones maliciosas,

observándose también que el enfoque propuesto resultó escalable para grafos de gran tamaño y más eficaz que métodos tradicionales como DeepWalk, Node2Vec, GCN y GraphSAGE en la detección del fraude; en conclusión, los autores sostuvieron que el fraude en Ethereum constituye una conducta compleja, encubierta y altamente adaptable, cuya detección exige comprender su cadena operativa, sus patrones de transferencia y su estructura de interacción, por lo que el modelo Aparecium representa una herramienta eficaz para anticipar, identificar y rastrear comportamientos de estafa en entornos blockchain.

A nivel nacional

Carrero (2024) tuvo como objetivo general:

Proponer la tipificación de la modalidad del phishing en el artículo 8 de la Ley de Delitos Informáticos en el Perú; metodológicamente, desarrolló una investigación jurídica de enfoque cualitativo con método analítico, sustentada en el examen de legislación nacional y extranjera, doctrina y datos estadísticos, sin emplear cuestionario ni encuesta, sino análisis documental como técnica principal; en cuanto a los resultados generales, el autor evidenció que la regulación peruana presenta vacíos normativos frente al phishing, pese al incremento sostenido de los delitos informáticos, y de manera específica señaló que, según el Ministerio Público, al mes de noviembre de 2019 se registraron 6,906 delitos informáticos, cifra superior en 79.33 % respecto del mismo periodo de 2018, cuando se reportaron 3,851 casos, precisando además que los delitos informáticos contra el patrimonio representaron el 38.24 % del total en 2019, mientras que en 2020 se contabilizaron 8,674 delitos informáticos, de los cuales el 54.65 % correspondió a delitos contra el patrimonio, equivalentes a 4,741 hechos, añadiendo también que, conforme a fuentes internacionales citadas en la tesis, en 2020 el 34 % de los delitos informáticos estuvo vinculado al phishing y que en 2021 se reportaron más de 173 mil intentos de infección móvil orientados a la sustracción de datos personales y bancarios; asimismo, sostuvo que el avance tecnológico, el acceso masivo a internet y la falta de una previsión penal expresa favorecen la expansión de esta modalidad; en

conclusión, determinó que la incorporación del phishing en la Ley N.° 30096 es jurídicamente viable y necesaria, debido a que su ausencia normativa limita la respuesta penal frente a una conducta que afecta de forma creciente el patrimonio y los datos personales de los usuarios de medios digitales.

Mendoza (2023) tuvo como objetivo general:

Analizar la regulación del delito de estafa informática y su tipificación en el ordenamiento jurídico en el distrito fiscal de Lima Norte durante el año 2022; metodológicamente, desarrolló una investigación de enfoque cualitativo, de tipo aplicada y diseño basado en la teoría fundamentada, trabajando con participantes vinculados al Ministerio Público y utilizando como técnicas de recolección de datos el análisis de fuente documental y la entrevista, mediante una guía de entrevista como instrumento; en cuanto a los resultados generales, la autora evidenció que la legislación peruana no regula de manera expresa y adecuada la estafa informática, lo que limita la persecución penal efectiva de esta modalidad delictiva, y de forma específica identificó que, pese a existir un marco normativo compatible con el Convenio de Budapest y ciertos avances institucionales, en la práctica muchos casos no llegan a sancionarse debidamente por la falta de correcta tipificación, la imposibilidad de individualizar al ciberdelincuente, la carencia de especialistas, la escasa celeridad procesal y las limitaciones de presupuesto, logística y capacitación; además, citó que, según información del Ministerio Público referida por la Agencia Peruana de Noticias, la Fiscalía Provincial Especializada en Ciberdelincuencia de Lima Centro logró 14 sentencias por suplantación de identidad, fraude informático y estafa agravada a través de medios electrónicos, aunque ello resultaba insuficiente frente al crecimiento y complejidad del fenómeno; en conclusión, determinó que la ausencia de una correcta tipificación del delito de estafa informática genera impunidad, falta de celeridad procesal y debilidad en la investigación y sanción por parte de los operadores jurídicos, por lo que resulta necesario revisar y fortalecer la legislación penal y procesal vigente para permitir una respuesta más eficaz frente a la ciberdelincuencia.

Cobeñas (2025) tuvo como objetivo general:

Identificar en qué medida la persecución penal es eficiente durante la investigación preparatoria por delitos de fraude informático en el distrito fiscal de Lambayeque, 2024; metodológicamente, desarrolló una investigación básica con diseño mixto, aplicando en la fase cuantitativa una muestra de 372 abogados y efectivos policiales y, en la fase cualitativa, entrevistas a 6 expertos en la materia, utilizando como técnicas la encuesta, la entrevista y el análisis de información institucional vinculada al desempeño fiscal y policial; en cuanto a los resultados generales, la autora demostró que existen brechas relevantes en recursos tecnológicos, sobrecarga procesal y coordinación interinstitucional que limitan la respuesta efectiva del Ministerio Público durante la recolección y análisis de evidencias digitales, y de manera específica reportó que, según SIDPOL, en 2024 se registraron 42,000 denuncias por delitos informáticos a nivel nacional, lo que representó un incremento del 40 % respecto de 2023, mientras que en Lambayeque se consignaron 1,500 denuncias por este delito, además de evidenciar que la carga procesal, la falta de capacitación especializada, la insuficiencia de equipos tecnológicos sofisticados y las limitaciones de infraestructura afectan negativamente la actuación fiscal, aunque destacó como fortaleza el adecuado manejo de la cadena de custodia y la validación de pruebas electrónicas; en conclusión, determinó que la persecución penal por fraude informático en Lambayeque presenta deficiencias estructurales que reducen su eficiencia, por lo que resulta necesario fortalecer la formación especializada en delitos informáticos, optimizar los procesos internos y mejorar la disponibilidad de herramientas tecnológicas y forenses para responder de manera más eficaz a las exigencias del entorno digital actual.

García (2023) tuvo como objetivo general:

Determinar la relación entre la obtención fraudulenta del crédito bancario en etapa de pandemia por COVID-19 y el delito informático en Lima durante el año 2021; metodológicamente, desarrolló una investigación de enfoque cualitativo, de tipo básica pura, dentro del campo de las ciencias sociales, empleando como técnicas principales el análisis jurídico-documental y la interpretación normativa, orientadas al estudio del crédito fraudulento

bancario y su encuadre como delito informático; en cuanto a los resultados generales, el autor identificó que en el contexto de pandemia se intensificó una modalidad delictiva consistente en obtener créditos bancarios de manera fraudulenta mediante el uso de medios tecnológicos y electrónicos, aprovechando la virtualización de los servicios financieros y las restricciones presenciales, lo que generó afectaciones al sistema financiero peruano y mayores dificultades para identificar a los autores intelectuales, provocando impunidad y desconfianza social; de forma específica, sostuvo que esta conducta se articuló con una deficiente regulación del Código Penal peruano frente a nuevas formas de fraude financiero digital, evidenciándose la necesidad de mejorar el libro segundo, título X y capítulo I del Código Penal, así como fortalecer el control estatal y la supervisión de las entidades financieras, dado que la modalidad estudiada se valía de herramientas informáticas y de la interacción virtual para concretar el engaño y perjudicar tanto a ciudadanos como a instituciones; en conclusión, determinó que la obtención fraudulenta del crédito bancario durante la pandemia constituye una manifestación del delito informático, cuya regulación actual resulta insuficiente, por lo que se requiere una adecuación normativa más precisa que permita enfrentar eficazmente esta nueva modalidad de fraude financiero.

Peralta (2022) tuvo como objetivo general:

Fundamentar por qué las criptomonedas instigan los delitos de estafa perpetrados por los ciberdelincuentes en el Perú; metodológicamente, desarrolló una investigación de enfoque cualitativo, de tipo básica y diseño de teoría fundamentada, empleando como técnicas de recolección de datos la entrevista, el análisis doctrinario y el análisis normativo, mediante una guía de preguntas de entrevista y guías de análisis normativo y doctrinario, aplicadas a 10 participantes especialistas en derecho penal y constitucional, con interpretación jurídica basada en la hermenéutica; en cuanto a los resultados generales, el autor evidenció que el uso de las criptomonedas termina configurándose como un hecho doloso en el delito de estafa cuando es ejecutado por ciberdelincuentes, debido a que inducen a las víctimas a pagar con criptomonedas y no con monedas nacionales o extranjeras,

aprovechando el anonimato, la ausencia de intermediarios y la falta de regulación legal en el país; de manera específica, sostuvo que el uso del bitcoin puede facilitar fraudes en compras online por páginas publicitarias virtuales porque las transacciones se realizan en la red sin intervención directa de un administrador o tercero, mientras que el blockchain facilita el delito de estafa en el e-commerce al permitir transacciones de compra y venta en el anonimato e incluso el uso de identidades falsas, dificultando el rastreo y la recuperación del dinero por parte del agraviado; en conclusión, determinó que las criptomonedas, al no estar normadas legalmente en el Perú y operar sobre tecnologías que favorecen el anonimato, constituyen un medio idóneo para la comisión de delitos de estafa por ciberdelincuentes, por lo que resulta necesario que el Estado adecúe su regulación penal y financiera frente a esta nueva modalidad delictiva.

Nieto (2025) tuvo como objetivo general:

Analizar el lavado de activos con criptomonedas y evaluar el control estatal frente a delitos como narcotráfico, extorsión y minería ilegal en el Perú; metodológicamente, desarrolló una investigación de enfoque cualitativo, con diseño no experimental de tipo descriptivo documental y carácter teórico, empleando como técnica la guía de análisis documental para sistematizar normas, reportes de la Unidad de Inteligencia Financiera (UIF), de la Superintendencia de Banca, Seguros y AFP (SBS) y evidencia pública de casos, aplicando además el método exegético, el análisis y la síntesis, con procesamiento de la información mediante ATLAS.ti 23; en cuanto a los resultados generales, identificó que las criptomonedas facilitan el lavado de activos por su anonimato, descentralización y facilidad de transferencia internacional, precisando que este proceso se desarrolla en tres fases: colocación o introducción, estratificación mediante transferencias múltiples y mezcla de criptoactivos, e integración o reinserción de fondos como aparentemente legales; de forma específica, reportó que, entre 2014 y 2024, el tráfico ilícito de drogas registró 1283 casos con un monto involucrado de 19 541 millones de dólares, mientras que la minería ilegal presentó 780 casos, pero concentró 80 880 millones de dólares, lo que evidencia la magnitud de los flujos ilícitos canalizados mediante activos virtuales, y

además sostuvo que el Estado peruano ha mostrado avances normativos, especialmente con la Resolución SBS N.° 02648-2024 para proveedores de servicios de activos virtuales, aunque persisten vacíos regulatorios, escasa articulación institucional y limitada infraestructura tecnológica para el rastreo en blockchain; en conclusión, determinó que el lavado de activos mediante criptomonedas constituye un problema creciente que afecta la integridad financiera y la economía nacional, por lo que resulta indispensable fortalecer la regulación, la supervisión de los proveedores de servicios de activos virtuales y la coordinación nacional e internacional para prevenir y reducir este riesgo.

A nivel local

Pulache y Sandoval (2025) tuvieron como objetivo general:

> Determinar la relación entre las tecnologías emergentes y la percepción de seguridad de los clientes del BCP en Tumbes; metodológicamente, desarrollaron una investigación de tipo descriptivo correlacional, con diseño no experimental y transversal, bajo enfoque cuantitativo, trabajando con una muestra de 320 clientes del BCP en Tumbes, a quienes se les aplicó la técnica de encuesta mediante cuestionario con escala de Likert; en cuanto a los resultados generales, se evidenció que el 53 % de los encuestados ubicó a la variable tecnologías emergentes en un nivel alto, mientras que el 58 % situó a la percepción de seguridad en un nivel alto, y en la prueba inferencial se obtuvo un coeficiente Rho de Spearman de 0.954 con significancia bilateral de 0.01, lo que demostró una relación positiva muy fuerte y estadísticamente significativa entre ambas variables; de forma específica, la dimensión inteligencia artificial presentó una correlación de 0.737 con significancia menor a 0.01, la dimensión realidad aumentada mostró una correlación de 0.724 con significancia bilateral menor a 0.001, y la dimensión plataformas virtuales alcanzó una correlación de 0.807 con significancia bilateral menor a 0.001, evidenciando en todos los casos asociaciones positivas muy fuertes con la percepción de seguridad; en conclusión, los autores determinaron que la implementación de inteligencia artificial, realidad aumentada y plataformas digitales incrementa de manera

directa la confianza y la seguridad percibida por los clientes, fortaleciendo su experiencia en el uso de servicios bancarios digitales.

2.1.2 DEFINICIÓN DE TÉRMINOS BÁSICOS

Estafa

Se da cuando una persona engaña a otra persona para conseguir un beneficio económico. Esto ocurre cuando a través de algún engaño, artimaña o falsedad, se induce a la víctima a realizar un acto que le produce un prejuicio económico. En estos casos, el estafador es alguien que engaña a un tercero con la intención de hacerse con los bienes de otro (Gómez, 2023). Este tipo de conducta es considerada delito en derecho, ya que se considera un ataque a la confianza que se tiene en la sociedad y en la vida comercial. Es decir, este delito consiste en crear una situación engañosa que cause un perjuicio material a otra persona. Asimismo, se reconoce que este ilícito ha evolucionado hacia entornos digitales, ampliando su alcance y complejidad (Enríquez-Chapi et al., 2024)

Estafa informática

Es un tipo de estafa cometido a través de medios electrónicos o digitales, como la computadora, internet o el móvil.

Bajo esta forma de estafa, los estafadores utilizan métodos más sofisticados como phishing, malware o ingeniería social, a fin de engañar a un individuo y conseguir las claves, números de tarjeta, además de robar los datos como nombres, apellidos, tal vez correos electrónicos (Ayala Medina, 2024). Se utilizan estos datos luego para realizar fraudes financieros o robos de identidad. En el caso de una estafa informática, se pueden ocasionar grandes problemas a las personas naturales y jurídicas. Asimismo, este tipo de delito ha evolucionado en complejidad debido al uso de tecnologías digitales avanzadas que dificultan su detección y persecución (Federal Bureau of Investigation, 2023).

Sistemas de inversión online

Las plataformas de inversión son herramientas disponibles en Internet que permiten a los usuarios realizar inversiones a través de redes. Estos sistemas ofrecen diversas oportunidades de inversión en acciones, bonos, fondos de inversión, criptomonedas y otros productos financieros (Cabrera Soto & Lage Codorniu, 2022). Los usuarios pueden conectarse en cualquier lugar que tenga acceso a Internet cómodamente. No obstante, pueden conllevar riesgos como la volatilidad del mercado, la probabilidad de que se pierdan todos o parte de los fondos, la exposición a riesgos de seguridad cibernética, incluida la ESTAFA, la probabilidad de cometer errores de inversión, el riesgo de liquidez, etc. Asimismo, se advierte que los mercados de criptomonedas presentan altos niveles de incertidumbre y riesgo que pueden afectar a los inversionistas (Kılcı & Yılancı, 2025).

Phishing

Se trata de la forma que utilizan los delincuentes por la cual intentan obtener información sensible, desde contraseñas hasta datos de tarjetas, o datos privados, por ejemplo, suplantando a entidades legítimas y de confianza, como bancos, empresas o administraciones públicas (Phillips & Wilder, 2022). Normalmente, el phishing se lleva a cabo a través de correos, mensajes por diversas plataformas como WhatsApp, Telegram entre otras, así como por medio de llamadas telefónicas, o una página web que simule ser verdadera.

Asimismo, reportes internacionales evidencian que estas modalidades de fraude digital continúan en incremento y afectan a millones de usuarios a nivel global (Federal Trade Commission, 2023).

Transferencias falsas

También llamadas estafas de transferencia, se basa en engañar a una persona, realizando una transferencia de dinero a partir con información falsa o falsa. Esto incluye el envío de comprobantes de pago alterados para que pareciera una transacción exitosa (Ayala, 2024). Lo que indujo a la víctima a creer que recibió el pago. Asimismo, este tipo de fraude se vincula con modalidades de engaño digital

que afectan directamente la confianza en los sistemas de pago electrónicos (Federal Trade Commission, 2023).

Comercio electrónico fraudulento

Implica la realización de actividades fraudulentas en el ámbito del comercio electrónico, como el uso de plataformas en línea para estafar a consumidores o crear páginas web para robar las credenciales de pago de los usuarios (Amaya, 2024). Esto se puede traducir en la disponibilidad comercialización, ya sea venta de productos o servicios falsos, no recibidos o de baja calidad en comparación con lo prometido. Asimismo, este tipo de fraude se ha incrementado con el uso de tecnologías digitales y plataformas virtuales, afectando la confianza en el comercio electrónico (Federal Trade Commission, 2023).

Criptomonedas

Son monedas que al ser virtuales y al utilizar la tecnología blockchain y de la criptografía garantizan la seguridad de las transacciones. Por este motivo, teniendo en cuenta que monedas tradicionales, como el dólar o el euro están reguladas, las criptomonedas no se encuentran refrendadas por ningún estado o autoridad central, sino que operan en una red descentralizada de computadoras (Cabrera Soto & Lage Codorniu, 2022). Es imperativo mencionar que las criptomonedas también pueden ser inestables y están vinculadas a riesgos, como la especulación del mercado, la falta de normatividad legal vigente que las regule y la probabilidad que pueden ser utilizadas en actividades ilícitas.

Como tal, es fundamental comprender cómo funcionan y tomar precauciones al usarlas. Asimismo, diversos estudios advierten que estos activos presentan altos niveles de riesgo e incertidumbre en los mercados financieros (Rojas Rincón, 2024).

Bitcoin

Fue desarrollada en 2009 bajo el seudónimo de Satoshi Nakamoto, y es la criptomoneda más conocida. Funciona como una forma de dinero digital

descentralizado, esto quiere decir, que ninguna organización central o gobierno lo apoya o refrenda (López Rivera, 2023). El precio inicial del Bitcoin en sus primeros días de operaciones en 2009 era prácticamente insignificante, ya que no había un mercado establecido para determinar su valor. De hecho, en sus primeras transacciones, se vendieron por apenas unos centavos o incluso menos. El precio de Bitcoin ha experimentado varios aumentos y descensos bruscos a lo largo del tiempo. En la actualidad, su precio ha oscilado alrededor de varios miles de dólares estadounidenses. Asimismo, estudios económicos evidencian la alta volatilidad del Bitcoin y su comportamiento especulativo en los mercados financieros (Demmler, 2023).

Ether

Esta moneda es exclusiva de la plataforma Ethereum. Funciona como una forma de dinero digital utilizada para realizar transacciones, pagar tarifas de transacción y ejecutar contratos inteligentes en la red Ethereum (De Senna & Souza, 2023). Ether es descentralizado y se basa en tecnología blockchain, lo que implica que se realicen registros y certificaciones de las transacciones de forma segura en una red distribuida de computadoras. Asimismo, estudios recientes destacan el papel de las criptomonedas como Ethereum en la evolución de los sistemas financieros digitales y su integración en nuevas tecnologías (Barrutia et al., 2023).

Litecoin

En 2011, Charlie Lee, un ex desarrollador de Google, creó la criptomoneda, que es de código abierto y descentralizada (Cabrera & Lage, 2022). Se desarrolló como una alternativa más rápida y eficiente a Bitcoin, con el objetivo de mejorar algunas de las limitaciones percibidas de la primera criptomoneda.

Asimismo, estudios sobre el mercado de criptomonedas destacan la aparición de nuevas monedas digitales como respuesta a las limitaciones técnicas y de escalabilidad de Bitcoin (Demmler & Fernández, 2022).

III. MATERIALES Y MÉTODOS

3.1 TIPO Y DISEÑO DE INVESTIGACIÓN

3.1.1 TIPO DE INVESTIGACIÓN

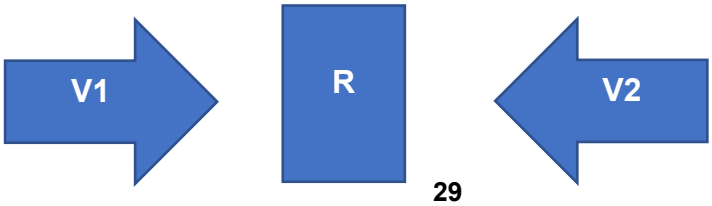
La naturaleza de este estudio fue de enfoque cuantitativo que se alinea con un enfoque dogmático jurídico; en donde se analizó la doctrina jurídica comparada. La dogmática jurídica es aquella ciencia o rama que dentro del ámbito del derecho estudia de forma sistemática y crítica las normas jurídicas, así como de los principios y conceptos que las fundamentan. Su objetivo principal fue analizar y comprender el derecho en su totalidad, incluyendo su estructura, contenido, evolución histórica, interpretación y aplicación.

La dogmática jurídica se dedica a analizar minuciosamente las estructuras legales, aunque lo hace de manera abstracta, sin considerar su aplicación concreta en la vida real (Tantaleán, 2016).

3.1.2 DISEÑO DE INVESTIGACIÓN

El diseño fue “no experimental”; esto permitió examinar la relación entre las variables y determinar si existe una asociación entre el delito de estafa informática y el uso de criptomonedas; además, se compararon diferentes casos o grupos en relación con estas variables para identificar posibles patrones o diferencias significativas.

Este modelo de diseño que surge en investigaciones sistemáticas en las cuales el investigador no tiene influencia sobre las variables independientes, ya sea porque los eventos ya han ocurrido o porque son intrínsecamente controlables.
Se evidenció a través del siguiente esquema:



M:

Leyenda:

M: Se refiere a la muestra utilizada en la investigación.
V1: Delito de estafa informática.
V2: Criptomonedas.
R: Posible relación.

Donde:

M: Se refiere a la muestra utilizada en la investigación.
O1: Se trata de la observación de la variable X, que en este caso es el Delito de Estafa Informática.
O2: Se refiere a la observación de la variable Y, la cual en este contexto son las Criptomonedas.
R: Es el grado de relación entre ambas variables.

3.2 POBLACIÓN, MUESTRA Y MUESTREO

3.2.1 POBLACIÓN

La investigación que se presenta a continuación aborda diversos temas que delimitan su alcance y contexto. En primer lugar, con relación al universo físico, al ser un estudio dogmático, no se definió un ámbito geográfico específico, lo que permitió que la mirada fuera más amplia y general. Por otra parte, el universo social se centró en los profesionales del derecho y juristas, que fueron objeto de estudio. Para finalizar con el universo temporal, en el transcurso del año 2023 se desarrolló la presente investigación. La combinación de estos tres aspectos definió el marco y el alcance de esta investigación.

3.2.2 MUESTRA

Para la obtención de la información se utilizó un enfoque no probabilístico; es decir, no se empleó un método aleatorio en la selección de las muestras. La técnica de

muestreo que se aplicó fue la intencional, considerándose la más adecuada para el caso. Esto se debe a que es un método de muestreo no probabilístico que recopila información de una población específica intencionalmente.

Juntamente con la doctrina, la jurisprudencia penal y la normativa, otras fuentes que sirvieron para recolectar información y la debida utilización, fue el marco muestral. Esta fusión de elementos metodológicos cimentó la investigación realizada y su desarrollo sistemático.

3.3 TÉCNICAS E INSTRUMENTOS PARA OBTENER INFORMACIÓN, ASÍ COMO LA PRECISIÓN Y LA FIABILIDAD DE LOS DATOS RECOPILADOS.

Las metodologías para obtener información pueden estar presentadas de diversas formas las cuales pueden ser clasificadas y aplicadas de muchas maneras, Arias (2012). En este sentido, la observación sistemática y fiable de acciones o comportamientos permite la obtención de datos o información clara, precisa y consistente. Estos enfoques metodológicos son prácticos para la obtención información y para el filtrado de investigación. En este estudio para el propósito de recopilar datos sobre las variables y dimensiones, se utilizaron las técnicas e instrumentos que se enumeran a continuación:

3.3.1 TÉCNICAS

Se utilizó la encuesta con la finalidad de captar datos y examinar ambas variables materia de investigación como la relación existente entre ambas. Este método se consideró eficaz y útil para obtener información sobre los temas materia de investigación.

Arias (2012), refiere que cuanto a la encuesta es un método que busca obtener datos aportados por un grupo o muestra de personas sobre sí mismo o sobre determinado asunto.

3.3.2 INSTRUMENTOS

Se utilizó como instrumento el cuestionario para recoger información, el cual busca ayudar con la relación entre las dos variables “Delito de Estafa Informática” y “Criptomonedas”. Esta herramienta permitió obtener información detallada y directa de los encuestados lo que permitió tener más detalles que antes no teníamos.

3.3.3 VALIDEZ

La estrategia de “Juicio de expertos” se utilizó para validar la forma, el contenido y la estructura de los instrumentos de la investigación. Se ha contado con expertos en la materia que revisaron el proceso aportando sus criterios para garantizar la calidad de la presente investigación.

3.3.4 CONFIABILIDAD

La confiabilidad del instrumento se determinó mediante el coeficiente Alfa de Cronbach, con el propósito de evaluar la consistencia interna de los ítems empleados en la recolección de datos. Como resultado, se obtuvo un valor de 0,81, lo que evidencia un nivel de confiabilidad muy alto, confirmando la viabilidad y estabilidad del instrumento para su aplicación en la investigación. Para ello, el cuestionario fue sometido a una prueba piloto aplicada a 50 operadores del derecho pertenecientes a diversas instituciones, entre ellas el Colegio de Abogados de Tumbes, el Ministerio Público y el Poder Judicial de Tumbes. En consecuencia, se determinó que el instrumento presenta condiciones adecuadas de confiabilidad y validez para medir las variables del estudio.

Tabla 1: *Interpretación del coeficiente de confiabilidad*

Rango	Nivel de confiabilidad
0,81 a 1,00	Muy alta
0,61 a 0,80	Alta
0,41 a 0,60	Moderada
0,21 a 0,40	Baja

Rango	Nivel de confiabilidad
0,01 a 0,20	Muy baja

Nota. Adaptado de Palella y Martins (2006).

3.4 PROCEDIMIENTO

El procedimiento de recolección y análisis de datos se desarrolló de manera secuencial y ordenada. En una primera etapa, se diseñó el instrumento de recolección de datos en función de las variables, dimensiones e indicadores establecidos en la matriz de consistencia. Posteriormente, dicho instrumento fue aplicado a la muestra seleccionada mediante herramientas tecnológicas de encuesta, lo que permitió recopilar la información necesaria de forma sistemática y uniforme. Una vez obtenidos los datos, estos fueron organizados, codificados y registrados en una base de datos para facilitar su procesamiento estadístico.

En la fase de procesamiento, la información recolectada fue revisada previamente para verificar su integridad, consistencia y pertinencia con los objetivos de la investigación. Luego, se realizó la tabulación de los datos y su representación en tablas estadísticas, lo que permitió describir el comportamiento de las variables de estudio. Para el análisis descriptivo se emplearon frecuencias absolutas, frecuencias relativas y porcentajes; asimismo, cuando correspondió, se utilizaron medidas de tendencia central para resumir la distribución de los datos obtenidos. Este tratamiento permitió caracterizar los resultados de manera clara y objetiva.

En el análisis inferencial se utilizó la prueba Tau-b de Kendall, debido a que las variables fueron medidas en escala ordinal y el propósito del estudio fue determinar la relación existente entre ellas. Este coeficiente permitió establecer tanto la dirección como la intensidad de la asociación entre las variables analizadas. Su valor oscila entre -1 y +1, donde los coeficientes cercanos a 0 indican ausencia o debilidad de relación, mientras que los valores próximos a +1 evidencian una relación positiva fuerte y los valores cercanos a -1 una relación negativa fuerte. En esa línea, para la interpretación de la magnitud de la correlación se consideró que los valores entre 0.00 y 0.19 reflejan una relación muy débil; entre 0.20 y 0.39, débil;

entre 0.40 y 0.59, moderada; entre 0.60 y 0.79, fuerte; y entre 0.80 y 1.00, muy fuerte; manteniéndose el mismo criterio cuando la correlación sea negativa, pero en sentido inverso (Hernández et al., 2014).

Para la interpretación de la magnitud y dirección de la relación entre las variables, se consideró el criterio expuesto en la siguiente tabla, adaptado al coeficiente Tau-b de Kendall.

Tabla 2: *Interpretación de la magnitud y dirección del coeficiente Tau-b de Kendall*

Valor del coeficiente Tau-b	Dirección e intensidad de la relación
-1.00 a -0.80	Relación negativa muy fuerte
-0.79 a -0.60	Relación negativa fuerte
-0.59 a -0.40	Relación negativa moderada
-0.39 a -0.20	Relación negativa débil
-0.19 a -0.01	Relación negativa muy débil
0.00	Ausencia de relación
0.01 a 0.19	Relación positiva muy débil
0.20 a 0.39	Relación positiva débil
0.40 a 0.59	Relación positiva moderada
0.60 a 0.79	Relación positiva fuerte
0.80 a 1.00	Relación positiva muy fuerte

Nota. Elaboración propia. Adaptado de Hernández-Sampieri et al. (2014) para fines de interpretación correlacional en variables ordinales.

La contrastación de hipótesis se efectuó con base en el nivel de significancia estadística establecido para la investigación. En ese sentido, se consideró que existía evidencia suficiente para aceptar la hipótesis de investigación cuando el valor de significancia fue menor que 0.05; en caso contrario, se aceptó la hipótesis nula. De esta manera, el análisis no solo permitió describir los datos obtenidos, sino también establecer inferencias respecto de la relación entre las variables, en concordancia con el enfoque cuantitativo y el nivel correlacional del estudio.

3.5 MÉTODO DE ANÁLISIS DE DATOS

Se usaron técnicas de estadística inferencial a fin de procesar los datos en sus estadísticas descriptivas y en contrastar las hipótesis mediante el programa SPSS versión 25. Igualmente se aplicó la versión 25 para realizar los exámenes de las teorías con la medida de asociación entre variables Tau-b Rho de Kendall. Se pudo utilizar el uso de técnicas inferenciales con el fin de conocer cuál es el grado de correlación que existe entre el delito de Estafa Informática y las Criptomonedas.

3.6 ASPECTOS ÉTICOS

El investigador tuvo en cuenta varias cuestiones éticas fundamentales en la presente tesis. En primer lugar, que se respete en el estudio, la importancia de todos los participantes y también estos no sean en ningún modo discriminados por su origen, raza, sexo, ni de otra índole. Igualmente, se impide y no se aceptará en ninguna etapa la segregación. Además, se garantizará la integridad de los resultados en cualquier fase de recolección y análisis de datos. Se apoya un entorno seguro y confidencial donde los participantes pueden expresar sus opiniones con total libertad, regido por protección y seguridad de datos. Igualmente, se tiene en cuenta la propiedad intelectual y la normativa de derechos de autor de forma que se cumple la normativa que les corresponde en los marcos de investigación. Estas consideraciones éticas son fundamentales para garantizar la integridad, la confiabilidad y el respeto hacia todos los involucrados en el estudio.

3.7 OPERACIONALIZACIÓN DE VARIABLES

Variable Independiente: Delito de estafa informática

En comparación con otras formas de delito, el objetivo principal del delito de estafa informática es obtener beneficios ilícitos mediante el engaño y la manipulación de personas a través de medios electrónicos o informáticos.

Paralelo al delito de estafa regulado por nuestro ordenamiento jurídico en el Código Penal Peruano artículo 196.

En el Perú hay una regulación efectiva y actualizada que aborde directamente la estafa informática en su totalidad. Se puede citar la opinión del profesor BALMACEDA HOYOS, quien señala que, dada la evolución de los medios tecnológicos informáticos, así como la naturaleza especial y transfronteriza de este tipo de delitos, y ante la ausencia de un marco legal específico, solo se podría aplicar la legislación existente sobre el delito de estafa en su forma convencional. Según este autor, las estafas cometidas a través de medios informáticos podrían ser sancionadas bajo esta figura, pero subraya la necesidad imperiosa de contar con una legislación adaptada a la era digital.

Variable dependiente: Criptomonedas

El pilar fundamental de la nueva sociedad de la información es, sin lugar a duda el Internet. El ciberespacio, es de acceso fácil a todas las personas, se puede utilizar por todos para ejecutar un sinfín de transacciones y comunicaciones. En general, se usa para fines legítimos o positivos que serán de utilidad para el hombre. No obstante, las personas consiguen hacer uso de ello para su propio beneficio a veces incluso de forma ilegal.

3.8 HIPÓTESIS

Hipótesis general

H.1: Existe relación estadísticamente significativa entre el delito de estafa informática y las criptomonedas en el Perú, 2023.

Hipótesis específicas

H.E.$_1$: Existe relación estadísticamente significativa entre los sistemas de inversión online y las criptomonedas en el Perú, 2023.

H.E.$_2$: Existe relación estadísticamente significativa entre el phishing y las criptomonedas en el Perú, 2023.

H.E.$_3$: Existe relación estadísticamente significativa entre las transferencias falsas y las criptomonedas en el Perú, 2023.

H.E.$_4$: Existe relación estadísticamente significativa entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023.

IV. RESULTADOS Y DISCUSIÓN

4.1 RESULTADOS INFERENCIALES

Objetivo general: Determinar la relación entre el delito de estafa informática y las criptomonedas en el Perú, 2023.

Hipótesis general:

H_1: Existe relación estadísticamente significativa entre el delito de estafa informática y las criptomonedas en el Perú, 2023.

Tabla 3: *Nivel de correlación entre el delito de estafa informática y las criptomonedas en el Perú, 2023*

		Criptomonedas en el Perú
Delito de estafa informática	τb	0.309*
	p-valor	0.003

Nota: *Extraído del programa SPSS*

La Tabla 3 evidencia que entre el delito de estafa informática y las criptomonedas en el Perú, 2023, existe una relación positiva débil y estadísticamente significativa, debido a que se obtuvo un coeficiente τb = 0.309, valor que, de acuerdo con el baremo de interpretación, se ubica en un nivel de asociación débil. Asimismo, el p-valor = 0.003 es menor al nivel de significancia establecido (0.05), lo que indica que la relación encontrada no es producto del azar. En consecuencia, se acepta la

hipótesis general de investigación, concluyéndose que el delito de estafa informática se relaciona de manera significativa con las criptomonedas en el Perú, 2023; no obstante, la intensidad de dicha relación es baja, lo que permite inferir que, aunque ambas variables presentan asociación, esta no se manifiesta con alta fuerza.

Objetivo específico 1: Determinar la relación entre los sistemas de inversión online y las criptomonedas en el Perú, 2023.

Hipótesis especifica 1:

H_1: Existe relación estadísticamente significativa entre los sistemas de inversión online y las criptomonedas en el Perú, 2023.

Tabla 4: *Nivel de correlación entre los sistemas de inversión online y las criptomonedas en el Perú, 2023.*

		Criptomonedas en el Perú
Sistemas de inversión online	τb	0.308*
	p-valor	0.001

Nota: *Extraído del programa SPSS*

La Tabla 4 evidencia que, entre los sistemas de inversión online y las criptomonedas en el Perú, 2023, existe una relación positiva débil y estadísticamente significativa, dado que se obtuvo un coeficiente τb = 0.308, valor que, según el baremo de interpretación, corresponde a una asociación débil. Del mismo modo, el p-valor = 0.001 es menor al nivel de significancia de 0.05, lo que demuestra que la relación encontrada no es producto del azar. En consecuencia, se acepta la hipótesis específica 1 de investigación, concluyéndose que los sistemas de inversión online se relacionan de manera significativa con las criptomonedas en el Perú, 2023; sin embargo, la intensidad de dicha relación es baja, lo que indica que la asociación entre ambas variables existe, aunque no con elevada fuerza.

Objetivo específico 2: Determinar la relación entre el phishing y las criptomonedas en el Perú, 2023.

Hipótesis especifica 2:

H_2: Existe relación estadísticamente significativa entre el phishing y las criptomonedas en el Perú, 2023.

Tabla 5: *Nivel de correlación entre el phishing y las criptomonedas en el Perú, 2023.*

		Criptomonedas en el Perú
Phishing	τb	0.201*
	p-valor	0.001

Nota: *Extraído del programa SPSS.*

La Tabla 5 evidencia que, entre el phishing y las criptomonedas en el Perú, 2023, existe una relación positiva débil y estadísticamente significativa, puesto que se obtuvo un coeficiente τb = 0.201, valor que, según el baremo de interpretación, corresponde a una asociación débil. Asimismo, el p-valor = 0.001 es menor al nivel de significancia de 0.05, lo que demuestra que la relación observada no es producto del azar. En consecuencia, se acepta la hipótesis específica 2 de investigación, concluyéndose que el phishing se relaciona de manera significativa con las criptomonedas en el Perú, 2023; sin embargo, la intensidad de dicha relación es baja, lo que indica que la asociación entre ambas variables existe, aunque con escasa fuerza.

Objetivo específico 3: Determinar la relación entre las transferencias falsas y las criptomonedas en el Perú, 2023.

Hipótesis especifica 3:

H_3: Existe relación estadísticamente significativa entre las transferencias falsas y las criptomonedas en el Perú, 2023.

Tabla 6: *Nivel de correlación entre las transferencias falsas y las criptomonedas en el Perú, 2023.*

		Criptomonedas en el Perú
Transferencias falsas	τb	0.304*
	p-valor	0.003

Nota. *Extraído del programa SPSS.*

La Tabla 6 evidencia que, entre las transferencias falsas y las criptomonedas en el Perú, 2023, existe una relación positiva débil y estadísticamente significativa, dado que se obtuvo un coeficiente τb = 0.304, valor que, de acuerdo con el baremo de interpretación, corresponde a una asociación débil. Asimismo, el p-valor = 0.003 es menor al nivel de significancia de 0.05, lo que demuestra que la relación observada no es producto del azar. En consecuencia, se acepta la hipótesis específica 3 de investigación, concluyéndose que las transferencias falsas se relacionan de manera significativa con las criptomonedas en el Perú, 2023; sin embargo, la intensidad de dicha relación es baja, lo que indica que la asociación entre ambas variables existe, aunque con limitada fuerza.

Objetivo específico 4: Determinar la relación entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023.

Hipótesis especifica 4:

H_4: Existe relación estadísticamente significativa entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023.

Tabla 7: *Nivel de correlación entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023.*

Tau de Kendall

		Criptomonedas en el Perú
Comercio electrónico fraudulento	τb	0.305*
	p-valor	0.008

Nota. *Extraído del programa SPSS.*

La Tabla 7 evidencia que, entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023, existe una relación positiva débil y estadísticamente significativa, debido a que se obtuvo un coeficiente τb = 0.305, valor que, de acuerdo con el baremo de interpretación, corresponde a una asociación débil. Asimismo, el p-valor = 0.008 es menor al nivel de significancia de 0.05, lo que demuestra que la relación encontrada no se debe al azar. En consecuencia, se acepta la hipótesis específica 4 de investigación, concluyéndose que el comercio electrónico fraudulento se relaciona de manera significativa con las criptomonedas en el Perú, 2023; sin embargo, la intensidad de dicha relación es baja, lo que indica que la asociación entre ambas variables existe, aunque no con elevada fuerza.

4.2 DISCUSIÓN

La estafa informática es entendida como una modalidad delictiva que traslada el engaño tradicional al entorno digital mediante el uso de medios electrónicos, plataformas virtuales y herramientas tecnológicas para producir un perjuicio patrimonial. Por su parte, las criptomonedas son activos digitales caracterizados por la descentralización, el anonimato relativo y la rapidez en las transferencias, elementos que, aunque responden a una lógica de innovación financiera, también pueden ser aprovechados por ciberdelincuentes en entornos de escasa regulación. En la tabla 3, se distingue un coeficiente de correlación positiva débil de Tau-b de Kendall de 0.309 entre el delito de estafa informática y las criptomonedas, con una significancia de 0.003 < 0.05, aceptándose la hipótesis alterna. Este hallazgo evidencia que existe una relación estadísticamente significativa entre ambas variables, aunque con intensidad reducida. En los reportes de Wang y Deng (2026), se identificó que en víctimas de fraude de inversión con criptomonedas la actitud de participación y el control conductual percibido influyeron positivamente en la intención de inversión, observándose correlaciones de r = 0.559 entre actitud y control conductual, y de r = 0.500 entre regulación y educación en inversión, lo que demuestra que los entornos de fraude con criptoactivos se sostienen sobre valoraciones cognitivas y percepciones individuales. Asimismo, Dulisse et al. (2025) hallaron que las plataformas de trading fraudulentas representaron el 41.1 % de los casos y las estafas tipo pig butchering el 27 %, concentrando más de dos tercios

de los fraudes analizados en 291 denuncias. Del mismo modo, Yan et al. (2023) reportaron que en Ethereum las estafas ocasionaron pérdidas por 14 mil millones de dólares en 2021, duplicando los 7.8 mil millones de 2020, y que su modelo de detección alcanzó una precisión de 0.977, un recall de 0.957 y un F1-score de 0.967, confirmando la complejidad del fraude en entornos blockchain. Los hallazgos de los autores descritos son semejantes a los encontrados en la presente investigación, ya que permiten sostener que las criptomonedas no originan directamente la estafa informática, pero sí constituyen un medio funcional que facilita su ejecución al combinar anonimato, velocidad operativa y dificultades de rastreo. En consecuencia, se infiere que la débil correlación hallada en el estudio no minimiza el fenómeno, sino que revela que la estafa informática vinculada a criptoactivos depende también de factores normativos, institucionales y tecnológicos que aún presentan importantes vacíos en el Perú.

Los sistemas de inversión online son concebidos como plataformas digitales que ofrecen oportunidades de colocación de capital en productos financieros, acciones, fondos o criptoactivos, pero también pueden convertirse en canales de fraude cuando operan bajo apariencias de legalidad y ausencia de control efectivo. En la tabla 4, se distingue un coeficiente de correlación positiva débil de Tau-b de Kendall de 0.308 entre los sistemas de inversión online y las criptomonedas, con una significancia de 0.001 < 0.05, aceptándose la hipótesis alterna. Este resultado permite afirmar que existe una relación estadísticamente significativa entre ambas variables. En el estudio de Wang y Deng (2026), se reportó que la investigación fue aplicada a 287 víctimas válidas de fraude de inversión con criptomonedas y que el modelo presentó una varianza acumulada explicada de 78.169 %, con valores de AVE entre 0.609 y 0.760, además de fiabilidad compuesta entre 0.884 y 0.941, lo que demostró solidez estadística en la relación entre factores cognitivos y la intención de inversión fraudulenta. Del mismo modo, en Dulisse et al. (2025) se observó que el 18.9 % de los casos parecían haber sido iniciados por la propia víctima al ingresar a sitios de inversión o plataformas de trading, mientras que las plataformas fraudulentas de inversión constituyeron la modalidad más frecuente del fraude con criptomonedas. En esa misma orientación, Peralta (2022) concluyó doctrinariamente que el uso de las criptomonedas se convierte en un hecho doloso en el delito de estafa, en la medida en que induce al pago en criptoactivos, dificulta

la recuperación del dinero y se beneficia de la falta de regulación nacional. Los hallazgos de los estudios citados son similares a los obtenidos en esta investigación, puesto que evidencian que los sistemas de inversión online se vinculan con las criptomonedas como espacios donde se construye confianza aparente, se ofrecen beneficios ilusorios y se reduce la percepción de riesgo del usuario. Por ello, se puede interpretar que, aunque la correlación encontrada fue débil, los sistemas de inversión online funcionan como un escenario de captación especialmente sensible cuando confluyen opacidad regulatoria, deficiente educación financiera y ausencia de supervisión tecnológica especializada.

El phishing se entiende como una modalidad de fraude digital orientada a obtener datos personales, bancarios o claves de acceso mediante engaño, suplantación de identidad o manipulación de interfaces tecnológicas, para luego disponer de recursos económicos o activos digitales de la víctima. En la tabla 5, se distingue un coeficiente de correlación positiva débil de Tau-b de Kendall de 0.201 entre el phishing y las criptomonedas, con una significancia de 0.001 < 0.05, aceptándose la hipótesis alterna. Aunque esta fue la correlación más baja de las dimensiones analizadas, sigue siendo estadísticamente significativa, lo que confirma la existencia de una asociación entre ambas variables. En la investigación de Carrero (2024), se señaló que en el Perú, hasta noviembre de 2019, se registraron 6,906 delitos informáticos, cifra superior en 79.33 % a los 3,851 casos reportados en 2018, y que en 2020 se contabilizaron 8,674 delitos informáticos, de los cuales el 54.65 %, equivalentes a 4,741 hechos, correspondieron a delitos contra el patrimonio. Asimismo, el mismo autor indicó que el 34 % de los delitos informáticos estuvo vinculado al phishing y que en 2021 se reportaron más de 173 mil intentos de infección móvil orientados al robo de datos personales y bancarios. Por su parte, Yan et al. (2023) identificaron que el phishing era la segunda causa de pérdida dentro de la capa de negocio blockchain, por detrás de las estafas directas, y reportaron que el fraude y el phishing forman parte del mismo ecosistema criminal en Ethereum. Los hallazgos de ambos estudios son coherentes con los resultados de la presente investigación, ya que evidencian que el phishing actúa como un mecanismo de acceso o facilitación que luego puede desembocar en operaciones con criptomonedas, especialmente cuando el usuario es inducido a revelar claves o interactuar con plataformas falsas. En esa línea, se sugiere que la relación débil

encontrada en esta tesis responde a que el phishing no necesariamente culmina siempre en fraude con criptoactivos, pero sí se configura como una puerta de entrada relevante dentro del circuito delictivo digital.

Las transferencias falsas pueden comprenderse como maniobras engañosas que simulan operaciones económicas válidas con la finalidad de inducir error en la víctima, generando la apariencia de pago, envío o recepción de fondos que en realidad no se ha materializado de forma legítima. En la tabla 6, se distingue un coeficiente de correlación positiva débil de Tau-b de Kendall de 0.304 entre las transferencias falsas y las criptomonedas, con una significancia de 0.003 < 0.05, aceptándose la hipótesis alterna. Este resultado evidencia que ambas variables se relacionan de manera significativa. En la tesis de García (2023), se concluyó que durante la pandemia la obtención fraudulenta de crédito bancario se intensificó mediante el uso de medios tecnológicos y entornos virtuales, favorecida por la dificultad para identificar a los autores intelectuales y por la deficiente regulación penal frente a nuevas formas de fraude digital. Asimismo, Nieto (2025) reportó que entre 2014 y 2024 el tráfico ilícito de drogas registró 1,283 casos con 19,541 millones de dólares involucrados, mientras que la minería ilegal presentó 780 casos, pero concentró 80,880 millones de dólares, lo que evidencia la magnitud de los flujos ilícitos movilizados mediante activos virtuales y mecanismos de difícil rastreo. A ello se suma Cobeñas (2025), quien reportó que en 2024 se registraron 42,000 denuncias por delitos informáticos a nivel nacional, lo que representó un incremento del 40 % respecto de 2023, además de consignarse 1,500 denuncias en Lambayeque, evidenciándose limitaciones tecnológicas, sobrecarga procesal y falta de capacitación especializada. Los hallazgos de estos autores son semejantes a los encontrados en esta investigación, ya que muestran que las transferencias falsas encuentran en los entornos digitales y en los activos virtuales un medio operativo que favorece la simulación, el desplazamiento de fondos y la dificultad de verificación posterior. Por tanto, se interpreta que la relación hallada se explica no solo por el uso técnico de las criptomonedas, sino por la debilidad institucional para rastrear de forma eficiente operaciones simuladas o engañosas.

El comercio electrónico fraudulento es conceptualizado como aquella práctica engañosa realizada en entornos digitales de compraventa, en la que se induce al

usuario a pagar por bienes o servicios inexistentes, alterados o no entregados, aprovechando la confianza depositada en plataformas, redes sociales o páginas web que aparentan legitimidad. En la tabla 7, se distingue un coeficiente de correlación positiva débil de Tau-b de Kendall de 0.305 entre el comercio electrónico fraudulento y las criptomonedas, con una significancia de 0.008 < 0.05, aceptándose la hipótesis alterna. Este hallazgo demuestra que existe una relación significativa entre ambas variables. En el estudio de Peralta (2022), se concluyó que el uso del bitcoin facilita los fraudes en compras online porque la transacción en páginas virtuales no requiere la presencia de un intermediario o administrador, lo que favorece el anonimato del ciberdelincuente. Asimismo, dicho autor sostuvo que el blockchain facilita el delito de estafa en el e-commerce porque permite transacciones anónimas y la utilización de identidades falsas. Por otro lado, el antecedente local de Pulache y Sandoval (2025) reportó que en Tumbes el 53 % de los encuestados ubicó a las tecnologías emergentes en nivel alto y el 58 % a la percepción de seguridad en nivel alto; adicionalmente, hallaron una correlación de Rho = 0.954 entre tecnologías emergentes y percepción de seguridad, y de Rho = 0.807 entre plataformas digitales y percepción de seguridad, ambas con significancia inferior a 0.001. Aunque este estudio local no analizó fraude, sí evidencia que las plataformas digitales generan altos niveles de confianza en los usuarios, lo que puede convertirse en una condición de vulnerabilidad cuando dichas plataformas son utilizadas con fines fraudulentos. En consecuencia, los hallazgos de los autores citados son semejantes a los obtenidos en esta tesis, pues permiten sostener que el comercio electrónico fraudulento se relaciona con las criptomonedas no solo por el medio de pago, sino por el aprovechamiento de la confianza digital del usuario, la apariencia de legitimidad y la limitada posibilidad de reversión o recuperación del dinero una vez consumada la operación.

V. CONCLUSIONES

1. Se determinó que existe una relación positiva débil y estadísticamente significativa entre el delito de estafa informática y las criptomonedas en el Perú, 2023, al obtenerse un coeficiente τb = 0.309 y un p-valor = 0.003, lo que permitió aceptar la hipótesis general de investigación. En ese sentido, se concluye que las criptomonedas se vinculan con la estafa informática como un medio que puede facilitar la ejecución de conductas fraudulentas en entornos digitales, especialmente por su anonimato relativo, limitada trazabilidad y débil regulación normativa.

2. Se evaluó la relación entre los sistemas de inversión online y las criptomonedas en el Perú, 2023, identificándose una relación positiva débil y significativa, con un coeficiente τb = 0.308 y un p-valor = 0.001. Por ello, se concluye que los sistemas de inversión online guardan asociación con el uso de criptomonedas en escenarios donde la apariencia de legalidad, la promesa de rentabilidad y la limitada supervisión pueden facilitar mecanismos de captación engañosa.

3. Se estableció la relación entre el phishing y las criptomonedas en el Perú, 2023, encontrándose una relación positiva débil y estadísticamente significativa, con un coeficiente τb = 0.201 y un p-valor = 0.001. En consecuencia, se concluye que el phishing constituye una modalidad que se asocia con las criptomonedas al servir como vía de acceso a datos personales, credenciales o recursos digitales que luego pueden ser utilizados en operaciones fraudulentas.

4. Se identificó la conexión entre las transferencias falsas y las criptomonedas en el Perú, 2023, evidenciándose una relación positiva débil y significativa, con un coeficiente τb = 0.304 y un p-valor = 0.003. Por tanto, se concluye que las criptomonedas se relacionan con las transferencias falsas al facilitar operaciones de valor que aparentan legitimidad, pero que resultan difíciles de verificar, rastrear o revertir una vez consumado el perjuicio patrimonial.

5. Se analizó la asociación entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023, obteniéndose una relación positiva débil y estadísticamente significativa, con un coeficiente τb = 0.305 y un p-valor = 0.008. En consecuencia, se concluye que el comercio electrónico fraudulento se asocia con el uso de criptomonedas en la medida en que estas operan como medios de pago en entornos virtuales con limitada intermediación, insuficiente control y escasos mecanismos de protección al usuario.

VI. RECOMENDACIONES

1. En atención a que se concluyó la existencia de una relación significativa entre la estafa informática y las criptomonedas, se recomienda al Congreso de la República y al Ministerio de Justicia y Derechos Humanos promover la revisión y actualización del marco normativo penal, a fin de incorporar disposiciones más precisas sobre la utilización de criptoactivos en la comisión de delitos informáticos y fortalecer la respuesta jurídica frente a estas nuevas modalidades delictivas.

2. Considerando que los sistemas de inversión online se relacionan con las criptomonedas en contextos de limitada supervisión, se recomienda a la Superintendencia de Banca, Seguros y AFP (SBS) y a la Superintendencia del Mercado de Valores (SMV) reforzar los mecanismos de supervisión, advertencia pública y control sobre plataformas de inversión digital, especialmente aquellas que ofrecen operaciones con criptoactivos sin suficiente respaldo, autorización o transparencia.

3. Debido a que el phishing se relaciona significativamente con las criptomonedas como vía de acceso a credenciales y recursos digitales, se recomienda al Ministerio Público, a la Policía Nacional del Perú y a la Secretaría de Gobierno y Transformación Digital fortalecer campañas públicas de prevención, educación en ciberseguridad y capacitación técnica sobre identificación temprana de suplantación digital, sitios fraudulentos y riesgos vinculados al uso de activos virtuales.

4. Dado que las transferencias falsas se asocian con las criptomonedas en operaciones difíciles de rastrear y revertir, se recomienda a la Unidad de Inteligencia Financiera del Perú (UIF-Perú), a la SBS y a la Policía Nacional del Perú implementar y consolidar protocolos especializados de monitoreo, trazabilidad digital e intercambio de información sobre operaciones sospechosas con criptoactivos, con el propósito de mejorar la detección y persecución de transferencias fraudulentas.

5. En razón de que el comercio electrónico fraudulento se relaciona con las criptomonedas en entornos de escasa protección al consumidor, se recomienda al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), a la SBS y a las entidades responsables de transformación digital fortalecer los mecanismos de orientación al consumidor, supervisión de plataformas virtuales y difusión de alertas sobre riesgos en operaciones comerciales realizadas con criptoactivos.

VII. REFERENCIAS BIBLIOGRÁFICAS

Actuaries Institute. (2024). Digital assets and cybercrime. https://actuary.org/wp-content/uploads/2024/10/DigitalAssetCYBER.pdf

Airant. (2024). Money laundering and cryptocurrency. https://airant.org/wp-content/uploads/2024/07/Report_-Money_laundering_and_Cryptocurrency.pdf

Amaya Cogollo, G. S. (2024). Implicaciones legales y desafíos en la persecución de fraudes, estafas y otros delitos cibernéticos en el comercio electrónico en Colombia [Trabajo de grado, Universidad Autónoma de Bucaramanga]. https://repository.unab.edu.co/bitstream/handle/20.500.12749/27637/TESIS.pdf

Anggriawan, R., & Susila, M. E. (2024). *Cryptocurrency and its nexus with money laundering and terrorism financing within the framework of FATF recommendations*. Novum Jus, 18(2), 249–277. https://doi.org/10.14718/NovumJus.2024.18.2.10

Araya-Pizarro, S. C., González-Arancibia, C. E., & Oyanadel-Díaz, P. D. (2025). *Intención de adopción de criptomonedas entre universitarios chilenos: un enfoque psicosocial y cognitivo*. Información Tecnológica, 36(6), 43–52. https://doi.org/10.4067/S0718-07642025000600043

Arce Quenaya, E. N. (2026). Valoración de medios probatorios en delitos informáticos en el departamento de Puno, 2023 [Tesis de licenciatura, Universidad Privada San Carlos]. https://repositorio.upsc.edu.pe/bitstream/handle/UPSC/1268/Edy_Nestor_ARCE_QUENAYA.pdf

Arciniega Gil, L. R. (2021). *La regulación de las monedas digitales: experiencias compartidas desde el derecho europeo y francés*. FORO: Revista de Derecho, (36), 29–47. https://doi.org/10.32719/26312484.2021.36.2

Arias, J., Holgado, J., Tafur, T., & Vásquez, M. (2022). Metodología de la investigación: El método ARIAS para realizar un proyecto de tesis. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C.

Ayala Medina, L. I. (2024). Elementos relevantes del fraude informático mediante redes sociales [Tesis de licenciatura, Universidad Católica Los Ángeles de

Chimbote]. https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/39580/TIPICIDAD_INFORMATICOS_AYALA_MEDINA_LINDORFO_IBERNON.pdf

Barrutia Barreto, I., Morales Alberto, M. N., García Soto, C. E., & Vergaray Huaman, J. C. (2023). *Criptomonedas: historia, inmersión en los procesos productivos y perspectivas a futuro de las CBDC*. Lecturas de Economía, (99), 245–282. https://doi.org/10.17533/udea.le.n99a351176

Bank for International Settlements. (2023). Cryptocurrencies and decentralised finance. https://www.bis.org/publ/arpdf/ar2023e3.pdf

Barroilhet, A. (2022). *Criptomonedas y blockchain en la adolescencia*. Revista de Derecho, (25), 117–149. https://doi.org/10.22235/rd25.2776

Carrero Pérez, J. S. (2024). Incorporación de la modalidad del phishing en la Ley de Delitos Informáticos [Tesis de licenciatura, Universidad Católica Santo Toribio de Mogrovejo]. Repositorio Institucional USAT. https://repositorio.usat.edu.pe/server/api/core/bitstreams/0c352d02-d5b8-40ab-9317-1c49c38be7c8/content

Cabrera Soto, M., & Lage Codorniu, C. (2022). *Criptomonedas: ¿qué son y qué pretenden ser?* Economía y Desarrollo, 166(1), e8. http://scielo.sld.cu/pdf/eyd/v166n1/0252-8584-eyd-166-01-e8.pdf

Calvo, P. (2023). *Metaverso: desafíos éticos de la tokenización de la economía*. Filosofia Unisinos, 24(1), e24106. https://doi.org/10.4013/fsu.2023.241.06

Carpentier-Desjardins, C., et al. (2023). DeFi crime landscape. https://arxiv.org/abs/2310.04356

Carrizosa Acosta, X. L. (2024). Los retos de la investigación y sanción penal del delito de estafa en espacios digitales [Trabajo de grado, Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/server/api/core/bitstreams/8ae62387-87af-45c8-8ee2-f3cf77abc2cb/content

Chainalysis. (2026). Crypto crime report 2026. https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/

Campos-Jaque, Z., Yanine, F., & Catalán, S. (2025). *The impact of audiovisual content on Bitcoin's transaction volume and price*. Revista Finanzas y Política Económica, 17, 1–25. https://doi.org/10.14718/revfinanzpolitecon.v17.2025.7

Cerdas Herrera, M., & Astorga Cerdas, C. (2024). *Análisis de las posibles repercusiones económicas y legales de la implementación de las criptomonedas en Costa Rica*. Revista Rupturas, 14(1), 1–29. https://doi.org/10.22458/rr.v14i1.5177

Cerna, D. M. (2018). *El uso de las Criptomonedas como medio para la impunidad del delito de lavado de activos.* Trujillo: Universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/36934/cerna_fj.pdf?sequence=1&isAllowed=y

Cobeñas Morales, V. N. (2025). Eficiencia de la persecución penal durante investigación preparatoria por delitos de fraude informático del distrito fiscal de Lambayeque, 2024 [Tesis de maestría, Universidad César Vallejo]. Repositorio institucional de la Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/171083/Cobe%c3%b1as_MVN-SD.pdf?sequence=1&isAllowed=y

COPOLAD. (2025). Criminal use of cryptocurrency. https://copolad.eu/wp-content/uploads/2025/02/COPOLAD_Publicaciones_Criptoactivos_English-1.pdf

Cortés Cortés, J. A., Carvajal Bernal, J. C., & Bernal Cardozo, J. E. (2024). *La democratización del uso de las criptomonedas en Colombia con base en la regulación actual*. Cofin Habana, 18(2), e3. http://scielo.sld.cu/pdf/cofin/v18n2/2073-6061-cofin-18-02-e3.pdf

Chilcon. (2019). *El Cibercrimen en el Perú y su incidencia en la Seguridad Nacional.* Lima: Centro de Altos Estudios Nacionales. Obtenido de https://renati.sunedu.gob.pe/handle/sunedu/393223

Crisóstomo Zúñiga, R. A., Núñez Morales, J. P., & Núñez, N. A. (2024). *Las criptomonedas como catalizadores de la inclusión financiera en América Latina*. The Anáhuac Journal, 24(2), 204–232. https://doi.org/10.36105/theanahuacjour.2024v24n2.2389

Cubero Mora, V. (2025). La estafa informática en Costa Rica [Tesis de maestría, Universidad de Costa Rica]. https://www.kerwa.ucr.ac.cr/server/api/core/bitstreams/53e0301e-843d-4b2f-8a76-9f2ca4fcdd38/content

Dávila Castillo, M. R., Santander Moreno, J. J. & Chuga Quemac, R. E. (2024). Desafíos contables y tributarios de la era de las criptomonedas en el contexto ecuatoriano. Universidad y Sociedad 16(1), 561-572.

De Senna, V., & Souza, A. M. (2023). *Cryptocurrency and financial system: Systematic literature review*. Revista de Administração de Empresas, 63(4), e2022-0019. https://doi.org/10.1590/S0034-759020230403x

Demmler, M. (2023). *Leading cryptocurrencies between 2019 and 2021: Analysis of market prices and portfolio design*. Análisis Económico, 38(99), 145–165. https://doi.org/10.24275/uam/azc/dcsh/ae/2023v38n99/Demmler

Demmler, M., & Fernández Domínguez, A. O. (2022). *Speculative bubble tendencies in time series of Bitcoin market prices*. Cuadernos de Economía, 41(86), 159–183. https://doi.org/10.15446/cuad.econ.v41n86.85391

Dulisse, B., Fitch, C., Denis, J., & Connealy, N. (2025). Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency. Journal of Economic Criminology, 9, 100178. https://www.sciencedirect.com/science/article/pii/S2949791425000545?via%3Dihub

Enríquez-Chapi, B. J., Muñoz-Chulde, D. A., Guerrón-Bracero, M. S., & Santander-Moreno, J. J. (2024). La estafa electrónica en el sistema penal ecuatoriano. Iustitia Socialis, 9(1), 336–345. https://dialnet.unirioja.es/servlet/articulo?codigo=9545779

European Central Bank. (2023). Crypto assets: Implications for financial stability. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

European Criminal Law Review. (2024). Combating cryptocurrency crime. https://eucrim.eu/articles/prospects-and-models-of-combating-cryptocurrency-crimes/pdf/

Federal Bureau of Investigation. (2023). Internet crime report 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Federal Trade Commission. (2023). Consumer sentinel network data book 2023. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023

Gómez Fonseca, J. (2023). El ciberdelito como agravante de la estafa [Tesis de maestría, Universidad La Gran Colombia]. https://repository.ugc.edu.co/server/api/core/bitstreams/a59bfbac-7a58-451e-be0e-2749972b8722/content

Gómez Vilcatoma, C. F. (2026). Dificultades en la individualización del ciberdelincuente [Tesis de licenciatura, Universidad Nacional de San Cristóbal de Huamanga]. https://repositorio.unsch.edu.pe/server/api/core/bitstreams/8d5142fc-a8a3-4a1d-8ef3-7849a4e7c82d/content

Granja-Martínez, L. N., Proaño-Reyes, G. M., & Castro-Sánchez, F. J. (2025). *El poder liberatorio y curso ilegal de criptomonedas, actos criminales en Ecuador*. Noesis. Revista Electrónica de Investigación, 7(esp. 2), 1368–1384. https://doi.org/10.35381/noesisin.v7i2.662

García Terán, P. V. (2023). Obtención fraudulenta de crédito bancario como delito informático en etapa de pandemia Lima, 2021 [Tesis de pregrado, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú. https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/2426/Garcia%20Teran%2c%20Pedro%20Veda.pdf?sequence=1&isAllowed=y

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, M. P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill Education. https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Kılcı, E. N., & Yılancı, V. (2025). *Do uncertainties and risks have an impact on cryptocurrency returns? Evidence from the symmetric and asymmetric Fourier quantile causality test*. Estudios de Economía, 52(1), 27–58. https://doi.org/10.4067/S0718-52862025000100027

Lambis-Alandete, E., Jiménez-Gómez, M., Velázquez-Henao, J.D. Comparación de algoritmos de Deep Learning para pronósticos en los precios de criptomonedas. Ingeniería y Competitividad,2023, 25(3); e-21312845. doi: 10.25100/iyc.v25i3.12845

La República. (2024, junio 3). *Link Flow estafa usuarios en Perú: ¿qué hizo la plataforma digital y cómo clientes podían ganar dinero en línea?* https://larepublica.pe/sociedad/2024/05/30/estafa-de-link-flow-en-peru-que-es-y-para-que-servia-plataforma-que-permitia-ganar-dinero-en-linea-link-flow-estafa-lrsd-447510

Lengyel-Almos, K. E., & Demmler, M. (2021). *Is the Bitcoin market efficient? A literature review* [¿El mercado de Bitcoin es eficiente? Una revisión de la literatura]. Análisis Económico, 36(93), 167–187. https://doi.org/10.24275/uam/azc/dcsh/ae/2021v36n93/lengyel

Loannidis, I. (2025). Crypto crime literature review. https://www.diva-portal.org/smash/get/diva2:2001226/FULLTEXT02.pdf

Lyer, K. (2026). Cryptocurrency and national security risks. https://www.sciencedirect.com/science/article/pii/S2590291126001142

López Rivera, G. A. (2023). *¿Es el Bitcoin dinero? Un análisis de su condición dineraria desde la teoría crediticia del dinero*. Revista Chilena de Derecho y Tecnología, 12, e69921. https://doi.org/10.5354/0719-2584.2023.69921

Luciani Toro, L. R., Castellanos Sánchez, H. A., Hurtado Briceño, A. J., & Zerpa de Hurtado, S. (2023). *Una aproximación al tratamiento contable de criptomonedas en el marco de las NIIF*. Innovar, 33(88), 51–66. https://doi.org/10.15446/innovar.v33n88.106257

Menacho-Inga, W. G., Proaño-Reyes, G. M., & Castro-Sánchez, F. J. (2025). *El uso de criptomonedas y el lavado de activos en Ecuador*. Noesis. Revista Electrónica de Investigación, 7(2, edición especial), 832–845. https://doi.org/10.35381/noesisin.v7i2.620

Meza, E. R. (2019). *A PROPÓSITO DE LA DIGITALIZACIÓN DEL DINERO: Las Criptomonedas y su Incidencia Tributaria en el Perú, el Caso del Bitcoin.* Lima: Universidad de Lima. Obtenido de https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/11357/Roman_Yrigoin_Meza_Maurtua.pdf?sequence=1&isAllowed=y

Mendoza Morales, A. B. (2023). Delito de estafa informática y su tipificación en el ordenamiento jurídico, distrito fiscal de Lima Norte 2022 [Tesis de maestría, Universidad César Vallejo]. Repositorio institucional de la Universidad César Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/130844/Mendoza_MAB-SD.pdf?sequence=1&isAllowed=y

Mora-Calderón, O., & Ramírez-Marín, R. (2022). *Consecuencias financieras, contables y tributarias de las monedas virtuales en el mercado costarricense, un estudio exploratorio*. Revista Nacional de Administración, 13(1), e4230. https://doi.org/10.22458/rna.v13i1.4230

Muñoz de Luna, Á. B., Martín Gómez, S., & Atanes Torres, R. (2025). *Análisis de la inversión en criptomonedas con metodología de análisis de sentimiento: una revolución digital al descubierto*. Zona Próxima, (42), 104–123. http://www.scielo.org.co/pdf/zop/n42/2145-9444-zop-42-104.pdf

Nieto Chávez, H. (2025). Lavado de activos con criptomonedas y control estatal en el Perú. Gaceta Científica, 11(4), 1–10. https://doi.org/10.46794/gacien.11.4.2670

OECD. (2022). Regulatory approaches to crypto assets. https://www.oecd.org/finance/crypto-assets.htm

Olushola, A. (2025). Cryptocurrency exchange crimes dataset. https://www.frontiersin.org/articles/10.3389/fbloc.2025.1713637/full

Orobets, K. (2025). Crimes with cryptocurrency. https://dialnet.unirioja.es/descarga/articulo/10304595.pdf

Palma Mera, A. A. (2023). *El desarrollo económico en el Ecuador: las criptomonedas y el derecho tributario*. Revista San Gregorio, 1(56), 205–217. https://doi.org/10.36097/rsan.v1i56.2385

Palella Stracuzzi, S., & Martins Pestana, F. (2006). Metodología de la investigación cuantitativa (2.ª ed.). FEDEUPEL. https://gc.scalahed.com/recursos/files/r161r/w23578w/w23578w.pdf

Peralta Luque, H. O. (2022). *Las criptomonedas y los delitos de estafa perpetrados por los ciberdelincuentes, Perú, 2022.* Lima: Universidad Cesar Vallejo. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/100790

Phillips, R., & Wilder, B. (2022). Tracing cryptocurrency scams. https://arxiv.org/abs/2005.14440

Puentes Díaz, J. C. (2018). *Sistema Ponzi vs sistema multinivel: aproximación legal de los multiniveles.* Bogotá: Universidad Católica de Colombia. Obtenido de https://repository.ucatolica.edu.co/entities/publication/b31ad0c1-be30-4eec-adc0-48c34b7a6a6

Pulache Roque, J. F., & Sandoval Linares, A. Y. (2025). Tecnologías emergentes y su relación con la percepción de seguridad de los clientes, BCP Tumbes 2025 [Tesis de pregrado, Universidad Nacional de Tumbes]. Repositorio institucional de la Universidad Nacional de Tumbes. https://repositorio.untumbes.edu.pe/server/api/core/bitstreams/09a4a21a-7766-44b5-8577-5852ec0c48a7/content

Riveros Dullmann, F. A. (2023). *Constitución política y regulación de criptomonedas en Bolivia*. Revista Jurídica Derecho, 12(18), 201–218. http://www.scielo.org.bo/pdf/rjd/v12n18/v12n18_a10.pdf

Rojas Rincón, J. S. (2024). *Aproximación bibliométrica a la incertidumbre y el riesgo en los mercados de criptomonedas*. Lecturas de Economía, (101), 203–233. https://doi.org/10.17533/udea.le.n101a354009

Rojas Rincón, J. S. (2023). *Caracterización del riesgo percibido en el uso de criptomonedas: Una revisión de literatura*. Revista Lasallista de Investigación, 20(1), 191–206. https://doi.org/10.22507/rli.v20n1a12

Salas Ocampo, L. D., & Alfaro Salas, M. (2022). *Criptomonedas y su efecto en la estabilidad del sistema financiero internacional: Apuntes para Centroamérica*. Revista Relaciones Internacionales, 95(1), 33–78. https://doi.org/10.15359/ri.95/1.2

Sapa Oruro, Y. (2025, agosto 13). *¿Trading o delito? Cómo el uso legítimo de criptomonedas puede llevarte a una investigación penal en Perú.* LP Derecho. https://lpderecho.pe/trading-delito-como-uso-legitimo-criptomonedas-llevarte-investigacion-penal-peru/

Shi, J., et al. (2025). Crypto cybercrime detection dataset. https://arxiv.org/abs/2501.15553

Silva, G., Mendes Filho, L., & Marques Júnior, S. (2022). *Intención de usar criptomonedas por gestores de emprendimientos turísticos: un abordaje utilizando el Technology Acceptance Model (TAM)*. Revista Brasileira de Pesquisa em Turismo (RBTUR), 16, e2556. https://doi.org/10.7784/rbtur.v16.2556

TRM Labs. (2026). 2026 crypto crime report. https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

Ultreras-Rodríguez, A., De La Paz-Rosales, M. T. J., Tostado-Ramírez, M. I., & Bueno-Fernández, M. M. (2026). *La Ley Bitcoin en El Salvador: un análisis integral sobre su diseño, implementación e impacto socioeconómico*. Revista InveCom, 6(1), e601007. https://doi.org/10.5281/zenodo.15232884

United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cybercrime and cryptocurrencies. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

Valencia Marín, F. D. (2021). *Panorama actual del bitcóin: Una descripción práctica y jurídica de las criptomonedas en Colombia y Ecuador*. FORO: Revista de Derecho, (36), 49–71. https://doi.org/10.32719/26312484.2021.36.3

Wang, J., & Deng, L. (2026). Influencing factors and mechanisms of action on the participation intentions of cryptocurrency investment fraud victims—A quantitative examination from the perspective of the theory of planned behavior. PLOS One, 21(2), e0339989. https://doi.org/10.1371/journal.pone.0339989

World Bank. (2023). Crypto-assets and financial consumer protection. https://www.worldbank.org/en/topic/financialsector

Wu, J., et al. (2022). Financial crimes in Web3. https://arxiv.org/abs/2212.13452

Xia, P., et al. (2024). Cryptocurrency abuse on the dark web

Yan, C., Zhang, C., Shen, M., Li, N., Liu, J., Qi, Y., Lu, Z., & Liu, Y. (2023). Aparecium: Understanding and detecting scam behaviors on Ethereum via biased random walk. Cybersecurity, 6, 46. https://doi.org/10.1186/s42400-023-00180-x

ANEXOS

Anexo 1: Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	TIPO Y DISEÑO DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA
Problema General	**Objetivo General**	**Hipótesis General**			
¿Cuál es la relación entre el delito de estafa informática y las criptomonedas en el Perú, 2023?	Determinar la relación entre el delito de estafa informática y las criptomonedas en el Perú, 2023.	Existe relación estadísticamente significativa entre el delito de estafa informática y las criptomonedas en el Perú, 2023.			
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Específicos**	**Variable Independiente:** Delito de Estafa Informática	**Tipo de investigación**: Correlacional y descriptiva	**Población y muestra**: 50 Colaboradores del Sistema Legal (Poder Judicial, Ministerio Público, Colegio de Abogados, Contraloría, Procuraduría) de Tumbes, Perú.
¿Cuál es la relación entre los sistemas de inversión online y las criptomonedas en el Perú, 2023?	Determinar la relación entre los sistemas de inversión online y las criptomonedas en el Perú, 2023.	Existe relación estadísticamente significativa entre los sistemas de inversión online y las criptomonedas en el Perú, 2023.			
¿Cuál es la relación entre el phishing y las criptomonedas en el Perú, 2023?	Determinar la relación entre el phishing y las criptomonedas en el Perú, 2023.	Existe relación estadísticamente significativa entre el phishing y las criptomonedas en el Perú, 2023.	**Variable Dependiente:** Criptomonedas	**Diseño de Investigación:** No experimental y cuantitativa	**Muestreo:** No probabilístico

¿Cuál es la relación entre las transferencias falsas y las criptomonedas en el Perú, 2023?	Determinar la relación entre las transferencias falsas y las criptomonedas en el Perú, 2023.	Existe relación estadísticamente significativa entre las transferencias falsas y las criptomonedas en el Perú, 2023.			
¿Cuál es la relación entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023?	Determinar la relación entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023.	Existe relación estadísticamente significativa entre el comercio electrónico fraudulento y las criptomonedas en el Perú, 2023.			

Anexo 2: Matriz de operacionalización

Variable		Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems
Variable Independiente:	Delito de Estafa Informática	Marazzo (2020), el concepto de estafa informática puede entenderse como la adaptación de estafas tradicionales en el contexto digital, aprovechando la evolución tecnológica. En este sentido, las estafas informáticas implican el uso de mecanismos informáticos para engañar a las personas con el objetivo de obtener beneficios económicos.	Para medir la Estafa Informática, se usarán sus dimensiones e indicadores, que estarán en una encuesta de 16 preguntas, que se puntuarán con la escala de Likert: 5= Siempre, 4= Casi siempre, 3= A veces, 2= Casi nunca y 1= Nunca; esto se hará con miembros del Colegio de Abogados de Tumbes, de Fiscalía, y del Poder Judicial de Tumbes, Perú, 2023	Sistemas de inversión Online	Influencia Social	1,2,3,4
					Conocimiento Financiero	
					Confianza excesiva	
					Falta de regulación	
				Phishing	Educación	5,6,7,8
					Falsificación	
					Apariencia legitima	
				Transferencias Falsas	Falsificación de información	9,10,11,12
					Ausencia de transferencia real	
					Presión	
					Pérdida de fondos	
				Comercio Electrónico Fraudulento	Ofertas tentadoras	13,14,15,16
					Falta de experiencia en compras online	
					Influencia	

Variable		Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems
Variable Dependiente:	Criptomonedas	El GAFI (2014) define las criptomonedas como formas descentralizadas de moneda virtual convertible, respaldadas por fundamentos matemáticos y protegidas mediante técnicas de criptografía.	Para medir la productividad laboral, se usarán sus dimensiones e indicadores, que estarán en una encuesta de 12 preguntas, que se puntuarán con la escala de Likert: 5= Siempre, 4= Casi siempre, 3= A veces, 2= Casi nunca y 1= Nunca; esto se hará con miembros del Colegio de Abogados de Tumbes, de Fiscalía, y del Poder Judicial de Tumbes, Perú, 2023.	Bitcoin	Anonimato	1,2,3,4
					Seguridad Criptográfica	
					Transferencias rápidas y globales	
				Ether	Economicidad	5,6,7,8
					Rentabilidad	
				Litecoin	Minería	9,10,11,12
					Tarifas de transacción bajas	
					Descentralizada	

Anexo 3: Instrumento de recolección de datos

1	2	3	4	5
Nunca	**Casi nunca**	**A veces**	**Casi Siempre**	**Siempre**

N.º	V1. Delito de Estafa	1	2	3	4	5
01	¿Considera usted que en el Perú deben implementarse mecanismos para proteger a los usuarios e inversores frente a las estafas informáticas en plataformas de inversión online que operan con criptomonedas, teniendo en cuenta la irreversibilidad de las transacciones y el anonimato de los usuarios?					
02	¿Cree usted que las características inherentes a las criptomonedas, como la descentralización y la falta de regulación clara en muchos países, están afectando el marco jurídico existente para combatir las estafas informáticas en sistemas de inversión online?					
03	¿Considera que podrían mejorar los sistemas de monitoreo y prevención de estafas en plataformas que usan criptomonedas, para que se logre una mayor efectividad en la persecución penal de los estafadores?					
04	¿Piensa usted que el creciente número de estafas relacionadas con criptomonedas en sistemas de inversión online afecta la confianza social en esta tecnología?					
05	¿Considera usted necesarias herramientas legales y tecnológicas para proteger a los usuarios de criptomonedas frente a ataques de phishing que buscan obtener información confidencial, como claves de acceso y datos personales, para vaciar billeteras digitales?					
06	¿Cree usted que la teoría jurídica actual aborda los riesgos asociados al phishing en transacciones con criptomonedas?					
07	¿Cree usted que las acciones coordinadas entre los sectores público y privado podrían mejorar la detección temprana y la respuesta ante ataques de phishing dirigidos a inversionistas y usuarios de criptomonedas?					

08	¿Considera usted que el phishing afecta la confianza pública en el uso de criptomonedas?					
09	¿Considera usted que deberían implementarse medidas legales para prevenir y sancionar las transferencias falsas en el ámbito de las criptomonedas?					
10	¿Cree usted que la falta de regulación específica para las criptomonedas dificulta la persecución penal y el marco teórico para la resolución de casos relacionados con transferencias falsas en plataformas de criptomonedas?					
11	¿Considera que deberían implementarse metodologías investigativas y forenses para rastrear transferencias fraudulentas en transacciones con criptomonedas, considerando la dificultad de rastreo que implica la tecnología blockchain y los sistemas descentralizados?					
12	¿Usted cree que impactan las transferencias falsas en la percepción pública y confianza hacia las criptomonedas?					
13	¿Considera usted que deberían implementarse mecanismos legales y de seguridad para evitar que los compradores sean víctimas de comercio electrónico fraudulento cuando utilizan criptomonedas como método de pago, dada la naturaleza irreversible de las transacciones?					
14	¿Cree usted que existen lagunas normativas que facilitan la proliferación de sitios web fraudulentos que aceptan pagos en criptoactivos?					
15	¿Considera que deberían coordinarse las acciones de monitoreo y control para detectar y desmantelar plataformas de comercio electrónico fraudulentas que operan con criptomonedas, teniendo en cuenta las limitaciones en la trazabilidad de los fondos?					
16	¿Cree usted que el aumento del comercio electrónico fraudulento, en el cual las criptomonedas son utilizadas como medio de pago, afecta la percepción pública de esta tecnología?					

1	2	3	4	5
Nunca	**Casi nunca**	**A veces**	**Casi Siempre**	**Siempre**

N.º	V2. Criptomonedas	1	2	3	4	5
01	¿Cree usted que deberían implementarse medidas legales y de ciberseguridad para proteger a los usuarios de Bitcoin frente a estafas informáticas, considerando las características de anonimato y descentralización que facilitan actividades delictivas en esta criptomoneda?					
02	¿Cree que el marco jurídico actual debería evolucionar para abordar los desafíos que presenta Bitcoin en la prevención y sanción de estafas informáticas, dado que su naturaleza descentralizada complica la identificación de los responsables?					
03	¿Cree usted que deben emplearse metodologías investigativas para rastrear transacciones fraudulentas en la red de Bitcoin, teniendo en cuenta la transparencia del blockchain, pero también los métodos sofisticados que los estafadores usan para ocultar sus actividades?					
04	¿Considera que el uso de Bitcoin en estafas informáticas afecta la percepción pública de esta criptomoneda?					
05	¿Considera usted que la red Ethereum presenta desafíos en la prevención de estafas informáticas, considerando el uso de contratos inteligentes y la rapidez con la que se ejecutan las transacciones en la plataforma?					
06	¿Cree usted que existen vacíos normativos en la regulación de los contratos inteligentes en torno a las criptomonedas como Ether?					
07	¿Cree que deberían emplearse métodos de investigación y seguimiento para rastrear transacciones fraudulentas y actividades delictivas en la blockchain de Ethereum, considerando que las transacciones son públicas, pero los usuarios pueden ocultar su identidad mediante técnicas avanzadas?					
08	¿Considera que la proliferación de estafas relacionadas con Ether afecta a la percepción pública y social de esta tecnología en cuanto a su adopción masiva?					
09	¿Cree usted que la regulación de Litecoin en relación con las estafas informáticas enfrenta desafíos?					

10	¿Considera usted que existen vacíos normativos respecto a la regulación de Litecoin y otras criptomonedas, especialmente en lo que respecta a su uso en fraudes y actividades delictivas?					
11	¿Cree que los juristas podrían colaborar con expertos en tecnología para abordar la implementación de metodologías o enfoques más efectivos a fin de investigar y rastrear transacciones fraudulentas que involucran Litecoin?					
12	¿Cree usted que cree que los juristas y operadores del derecho deben desempeñar el rol importante de educar al público además de fomentar un entorno más seguro en el uso de criptomonedas como Litecoin?					