



Universidad
Señor de Sipán

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

**Implicancias del dinero digital en el fraude financiero -
Chiclayo- 2024**

**PARA OPTAR EL GRADO ACADÉMICO DE BACHILLER EN
DERECHO**

Autora

Llamo Fernandez Yhadira Mirella

<https://orcid.org/0000-0003-1339-1939>

Línea de Investigación

**Desarrollo Humano, Comunicación y Ciencias Jurídicas para
enfrentar los desafíos Globales**

Sublínea de Investigación

Derecho Público y Derecho Privado

**Pimentel – Perú
2025**

**IMPLICANCIAS DEL DINERO DIGITAL EN EL FRAUDE FINANCIERO -
CHICLAYO- 2024**




DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la **DECLARACIÓN JURADA**, soy egresada de la Escuela profesional de Derecho de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autora del trabajo titulado:

IMPLICANCIAS DEL DINERO DIGITAL EN EL FRAUDE FINANCIERO - CHICLAYO- 2024

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán (CIEI USS) conforme a los principios y lineamientos detallados en dicho documento, en relación a las citas y referencias bibliográficas, respetando al derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y auténtico.

En virtud de lo antes mencionado, firman:

LLAMO FERNANDEZ YHADIRA MIRELLA	DNI N°: 74433909	
--	------------------	---

Pimentel, 12 de febrero de 2025




12% Similitud general

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

Filtrado desde el informe


- Bibliografía
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Fuentes principales

- 11%  Fuentes de Internet
- 4%  Publicaciones
- 7%  Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

-  **Texto oculto**
135 caracteres sospechosos en N.º de página
El texto es alterado para mezclarse con el fondo blanco del documento.

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.

Dedicatoria

A mis padres Juan Llamo Delgado y Margarita Fernández Contreras, por su amor, sacrificio y constante apoyo. Cada palabra de aliento, esfuerzo y enseñanza me han hecho ser quien soy hoy.

A mi hijo Dan Martín Torres Llamo, mi mayor motivación. Eres la razón por la que sigo luchando, para brindarte un futuro lleno de oportunidades. Este logro es tanto mío como tuyo.

A mi hermana Sandra Llamo Fernández, mi compañera de vida. Gracias por siempre estar allí cuando más te necesito. Compartir este camino contigo ha sido un regalo.

Este trabajo es el reflejo de todo lo que ustedes me han enseñado. Gracias por ser mi motor y mi inspiración constante.

Agradecimiento

En primer lugar, quiero agradecer a Dios por ser mi guía, por brindarme la sabiduría y la paciencia para enfrentar los desafíos y por darme la oportunidad de alcanzar este logro. A mis padres, por su amor incondicional, apoyo constante y esfuerzo incansable para darme lo mejor. A mi hijo, por recordarme cada día la importancia de seguir adelante, por darme las fuerzas para ser mejor. Y finalmente a mi hermana, su presencia ha sido un pilar fundamental en este camino.

A todos ustedes, de corazón, gracias. Este logro también es de ustedes.

ÍNDICE

Resumen.....	9
Abstract.....	10
I. INTRODUCCION	11
1.1. Realidad Problemática	11
1.2. Formulación del problema.....	15
1.3. Hipótesis	15
1.4. Objetivos.....	16
1.5. Teorías relacionadas	16
II. MATERIALES Y METODOS	26
III. RESULTADOS.....	27
IV. DISCUSION Y CONCLUSIONES	32
V. REFERENCIAS	36

Índice de Figuras

Figura 1.....	17
Figura 2.....	19
Figura 3.....	27
Figura 4.....	31

Índice de Tablas

Tabla 1	20
Tabla 2	21

Resumen

La presente investigación siguió un diseño no experimental, fue de tipo descriptivo, cualitativo, documental, cuyo objetivo principal es determinar cuáles son las implicancias del dinero digital en el fraude financiero, en este trabajo se identifican los factores que inciden en la lucha contra el fraude financiero, las Principales conductas sancionadas por la Ley de Delitos Informáticos en Perú y las formas más comunes de fraude financiero en Perú. La técnica e instrumento aplicada es análisis documental y fichas respectivamente, sobre material bibliográfico, artículos científicos, normativas vigentes, etc. Se concluye que el dinero digital es más vulnerable a fraudes como phishing y hacking, permitiendo a los delincuentes realizar transacciones de manera rápida y menos detectable. Además, su alto nivel de anonimato dificulta el rastreo de los criminales, lo que puede fomentar actividades delictivas. La evolución del dinero digital ha generado nuevas modalidades de fraude, como tokens falsos y manipulación de contratos inteligentes, lo que exige que tanto instituciones financieras como usuarios estén al tanto de las nuevas amenazas, asimismo, la naturaleza transnacional del dinero digital presenta retos para la regulación, ya que las diferencias normativas entre países pueden ser aprovechadas por los delincuentes para cometer fraudes a gran escala y por último, tenemos que muchos usuarios carecen de la educación financiera necesaria para reconocer riesgos y proteger sus activos, lo que los hace más vulnerables a estafas, especialmente en el ámbito de las criptomonedas.

Palabras clave: Fraude, dinero, financiero

Abstract

The present research followed a non-experimental design, it was descriptive, qualitative, documentary, whose main objective is to determine the implications of digital money in financial fraud. In this work, the factors that affect the fight against fraud are identified. financial, the Main behaviors sanctioned by the Computer Crimes Law in Peru and the most common forms of financial fraud in Peru. The technique and instrument applied is documentary analysis and files respectively, on bibliographic material, scientific articles, current regulations, etc. It is concluded that digital money is more vulnerable to fraud such as phishing and hacking, allowing criminals to carry out transactions quickly and less detectably. Additionally, its high level of anonymity makes it difficult to track criminals, which can encourage criminal activities. The evolution of digital money has generated new forms of fraud, such as fake tokens and manipulation of smart contracts, which requires both financial institutions and users to be aware of new threats. Likewise, the transnational nature of digital money presents challenges for the regulation, since regulatory differences between countries can be taken advantage of by criminals to commit large-scale fraud and lastly, many users lack the financial education necessary to recognize risks and protect their assets, which makes them more vulnerable to scams, especially in the area of cryptocurrencies.

Keywords: Fraud, money, financial

I. INTRODUCCION

1.1. Realidad Problemática

El dinero electrónico o dinero digital, es conocido como un sistema que permite acceder a pequeños créditos monetarios, funciona mediante unidades o símbolos que representan valores de dinero y están protegidos por cifrado para garantizar su seguridad, estas unidades son completamente digitales y pueden convertirse en efectivo cuando se necesite. (Gonzales, 2019).

Al no poseer una forma física las transacciones se llevan a cabo a través de medios digitales, como transferencias electrónicas, sin necesidad de tener billetes o monedas, además el dinero electrónico permite hacer pagos de forma rápida y eficiente lo cual facilita el comercio y las transacciones en línea. (Pedrosa, 2021).

El dinero electrónico se guarda en computadoras y se envía a través de redes digitales para realizar compras en línea en Internet, y en teoría este tipo de dinero podría utilizarse para pagar por artículos de bajo costo, incluso cantidades tan pequeñas como décimas de centavo de dólar, euro o sol, dependiendo del caso. (Gonzales, 2019).

No obstante, la mayoría de los comerciantes que aceptan dinero electrónico lo utilizan principalmente como una opción alternativa a otros métodos de pago para compras de mayor valor, este tipo de dinero está diseñado para facilitar pagos por artículos que cuestan menos de cinco dólares, lo que resulta eficiente ya que evita los costos asociados con el uso de tarjetas de crédito en especial cuando se trata de transacciones de bajo monto. (Pedroza, 2021).

El funcionamiento del dinero electrónico para un consumidor es el siguiente:

Primero, es necesario registrarse en un banco que ofrezca este servicio, luego de ello, hay que firmar un contrato con una empresa que provea el sistema la cual nos dará el software que necesitamos instalar en nuestra computadora, este software

permite descargar el dinero electrónico en el disco duro del equipo, la adquisición inicial de dinero se realiza contra nuestra cuenta bancaria o una tarjeta de crédito, una vez instalado el software en la computadora, procederemos a realizar nuestras compras en la red, asegurándonos que la tienda virtual que escojamos acepte Dinero Electrónico o Digital. (López, 2020).

Una vez que hemos elegido el producto y estamos listos para comprar, solo necesitamos hacer clic en el botón de pago, el software de la tienda generará una solicitud de pago con los detalles del artículo, su precio, la fecha y la hora, si es que aceptamos la solicitud, el software deduce el monto del precio y realiza el pago que se envía al banco para su verificación y posterior depósito en la cuenta de la tienda virtual, Una vez completado este proceso, la tienda recibe la confirmación y procede a enviar el producto que hemos adquirido, entre los sistemas de dinero electrónico o digital más populares en la actualidad se encuentran CyberCash, que está relacionado con CyberCoin, así como E-cash y el sistema DigiCash. (Fernández, 2019).

En la actualidad, el uso del dinero electrónico enfrenta ciertos desafíos que pueden desincentivar su adopción y para utilizar este sistema de pago, los consumidores deben instalar programas específicos en sus computadoras, lo que implica un costo adicional a corto plazo. (Lopez, 2019).

En Perú, la virtualización de la vida diaria se volvió más evidente durante la primera etapa de la pandemia, cuando el gobierno tuvo que implementar medidas estrictas de confinamiento, sin embargo, resulta conveniente recordar que el aumento del uso de las TIC ya era notable desde la última década, es así que en 2010, uno de cada tres peruanos utilizaba Internet, mientras que en 2021 esa cifra ascendió a tres de cada cuatro, la frecuencia de uso también aumentó y para el último trimestre de 2021, el acceso a Internet en los hogares peruanos alcanzó el 55%, lo que representó un

incremento de más de 9,6 puntos porcentuales respecto al mismo período en 2020. (LLa, 2022).

Sin duda, este fenómeno se debe a la gran oferta y demanda de teléfonos inteligentes en el mercado, que se han convertido en la principal herramienta para acceder a Internet, en los últimos seis años su uso ha aumentado significativamente, pasando del 22% en 2015 al 65% en 2021. (Ruiz, 2020).

Sin embargo, junto con las ventajas que ofrecen las TIC, la pandemia también reveló las numerosas *ciberamenazas* que enfrentan tanto a la ciudadanía como a los Estados, se reportaron diferentes tipos de ataques y delitos que aprovechaban precisamente estas tecnologías, incluyendo intentos de atraer a menores en las redes sociales para convertirlos en víctimas de abuso sexual, explotación, extorsión y otras conductas inaceptables. (Mantilla, 2019).

Al respecto, la Organización Internacional de Policía Criminal (Interpol) informa que los ciberdelincuentes han estado evolucionando y modificando sus objetivos para aumentar el impacto de sus ataques y robos, en lugar de dirigirse solo a individuos y pequeñas empresas más bien han ampliado su enfoque hacia grandes corporaciones, gobiernos e infraestructuras críticas, además, con el incremento de teletrabajo durante la pandemia, los delincuentes han aprovechado las nuevas vulnerabilidades en la seguridad para robar datos, obtener ganancias y causar problemas. (Quiroz, 2023).

Perú no ha sido ajeno al aumento global de este fenómeno criminal ya que entre enero y septiembre de 2021, la PNP recibió un total de 11,985 denuncias de este tipo en todo el país de los cuales el 70% se encontraba relacionada a fraudes informáticos, en contraste con esa realidad, se sabe que desde octubre de 2013 hasta julio de 2020, las fiscalías penales comunes y mixtas del Ministerio Público registraron 21,687 denuncias por delitos informáticos, lo que evidencia un aumento significativo de la ciberdelincuencia durante la emergencia sanitaria, en ese sentido se puede decir que la

creciente dependencia del ciberespacio ha creado un entorno favorable para los ciberdelincuentes, convirtiéndose en uno de los principales riesgos y desafíos en términos de seguridad ciudadana y defensa nacional. (Ruiz, 2020).

Para los investigadores, este es un problema que requiere una atención especial por parte del Estado peruano ya que afecta los derechos de grupos vulnerables tales como niños, adolescentes y adultos mayores, muchos de los cuales no tienen conocimientos sobre cómo manejar y proteger sus datos personales, además esta situación perjudica la operación y seguridad de instituciones tanto públicas como privadas y de todos los usuarios de Internet, independientemente de su propósito.

En la era digital, el rápido desarrollo de las tecnologías financieras ha cambiado la forma en que se manejan y se entienden las transacciones monetarias, el dinero digital que incluye criptomonedas, billeteras electrónicas y plataformas de pago en línea, ha cobrado relevancia en el ámbito económico ya que brinda comodidad y rapidez a los usuarios, sin embargo, esta evolución también ha llevado a un aumento significativo en los casos de fraude financiero. (Quiroz, 2023)

Explorar el tema del dinero digital es crucial por diversas razones, en primer lugar permite entender que estas herramientas digitales ayuda a los usuarios a estar más preparados para enfrentar los riesgos que conllevan, las estafas en línea, el phishing y el robo de identidad son solo algunas de las amenazas que afectan a los consumidores en el mundo digital, de igual forma nos permite entender cómo operan estos esquemas fraudulentos lo cual es fundamental para implementar medidas preventivas efectivas. (Rodríguez, 2022).

La relación entre el dinero digital y el fraude financiero ofrece una base firme para la creación de políticas públicas y regulaciones que protejan a los ciudadanos, los organismos reguladores financieros deben estar atentos a las tendencias emergentes

en el uso del dinero digital para desarrollar estrategias que reduzcan los riesgos y aseguren la seguridad de las transacciones. (Trond, 2019).

Velezmoro (2010) en su análisis sobre el modelo de gestión del riesgo operacional en una institución financiera peruana, destacó la importancia de controlar la exposición a este tipo de riesgo, también subrayó los beneficios de implementar las mejores prácticas en la gestión del riesgo operacional, lo que permite asignar menos capital a este riesgo según la regulación peruana, reduciendo así las provisiones necesarias para contingencias regulatorias y legales.

Asimismo, Arcenegui, Martín y Obrero (2016) destacaron el impacto económico, legal y reputacional que el fraude interno genera en el sector bancario en comparación con otros sectores, además de señalar la complejidad del estudio debido a problemas de confidencialidad que dificultan la creación y acceso a bases de datos, así, el objetivo de su investigación fue definir el perfil del defraudador, mostrando la relación entre las variables externas evaluadas (como la tasa de desempleo, la renta media por hogar, la evaluación del riesgo privado y el porcentaje de población en riesgo de pobreza o exclusión social) y las variables internas del banco (como el número de empleados en entidades financieras y oficinas bancarias).

1.2. Formulación del problema

¿Cuáles son las implicancias del dinero digital en el fraude financiero - Chiclayo- 2024?

1.3. Hipótesis

La falta de regulación adecuada, la vulnerabilidad de las plataformas digitales y la sofisticación de los ciberdelincuentes podrían incrementar la incidencia de fraudes financieros en un entorno cada vez más digitalizado, además, la dificultad para rastrear y recuperar activos digitales robados plantea serias implicancias para la seguridad financiera de individuos, empresas y sistemas financieros en su conjunto.

1.4. Objetivos

General

Determinar cuáles son las implicancias del dinero digital en el fraude financiero - Chiclayo- 2024

Específicos

- a. Identificar los factores que inciden en la lucha contra el fraude financiero
- b. Identificar las Principales conductas sancionadas por la Ley de Delitos Informáticos en Perú
- c. Identificar las formas más comunes de fraude financiero en Perú

1.5. Teorías relacionadas

El dinero digital, también conocido como dinero electrónico, e-money, moneda digital o efectivo digital, tiene dos definiciones reconocidas por los analistas:

- Es el dinero que se emite electrónicamente mediante una red de computadoras y sistemas de almacenamiento digital (criptomonedas).
- Es un medio de pago digital que equivale a una moneda específica, con los fondos almacenados en dispositivos como monederos electrónicos.

A lo largo del tiempo los sistemas financieros han trabajado para agilizar y facilitar el manejo del dinero físico, utilizando herramientas como cuentas bancarias, cheques, tarjetas de crédito y monederos electrónicos y más recientemente, monedas digitales, todo esto se encuentra adaptado a las necesidades y demandas de las personas. (Rodriguez, 2022).

Con respecto al dinero electrónico, el BCRP clasifica las representaciones electrónicas de dinero en tres categorías:

- Vinculadas a una cuenta bancaria, dentro de las cuales se incluyen tarjetas de crédito, débito y billeteras electrónicas.
- Sin conexión a una cuenta bancaria dentro de las cuales están el dinero móvil y tarjetas de prepago.
- Moneda digital del Banco Central, la cual es un tipo de dinero que aún no se ha implementado formalmente, pero que ha sido probado en varios países.

En cuanto a las monedas digitales, estas han sido desarrolladas de manera privada y tienen solo una representación electrónica siendo las criptomonedas su principal exponente.

Las criptomonedas son generadas por iniciativas privadas y no están bajo el control de ningún banco central, operan mediante la tecnología Blockchain lo que significa que son completamente virtuales, el valor de una moneda digital se determina por la oferta y la demanda que los propios usuarios asignan a estos activos. (Mantilla, 2019).

La primera criptomoneda en comenzar a operar fue el Bitcoin en 2009 y desde entonces han surgido otras con distintas características, como Ethereum, Litecoin y Dogecoin.

Los principales bancos centrales del mundo están evaluando la posibilidad de emitir monedas digitales que, a diferencia de las criptomonedas, estarían respaldadas por un banco central, lo que les otorgaría un valor tan estable y seguro como el de los billetes y monedas, estas monedas digitales de bancos centrales están en fase de investigación y tienen como objetivo abordar *la amenaza* que representan las monedas virtuales privadas. (Grillo, 2019).

Figura 1

Ventajas del dinero digital

Más práctico:	<ul style="list-style-type: none"> • Con el dinero digital, ya no necesitas llevar efectivo en los bolsillos.
Más seguro:	<ul style="list-style-type: none"> • En el caso de las monedas digitales, puedes establecer un código para tus transacciones, lo que impide que sean robadas, desviadas o perdidas.
Confidencial:	<ul style="list-style-type: none"> • Puedes mantener en secreto tus transacciones.
Menos costos adicionales:	<ul style="list-style-type: none"> • Una moneda digital no requiere impresión, almacenamiento físico ni transporte.
Reduce actividades ilegales:	<ul style="list-style-type: none"> • El dinero digital es fácil de rastrear, ya que deja una "huella", lo que dificulta delitos como la corrupción o la evasión fiscal.

Nota: Elaboración propia.

Figura 2

Desventajas del dinero digital

Ataques cibernéticos:	<ul style="list-style-type: none">• Los ataques de hackers son uno de los riesgos asociados con el dinero digital, además de las posibles fallas informáticas que pueden surgir.
Dificultades para los bancos centrales:	<ul style="list-style-type: none">• La función monetaria de los bancos centrales se complicaría al no poder determinar la cantidad de monedas digitales que utilizan las personas.
Falta de regulación:	<ul style="list-style-type: none">• Dado que el dinero virtual es creado y emitido por entidades privadas, no cuenta con una legislación que lo regule frente a posibles delitos electrónicos.
Acceso limitado:	<ul style="list-style-type: none">• Muchas personas aún no tienen acceso a este método de pago

Nota: Elaboración propia.

El Sistema Financiero está formado por entidades tanto privadas como públicas que tienen el objetivo de captar, gestionar y regular recursos financieros, actuando como intermediarios, lo cual significa que recogen fondos de aquellos que tienen un excedente y los ponen a disposición de quienes tienen déficit. (SBS, 2017).

A finales de mayo de 2019, el sistema financiero peruano estaba compuesto por 57 instituciones, de las cuales 54 realizan operaciones diversas y poseen activos que representan cerca del 90% del total de activos del sistema financiero en el país. (SBS, 2019).

Tabla 1

Estructura del Sistema Financiero Peruano

Empresa	Cantidad
Banca Múltiple	15
Empresas Financieras	11
Cajas municipales (CM)	12
Cajas rurales de ahorro y crédito (CRAC)	7
Entidades de Desarrollo de la Pequeña y Microempresa	9
Empresas de Arrendamiento Financiero	1
Banco de la Nación	1
Banco Agropecuario (Agrobanco)	1

Nota: Elaboración a partir de la información obtenida de SBS (2019)

Es el organismo responsable de regular y supervisar a los participantes del sistema financiero, así como de prevenir y alertar sobre el lavado de activos y el financiamiento del terrorismo, su autonomía está reconocida por la Constitución Política del Perú, y sus funciones están definidas en la Ley N° 26702, que es la Ley General del Sistema Financiero y del Sistema de Seguros, así como en la normativa orgánica de la Superintendencia de Banca, Seguros y AFP. (SBS, 2019)

Tabla 2

Evolución de la Supervisión de la SBS

Año	Evento histórico
1931	Creación de la Superintendencia de Bancos
1936	Se incluye compañías de capitalización y empresas de seguros al ámbito de supervisión de la SBS
1968	Se incluye las empresas financieras y las mutuales de vivienda al ámbito de competencia de la SBS
1979	SBS adquiere rango constitucional
1996	Se promulga la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la SBS
2000	Se incorpora a las AFP al control y supervisión de la SBS
2005	Se dicta la Ley número 28587, que regula la protección del usuario de servicios financieros
2007	Se incorpora la Unidad de Inteligencia Financiera del Perú a la SBS
2018	Se incorpora las cooperativas de Ahorro y Crédito a la supervisión de la SBS

Nota: Elaboración propia a partir de SBS (2019).

A nivel mundial, se reconoce que el fraude o el riesgo de fraude financiero que enfrentan las empresas, incluidas grandes organizaciones, está en el centro de la atención pública, a nivel nacional e internacional han surgido numerosos casos de fraude tan graves que han sido expuestos, como se menciona en el blog de Ernst & Young Global Limited (EYG, 2022). Estos casos involucran a personas influyentes, como políticos y empresarios reconocidos, y también reflejan situaciones en las que ha habido un exceso de confianza en uno o más empleados, lo que ha permitido que estos cometan fraudes que perjudican a grandes organizaciones. Un ejemplo de esto es el escándalo financiero de Enron que colapsó en 2001, marcando la mayor quiebra en la historia de Estados Unidos, resultado de un sofisticado esquema de fraude diseñado por sus ejecutivos. (Pareja, 2022).

Otro caso similar es el escándalo contable de WorldCom (2005), la segunda mayor empresa de telefonía de larga distancia en Estados Unidos, que se declaró en quiebra en 2002 tras revelarse un inflado de sus activos por 11,000 millones de dólares a través de prácticas contables dudosas por parte de sus altos ejecutivos. (Mantilla Falcón y Medina Espín, 2019).

Mendoza (2009) argumenta que el término fraude no se limita al ámbito de la gerencia o a las empresas que buscan obtener beneficios personales, sino que también puede surgir del egoísmo que lleva a desviar recursos hacia un grupo privilegiado, este tipo de fraude puede ser perpetrado tanto por empleados públicos como privados, manifestándose de forma intencionada o por negligencia, asimismo, podría ocurrir entre las mismas personas que trabajan dentro de la entidad reguladora, lo cual podría ocasionar grandes distorsiones en los estados financieros con el fin de maximizar el valor empresarial incluso si este es ficticio. (Cárdenas-Pérez, Benavides-Echeverría y Chango-Gala, 2021)

El concepto de fraude no se limita a la alteración de los estados financieros, ya que puede manifestarse en diversas áreas de las empresas, no solo implica la violación o el uso inapropiado de las políticas contables sino que también afecta otros principios fundamentales y pilares de las propias organizaciones, por esta razón, es crucial entender qué factores llevan a los contadores públicos a involucrarse en este tipo de delitos. (Hernández, 2018).

Martans (2012) se ha enfocado en un significado más ético del fraude financiero, definiéndolo como un medio para obtener beneficios a expensas de terceros mediante el engaño, asimismo señala que se trata de una acción que va en contra de la verdad y la transparencia, perjudicando a una persona o empresa esta definición sugiere que más allá de las acciones específicas involucradas en los fraudes financieros, lo que

realmente importa es que estas conductas son antiéticas y ponen en duda la integridad profesional de quienes son responsables.

Otros autores basan las definiciones en el actuar de las personas, un ejemplo claro es planteado por quien afirma que los fraudes financieros son delitos de gente inteligente avezada en los negocios, conocedora de las leyes y reglamentos y de las artimañas para eludir sanciones influyentes por su poder corruptor y que tiene relaciones mundanas, políticas y con los funcionarios. (Miranda, 1970).

Por su parte Enobong (2017) se centra en señalar que las conductas antiéticas de los profesionales tienen consecuencias perjudiciales, especialmente para las organizaciones ya que pueden provocar pérdidas económicas y escándalos financieros.

Según las definiciones presentadas y de acuerdo con la NIA 240 (2014), es posible profundizar en algunas de las técnicas comúnmente empleadas para perpetrar fraudes financieros tales como:

- Modificación, alteración o cambio de documentos administrativos o financieros.
- Falsificación de transacciones, situaciones o cualquier informe económico relevante.
- Presentación de información financiera con ajustes no justificados.
- Registro de asientos contables falsos o modificados en los libros.

A lo largo de la historia, han ocurrido varios escándalos financieros vinculados al fraude, los cuales evidencian principalmente debilidades institucionales que impactan directamente en los modelos económicos de los países afectados, estos problemas a menudo han llevado a la quiebra de empresas, lo que a su vez contribuye a un aumento en la tasa de desempleo. (Rodríguez Gómez, 2022).

En términos generales los casos de fraude que han sido expuestos están relacionados con diversos problemas económicos o financieros, incluso en gobiernos de países desarrollados, sin embargo, el concepto de fraude tiene una explicación más

amplia ya que según The Financial Crime Academy se trata de un acto intencional llevado a cabo por la gerencia o el personal de una empresa, con el objetivo de obtener un beneficio personal o grupal. (FCA, 2023). Este tipo de violaciones tiene un impacto significativo en los estados financieros, al distorsionar la información presentada, resulta importante distinguir que un error es un acto resultado de olvido o incompetencia, y suele tener efectos mínimos en los estados financieros. (Cando-Morejon et al., 2023).

El fraude puede definirse como un engaño destinado a obtener una ventaja injusta, generalmente de carácter financiero, sobre otra persona. Las distintas tipologías de fraude se pueden clasificar de diversas maneras, incluyendo: reclamaciones fraudulentas, manipulación del mercado, venta de valores falsificados, usurpación de identidad, robo de recursos, entre otros. (Kratcoski y Edelbacher, 2018).

El fraude es un fenómeno complejo que ha sido objeto de un extenso análisis tanto académico como en el ámbito operativo de las organizaciones donde este fenómeno se manifiesta con creciente frecuencia, se trata de un comportamiento incivilizado que se presenta no solo en ciertos ciudadanos, sino también en la propia administración y en el marco legal. (De la Torre, 2023).

Es fundamental considerar que, a nivel global, el fraude en las empresas ha aumentado debido a la facilidad con la que puede llevarse a cabo y a la ausencia de controles efectivos por parte de la dirección, la tecnología actual ha facilitado en gran medida la expansión de las organizaciones, pero también ha proporcionado un medio y una herramienta para llevar a cabo actividades y esquemas fraudulentos. (Grillo et al., 2019).

Torres (2018) propone cuatro componentes que de alguna manera, agrupan los elementos mencionados anteriormente a través del triángulo del fraude, estos componentes son: *presión, oportunidad, racionalización y proceso*

La negligencia y la falta de competencia de los profesionales son factores que abarcan diversos aspectos, como la avaricia y la competencia desleal, lo cual se debe, en parte, a la inadecuada remuneración que impacta en la satisfacción de las necesidades económicas de los contadores públicos y fomenta una cultura de búsqueda de ganancias rápidas. (López y Sánchez 2011).

Las medianas y grandes empresas son vistas como importantes generadoras de empleo a nivel global, su estructura empresarial ha sido objeto de numerosos estudios a lo largo de los años, y estos análisis han demostrado que la corrupción persistente, el fraude corporativo y otros incidentes perjudiciales afectan gravemente la confianza en muchas compañías, lo que a su vez provoca pérdidas económicas significativas. (De La Torre 2023)

Generalmente, cuando las empresas están involucradas en un fraude, su reputación se ve gravemente afectada, lo que resulta en una caída inmediata en el precio de sus acciones y puede llevar a una crisis financiera, un ejemplo de esto es el conocido caso de Parmalat que tuvo un impacto económico equivalente al 1% del Producto Interno Bruto (PIB) de Italia, además de la pérdida de proveedores e inversores en materias primas. (BBC Mundo, 2022).

En América Latina, Brasil es el país que presenta el mayor índice de fraude en el sector financiero, siendo parte de uno de los siete grupos de estafas financieras más comunes: Besta Fera, Banbra, Ponteiro, Passteal, Javali, Casbaneiro y Vadokrist; el caso más reciente es el de Ponteiro, donde se detectaron archivos maliciosos en 2022, lo que llevó a añadir 30 nuevos nombres a la lista inicial de 70 bancos que eran objetivos de este grupo. (Restrepo, 2022).

El fraude digital se refiere a los crímenes realizados a través de Internet, donde los ciberdelincuentes emplean diversas técnicas, como la clonación de tarjetas, el

hacking de cuentas, el phishing, el vishing y el smishing, para engañar a las víctimas y robar información personal, como contraseñas y datos de tarjetas de crédito, el objetivo de estas acciones es estafar o aprovecharse de las personas. (De La Torre 2023)

II. MATERIALES Y METODOS

La investigación fue de carácter básico y descriptivo, centrada en profundizar el entendimiento de la normativa que regula las figuras de dinero digital y fraude financiero. El investigador examinó la información y los datos disponibles sobre el tema en cuestión. El estudio se estructura en dos secciones: la primera detalla lo que entendemos por dinero digital, sus características, tipos, y ventajas. La segunda parte desarrolla temas como el fraude financiero.

La investigación se sustentó en documentos de diversas fuentes, como artículos, informes, normas, etc. Sobre fraude financiero.

En la fase descriptiva inicial, se utilizó el análisis documental y se hizo uso de fichaje como instrumento principalmente utilizado.

III. RESULTADOS

OG

Figura 3

Implicancias del dinero digital en el fraude financiero



Nota: Elaboración propia

OE1

1. Factores de Riesgo

Los factores de riesgo en el fraude financiero se pueden clasificar según el Triángulo del Fraude, que incluye:

- **Presión:** Circunstancias que llevan a una persona a cometer fraude, como problemas financieros personales o presiones laborales para cumplir con expectativas de rendimiento, la cual puede ser externa, como la exigencia de resultados por parte de accionistas o la situación económica de la empresa.
- **Oportunidad:** La capacidad de cometer fraude sin ser detectado, que puede surgir de debilidades en los controles internos de una organización. Un sistema de control interno robusto puede reducir significativamente este riesgo
- **Racionalización:** La justificación que el defraudador se da a sí mismo para cometer el fraude, como la creencia de que está siendo tratado injustamente o que el fraude es aceptable en su entorno

2. Tecnología y Ciberseguridad

La evolución tecnológica ha permitido que los métodos de fraude se vuelvan más sofisticados, sin embargo, también ha proporcionado herramientas para combatirlo, como la inteligencia artificial (IA), que permite analizar grandes volúmenes de datos en tiempo real, identificar patrones sospechosos y tomar decisiones rápidas para prevenir fraudes, la IA también ayuda en procesos de verificación de identidad y cumplimiento normativo, lo que es crucial para prevenir el lavado de dinero y otros delitos financieros.

3. Normativas y Cumplimiento

Las regulaciones y normativas son fundamentales en la lucha contra el fraude financiero. La implementación de leyes como en el caso de España, que establece medidas para prevenir el fraude fiscal, es un ejemplo de cómo la legislación puede ayudar a mitigar estos riesgos, las organizaciones deben cumplir con estas normativas para evitar sanciones y mantener la integridad de sus operaciones.

4. Educación y Capacitación

La formación continua del personal es esencial para prevenir el fraude, programas de capacitación que enseñan sobre las mejores prácticas en la detección y prevención de fraudes contribuyen a crear una cultura de integridad dentro de las organizaciones, la educación financiera también es clave para que los empleados y clientes reconozcan señales de alerta y eviten caer en fraudes.

5. Monitoreo y Auditoría

El monitoreo efectivo de transacciones y la realización de auditorías internas y externas son prácticas cruciales para detectar irregularidades y prevenir fraudes, estas medidas permiten identificar actividades sospechosas y tomar acciones correctivas de manera oportuna

6. Cultura Organizacional

Fomentar una cultura ética dentro de la organización es vital, un código ético sólido que promueva la transparencia y la responsabilidad puede ayudar a prevenir conductas fraudulentas, la presión para cumplir con metas poco realistas puede llevar a comportamientos deshonestos, por lo que es importante establecer expectativas razonables.

OE2

La Ley N° 30096, Ley de Delitos Informáticos, establece diversas conductas ilícitas y las sanciones correspondientes.

1. **Acceso no autorizado** la cual se ejecuta al ingresar a un sistema informático, red o base de datos sin autorización del titular.
2. **Interferencia**, se configura al dañar, modificar o destruir datos, programas o sistemas informáticos ajenos.
3. **Uso indebido de datos**, a evidenciarse el aprovechamiento de información reservada o confidencial sin el consentimiento del titular.
4. **Delitos relacionados con el phishing** se cumple al realizar suplantación de identidad para obtener información personal o bancaria.
5. **Hacking** se evidencia al realizar actitudes que comprometan la seguridad de los sistemas informáticos, como la intrusión y el acceso no autorizado.
6. **Distribución de malware** se configura al crear, utilizar o difundir software malicioso con el fin de causar daño o acceder a información sin autorización.
7. **Fraude informático** se tipifica al utilizar medios electrónicos para engañar a personas y obtener un beneficio económico.

OE3

Figura 4

Formas más comunes de fraude financiero en Perú

Phishing:	<ul style="list-style-type: none">• Los delincuentes envían correos electrónicos o mensajes de texto haciéndose pasar por bancos o entidades financieras, solicitando información personal y contraseñas.
Suplantación de identidad:	<ul style="list-style-type: none">• Los estafadores utilizan la información de una persona para abrir cuentas bancarias o solicitar créditos a su nombre.
Estafas por venta de productos:	<ul style="list-style-type: none">• En ocasiones, se ofrecen productos a precios muy bajos a través de redes sociales o plataformas de comercio electrónico, pero nunca se entregan.
Skimming:	<ul style="list-style-type: none">• Instalación de dispositivos en cajeros automáticos para copiar la información de las tarjetas de débito o crédito.
Créditos falsos:	<ul style="list-style-type: none">• Ofertas engañosas de créditos de fácil acceso que requieren un pago inicial y luego desaparecen.
Inversiones fraudulentas:	<ul style="list-style-type: none">• Ofrecen rendimientos altos y rápidos, especialmente en criptomonedas o proyectos de inversión que no existen.
Fraude en telecomunicaciones:	<ul style="list-style-type: none">• Llamadas telefónicas donde se ofrecen servicios o ganancias falsos, solicitando dinero adelantado o datos personales.

Nota: Elaboración propia

IV. DISCUSION Y CONCLUSIONES

Discusión

Se ha comprobado que la volatilidad de la moneda digital no es tan alta, lo que tiene un impacto significativo en su uso en el mercado financiero, este hallazgo coincide con la investigación de Cuentas y Paredes (2020), quienes en su estudio, afirman que la moneda digital es una forma de dinero digital bastante accesible para la población lo que produce efectos beneficiosos en el sistema financiero.

La actividad financiera se beneficia de la introducción de herramientas innovadoras y accesibles para las personas, así como de un control eficiente de los riesgos crediticio, lo cual se alinea con la investigación de Figueroa et al. (2019), titulada *Buenas Prácticas Financieras en la Gestión del Riesgo de Crédito de Empresas del Sector Bancario*, en la que se han creado modelos sofisticados para medir y mitigar los riesgos asociados al crédito.

Se ha demostrado que la actividad financiera se fortalece y complementa con la implementación de medidas de ciberseguridad, lo que genera confianza y seguridad en las personas, lo cual se coincide con la investigación de Becerra (2022) titulada *Innovación en pagos digitales en el Perú: Retos al 2030*, en la cual se señala que las transacciones digitales cuentan con las medidas de ciberseguridad necesarias, lo que permite brindar tranquilidad a los usuarios y los lleva a preferirlas sobre las transacciones en efectivo.

Los fraudes financieros que han afectado a diversas organizaciones a nivel mundial en los últimos años han planteado importantes interrogantes sobre la responsabilidad de los profesionales contables y su papel en la prevención y detección de estos delitos, como resultado, el Estado, las entidades económicas y las instituciones profesionales están preocupados por la persistente aparición de fraudes financieros y la

falta de mecanismos para detectarlos a tiempo, esto ha llevado a enormes pérdidas económicas, financieras y sociales para todos los involucrados, por esta razón es fundamental entender los factores relacionados con estos fraudes financieros.

Se pudieron identificar, desde diversas perspectivas, varios elementos que influyen en la comisión de fraudes financieros por parte de los profesionales de la contaduría, un aspecto destacado es que los contadores públicos pueden verse involucrados en estos delitos debido a factores internos relacionados con su personalidad y a factores externos derivados de las condiciones que enfrentan en su vida cotidiana, además menciona que entre los factores internos se encuentran la disonancia cognitiva, la intención de engañar, el deseo de poder la falta de motivación en el trabajo, la ausencia de racionalidad, el anhelo de satisfacer intereses personales y, finalmente, la falta de conciencia social. (Sánchez, Valencia y Saldarriaga, 2012).

Además, existen factores externos que facilitan la ocurrencia de estos delitos, como los descuidos intencionados, las oportunidades que surgen, la presión laboral de terceros, la excesiva confianza en los profesionales y los incentivos económicos que puede ofrecer un fraude financiero así, se puede concluir que los principales elementos que se manifiestan en la realización de fraudes financieros son: la oportunidad, la presión y la racionalización, que en conjunto forman el triángulo del fraude. (López y Sánchez, 2011).

No obstante, Huber (2017) respalda esta teoría desde la perspectiva de la contabilidad forense, señalando que estos elementos facilitan la comisión de delitos financieros, menciona también que la negligencia de los profesionales incluye varios factores, como la avaricia, la competencia desleal y la falta de integridad, también destaca que los bajos salarios afectan la satisfacción de las necesidades económicas de los contadores, lo que alimenta una cultura de búsqueda de dinero fácil, por último establece que la falta de competencia se relaciona con aspectos como la complejidad

de la información, la debilidad en el control interno y la incorrecta interpretación de criterios contables.

Conclusiones

1. El dinero digital es más vulnerable a fraudes como phishing y hacking, permitiendo a los delincuentes realizar transacciones de manera rápida y menos detectable. Además, su alto nivel de anonimato dificulta el rastreo de los criminales, lo que puede fomentar actividades delictivas. La evolución del dinero digital ha generado nuevas modalidades de fraude, como tokens falsos y manipulación de contratos inteligentes, lo que exige que tanto instituciones financieras como usuarios estén al tanto de las nuevas amenazas, asimismo, la naturaleza transnacional del dinero digital presenta retos para la regulación, ya que las diferencias normativas entre países pueden ser aprovechadas por los delincuentes para cometer fraudes a gran escala y por último, tenemos que muchos usuarios carecen de la educación financiera necesaria para reconocer riesgos y proteger sus activos, lo que los hace más vulnerables a estafas, especialmente en el ámbito de las criptomonedas.

2. La lucha contra el fraude financiero requiere un enfoque multifacético que incluya la identificación de factores de riesgo, el uso de tecnología avanzada, el cumplimiento normativo, la educación continua, el monitoreo efectivo y la promoción de una cultura organizacional ética.

3. La Ley N° 30096, Ley de Delitos Informáticos, define varias conductas ilícitas y sus respectivas sanciones tales como el acceso no autorizado, la Interferencia, el uso indebido de datos, delitos de phishing, hacking, distribución de malware y fraude informático

4. Los delincuentes utilizan diversas tácticas para defraudar a las personas, a través de phishing envían correos electrónicos o mensajes de texto haciéndose pasar por bancos o entidades financieras para solicitar información personal y contraseñas, la

suplantación de identidad implica el uso de datos de una persona para abrir cuentas bancarias o solicitar créditos a su nombre, el skimming se refiere a la instalación de dispositivos en cajeros automáticos para copiar la información de tarjetas de débito o crédito y por ultimo tenemos los créditos falsos que prometen fácil acceso a préstamos a cambio de un pago inicial, tras el cual desaparecen.

V. REFERENCIAS

- Cueva (2021) en su tesis titulada “Las Fintech como alternativa de inclusión financiera en Ecuador”.
- Fernández & Gouveia (2019) “Monedas digitales emitidas por bancos centrales: características, opciones, ventajas y desventajas” BBVA Research. España.
- González-Páramo (2019), “La digitalización del dinero”
- Grillo, O., Rivoir, A. y Morales, M. J. (2019). Tecnologías digitales: Miradas críticas de la apropiación en América Latina. CLACSO. <http://biblioteca.clacso.edu.ar/clacso/se/20191128031455/Tecnologias-digitales.pdf>
- Ignacio (2018). “Estrategia digital de la industria financiera, escenarios de competencia de bancos tradicionales con nuevos actores Fintech”.
- Lla Sihuincha et al (2022) “Convergencia tecnológica y su impacto en el sistema financiero digital global”
- López (2020) “La Revolución de Las Nuevas Monedas”. El País. España
- González-Millan & Guardiola-Plazas (2019) “La confiabilidad en las monedas digitales como inversión práctica en la economía del futuro” Universidad Francisco de Paula Santander
- Mantilla Falcón, L. M. y Medina Espín, P. G. (2019). Riesgo operativo y fraudes financieros en el sector cooperativo del segmento 3 y 4 del cantón Ambato. (Tesis de pregrado, Universidad Técnica de Ambato). <https://repositorio.uta.edu.ec/jsp>
- Martínez (2018) “Big Data Aplicado En El Sector Bancario Tradicional Para Lograr Una Mayor Ventaja Competitiva Frente A Las Fintech”.

Pedrosa & Perossa (2021), "Dinero fiduciario, dinero virtual y criptomonedas: 143 Semejanzas y diferencias".

Quiroz Peña, J. (2023). Cibercrimen y su asociación en el cometimiento de fraudes financieros en la pandemia de la COVID-19. Revista Venezolana de Gerencia, 28(102), 609-628.
<https://doi.org/https://doi.org/10.52080/rvgluz.28.102.11>

Ruiz (2020) "Avances en la introducción de monedas digitales de Banca Central" Banco Central de Reserva del Perú. Perú.

Sánchez (2019) en su tesis titulada "Billetera Virtual ventajas y desventajas de su implementación en Argentina

Trond (2019) "Aprovechar el dinero digital del Banco Central para estimular la actividad económica doméstica" Universidad Nacional Autónoma de México. México.