La psicología de la víctima de un fraude financiero: aplicaciones generales para El Salvador

The psychology of the victim of financial fraud: general applications for El Salvador

Nelson Ernesto Rivera Díaz[25]
Universidad de El Salvador
ORCID 0000-0001-5344-4295
Katya Eugenia Alfaro Delgado[26]
Psicóloga clínica
ORCID 0009-0008-7633-4847

Fecha de recepción 11/08/2025 **Fecha de evaluación 1/09/2025**

Resumen

El artículo analiza la psicología de las víctimas de fraude financiero, abordando la influencia de aspectos emocionales, sociales y tecnológicos sobre las condiciones de vulnerabilidad potencial. Se destaca que, aunque existen señales de alerta claras, muchas víctimas aún caen en esquemas sofisticados debido a factores como la baja estabilidad emocional y decisiones irracionales. Se realiza un repaso por las principales modalidades de fraude vigentes, como los esquemas piramidales y las estafas digitalizadas mediante plataformas pseudocriptográficas y ataques cibernéticos, con especial atención en la situación salvadoreña; además, se enfatiza la importancia de la conciencia y educación del usuario como primera defensa, reconociendo que la sofisticación de los métodos delictivos desafía

[25] Nelson Ernesto Rivera Díaz: licenciado en Relaciones Internacionales, máster en Finanzas y Economía, máster en Geopolítica, Conflictos Armados y Cooperación Internacional, con posgrados en Educación Financiera, Finanzas Personales y Finanzas para la Toma de Decisiones. Docente universitario, investigador científico certificado por el CONACYT, consultor empresarial y autor de varios libros sobre economía, finanzas y criptoactivos. ernesto.rivera@ues.edu.sv

[26] Katya Eugenia Alfaro Delgado: licenciada en Psicología, autorizada por la Junta de Vigilancia de la Profesión en Psicología. Con experiencia en perfilamiento profesional, reclutamiento, gestión del capital humano y manejo de entornos educativos para discapacidad cognitiva. Se desempeña como psicóloga en su propia clínica. psicologia.kead@gmail.com

los esfuerzos preventivos. En consecuencia, se resalta la necesidad de un enfoque multidisciplinario para estudiar y enfrentar el flagelo, integrando el rol de las características psicológicas como catalizador de vulnerabilidad, pudiendo llegar a conclusiones acerca de la necesidad de integrar aspectos psicológicos en la educación para la prevención de fraudes financieros.

Palabras clave: estafa, fraude financiero, psicología, comportamiento humano

Abstract

The article examines the psychology of financial fraud victims, addressing the influence of emotional, social, and technological factors on potential vulnerability conditions. It highlights that, despite the presence of clear warning signs, many victims still fall prey to sophisticated schemes due to factors such as low emotional stability and irrational decision-making. The study reviews the main current forms of fraud, including pyramid schemes and digitalized scams conducted through pseudo-cryptographic platforms and cyberattacks, with an special attention about the Salvadoran situation. Furthermore, it emphasizes the importance of user awareness and education as the first line of defense, while acknowledging that the increasing sophistication of criminal methods challenges preventive efforts. Consequently, the article underscores the need for a multidisciplinary approach to study and combat this issue, incorporating the role of psychological traits as catalysts of vulnerability, and concludes with the recommendation to integrate psychological aspects into educational strategies for financial fraud prevention.

Keywords: scam, financial fraud, psychology, human behavior

INTRODUCCIÓN

Los fraudes financieros son, en esencia, delitos que implican la pérdida de activos de la víctima, producto de un engaño. Dicho flagelo ha existido por siglos; sin embargo, la tecnologización de las finanzas ha facilitado los medios y recursos para que los ampones sofistiquen sus métodos, llevando el nivel de dificultad de prevención y persecución del delito a niveles que superan las posibilidades de los Estados y demás entidades financieras,

por lo que buena parte de la responsabilidad profiláctica recae en el cuido que el usuario tenga de sus propias operaciones.

De hecho, estudios revelan que las víctimas más propensas a caer en este tipo de fraudes tienen características comunes, especialmente en lo referente a su edad (Internet Crime Complaint Center, 2023a; Pérez Martínez & López Pérez, 2023), nivel educativo (Angulo-Rangel et al., 2023; DeLiema et al., 2020) y situación económica (Anguita-López, 2022; Castagno et al., 2025; Wang et al., 2021). En todo caso, la relación entre el perfil psicológico de la víctima potencial y su propensión a ser estafada guardan una cercanía importante la cual está determinada, en su mayoría, por factores estimulantes externos que inhiben la capacidad de alerta (Kemp & Moneva, 2020), teniendo una incidencia muy clara sobre otros aspectos de la salud y la calidad de vida previa y posterior a ser víctima del fraude (Herrera-Deyta, 2025; Rodríguez-Rodríguez et al., 2020).

Muy buena parte de las operaciones financieras realizadas autónomamente por el usuario resultan gestionadas por medios electrónicos, aunque las modalidades de estafa y fraude transitan con libertad entre el mundo tangible y el *metaverso*. En todo caso, los ataques cibernéticos difícilmente vayan a poder ser controlados o prevenidos por el usuario común, siendo que requieren de un nivel de sofisticación especializada en el campo de la informática. Diversos estudios en América Latina revelan que hay países que tienen una gestión bastante efectiva del fraude transaccional electrónico, destacando países que entre 2023 y 2024 alcanzaron cifras aceptablemente mínimas tales como Colombia con un 7.1 % de transacciones fraudulentas (Rodríguez-Martínez, 2024), Ecuador con un 8.1 % (Maldonado-Guñido et al., 2024) o República Dominicana con un 10.4 %, frente a un preocupante promedio latinoamericano del 20.2 % (Allende, 2024; Casanova-Villalba & Casanova-Villalba, 2024), según registros obtenidos de las empresas privadas proveedoras de servicios transaccionales.

Pese a no tener pleno control acerca de los fraudes producto de los ataques cibernéticos, el usuario igualmente puede verse vulnerado por otro tipo de tácticas de engaño que no atacan por el lado de la tecnología, sino por el lado de la desidia del usuario por gestionar su propia seguridad. Por ejemplo, Interpol reporta que, de los fraudes

financieros procesados, solo el 22 % representa causales estrictamente cibernéticas, dejando el resto en causales tales como el *phishing*, la ingeniería social y las *fake news* (Secretaría General de INTERPOL, 2020). *A priori*, dicha proporción revela que la responsabilidad de la mayoría de fraudes recae en el usuario, dejando expuesta su ignorancia y/o negligencia al defenderse de los múltiples ataques, siendo que ser víctima depende necesariamente de su propia educación (Rivera-Díaz, 2022). Sin embargo, dicha explicación resulta simplista, considerando que el comportamiento humano depende de múltiples factores, por lo que es muy probable que las causales de la victimización vayan más allá del conocimiento del individuo acerca de los riesgos, extendiéndose hasta las razones psicológicas que le mueven a tomar decisiones que ignoran los riesgos cada vez más evidentes (Kemp & Moneva, 2020).

METODOLOGÍA

La presente investigación se enmarca en un **diseño metodológico teórico-documental de tipo estado del arte**, orientado a la revisión, análisis e interpretación de los aportes científicos disponibles sobre la psicología de la víctima de fraude financiero. Su finalidad principal es **sistematizar los hallazgos teóricos y empíricos existentes** para comprender los procesos cognitivos, emocionales y conductuales que explican la vulnerabilidad de las personas ante este tipo de delitos, a la luz de los factores económicos y legales intervinientes.

El estudio se desarrolló bajo un **enfoque cualitativo**, centrado en el análisis conceptual y la integración de perspectivas provenientes de la psicología social, cognitiva y del comportamiento financiero. No se recolectó datos empíricos o primarios siendo que, como se expresa en el artículo, no se cuenta con una base de datos oficial al respecto de los fraudes financieros; en cambio, se recurrió a fuentes secundarias especilalizadas, seleccionadas a partir de su relevancia teórica y metodológica para la comprensión del fenómeno.

El proceso metodológico siguió tres etapas principales:

Revisión y selección de literatura especializada: se realizó una búsqueda en bases de datos académicas e institucionales, priorizando aquellas fuentes que proveyesen de estudios previos o de estadística nacional e internacional que permitiese relacionar a al fraude, la víctima y su comportamiento.

Análisis temático y categorización conceptual: las fuentes seleccionadas se organizaron según categorías lógicas, entre ellas *procesos cognitivos implicados en el engaño, emociones asociadas a la victimización, percepción del riesgo financiero y estrategias de manipulación utilizadas por los delincuentes.*

Integración de hallazgos: se elaboró una interpretación crítica de los principales modelos teóricos identificados, destacando las coincidencias, tensiones y vacíos existentes en la literatura sobre el perfil psicológico de las víctimas en relación con la información oficial y políticas públicas salvadoreñas.

De esta manera, el estudio no pretende validar hipótesis mediante mediciones empíricas, sino **proporcionar una visión integradora del conocimiento actual** sobre los mecanismos psicológicos que intervienen en la victimización por fraude financiero. Este enfoque permite reconocer patrones cognitivos y emocionales recurrentes que, al ser comprendidos, pueden orientar investigaciones futuras y contribuir al diseño de estrategias de prevención basadas en la comprensión del comportamiento humano.

RESULTADOS Y DISCUSIÓN

Conceptualización del fraude financiero

El fraude financiero es un flagelo multimodal y multicausal, que consiste en utilizar diversas técnicas de engaño con el fin de vulnerar la seguridad de la patrimonialidad financiera de las víctimas, despojándoles de activos que difícilmente lograrán recuperar, y cuya persecución del delito es, cuando menos, difícil de realizar. A diferencia de la defraudación financiera, en la que la base es la asimetría injusta entre actores económicos, toda modalidad de fraude tiene como fundamento la ingenuidad, ignorancia, convicción, buena

fe, ambición o apetito de riesgo de la víctima, pudiendo incluso llegar a combinar varias de esas causales. Por tanto, cuando un fraude financiero es cometido, la tecnología y los múltiples métodos de ciberataque juegan un papel meramente de catalizador, siendo que el verdadero combustible del fraude es la propia víctima y su incapacidad para responder al engaño de forma segura.

La comisión del fraude implica una serie de consideraciones técnicas y legales, aunque el factor común siempre es la exposición de escenarios no verificables pero plausibles, los cuales fungen como camino de la víctima hacia la pérdida de sus activos. Por tanto, es bien sabido que los perpetradores de los fraudes tiran de creatividad para generar condiciones engañosas, confusas y basadas en el efecto el efecto especulativo como una plataforma inestable para los usuarios menos cautos. Desde luego, el nivel de caución por parte del usuario de los servicios financieros no proviene de la espontaneidad, sino que depende de múltiples factores, preponderando la educación financiera y de gestión de riesgos que el individuo haya adquirido.

En tal sentido, podría decirse que el fraude financiero requiere de dos actores mínimamente; por un lado, el estafador que provoca una realidad engañosa; y, por otro, el estafado, quien cae en la trampa. Sin embargo, cuando se trata de pillaje por la vía de la ingeniería social, el *phishing* y las *fake news*, se requiere de la complicidad histórica de todo un modelo educativo inoperante que privó a los individuos de la consciencia de gestión de riesgos, lo cual les vuelve vulnerables. Desde luego, la educación no es suficiente para realizar la prevención, siendo que existen factores individuales que, pese a visualizar los riesgos, igualmente impulsan al individuo a ponerse en peligro a sí mismo.

Desde luego, los fraudes, pasa ser tipificados como tal, deben existir en un ecosistema jurídico que les puna, por lo que la complejidad y eficiencia legislativa juegan un papel crucial en la mitigación de riesgo de fraudes; sin embargo, no basta con un marco regulatorio, sino con un esquema de persecución del delito que sea capaz de fungir desde la disuasión hasta la condena, lo cual requiere de una capacidad investigativa para la recaudación de pruebas, lo cual suele complicarse por la facilidad que la tecnología brinda para el encubrimiento.

En este caso, la incipiente y trepidante aparición de las criptofinanzas acaban por complicar la labor de persecución del delito, proveyendo al estafador de recursos sumamente efectivos para garantizar su anonimato y, por consecuencia, no rastreabilidad. Dicha condición vuelve incluso más curiosa la situación de las víctimas, ya que tienden a confiar a ciegas en promesas de ganancia que provienen de alguien desconocido y que, por el mismo sistema críptico, tampoco podrán identificar en caso de ser necesario. Pese a dicha condición de incertidumbre, a una década de su entrada en el mercado, las criptomonedas alcanzaron cifras superiores al 70000 % de capitalización (Bermúdez Pacheco et al., 2021), demostrando que los usuarios le dan poca importancia a la identidad del socio con quien hace negocios, siempre que pueda percibir la posibilidad de una ganancia; esto, pese a que, en el mismo periodo de tiempo, se registraron pérdidas por más de 584 millones de dólares producto de ataques cibernéticos a las plataformas de criptomonedas (Mena Roa, 2021), lo cual pone en perspectiva una relación riesgo/beneficio bastante cuestionable de acuerdo a la Matriz de Riesgo Financiero parametrizada según la norma ISO 31000 acerca de la prevención de lavado de dinero y activos, la cual situaría el riesgo en una magnitud de vulnerabilidad del 20 %, catalogándola como inadmisible (Cox et al., 2005; Orellana-Osorio et al., 2019).

Y, pese a la alerta estadística de gestión del riesgo, el uso de criptoactivos no para de crecer junto a otros muchos medios tecnológicos que propician el fraude (Castillo-Tapuy & Montenegro-Ramírez, 2022), por lo que vale la pena cuestionarse acerca de cuáles son los factores que influyen para que el usuario de servicios financieros ignore la evidencias técnicas y empíricas, y se ponga en peligro a sí mismo.

Principales métodos de fraude financiero

Las modalidades de fraude financiero han evolucionado de forma adaptativa al entorno social, económico y tecnológico, por lo que sería contraproducente analizar los métodos utilizados por los ampones sin un contexto temporal definido. Hacia los albores de la segunda década del siglo XX, se registra que el 64.2 % de la población global hace uso regular y prioritario de los medios electrónicos para el manejo de sus finanzas, a pesar de que la

misma muestra expresó aún preferir el efectivo en un 79.4 % (Castro-Badillo et al., 2022), lo cual genera un contraste disociativo entre la práctica financiera y lo que a la población le gustaría conservar como práctica personal. En ese contexto, vale la pena enfocar los esfuerzos por categorizar los principales métodos de fraude financiero en un marco referencial de la tecnología financiera, a sabiendas de que las prácticas financieras tradicionales continuarán existiendo por algún tiempo, pero que tienen una clara tendencia a la extinción.

Visto el escenario de preponderancia tecnológica, resulta necesario comprender los fraudes que están más bien relacionados a la seguridad informática. Los fraudes financieros por ataque de *malware* son una forma de ciberdelito que implican el uso de software malicioso para robar información sensible, como datos bancarios, contraseñas y otros tipos de información financiera, con el fin de cometer fraudes (Amro, 2018). En este caso, el *software* es diseñado específicamente para infiltrarse en sistemas informáticos con el fin de obtener información financiera confidencial, manipular transacciones o desviar fondos sin autorización. Este fenómeno es especialmente relevante en el ámbito financiero moderno, donde la digitalización de las operaciones y la interconectividad de los sistemas bancarios han incrementado la exposición a ciberamenazas (Aguilar-Antonio, 2020; Manoharan & Sarker, 2024), destacando los malware tales como Troyanos bancarios, *Spyware*, *Ransomware* y *Man-in-the-Browser* (De La Torre Lascano & Quiroz Peña, 2023; Flores-Álava & Mena-Hernández, 2023; López-Pincay et al., 2024):

Una vez comprendida la conceptualización básica de las herramientas tecnológicas para la comisión de fraudes financieros, debe explorarse los diferentes tipos de estafas existentes y que suelen utilizar el *malware* como recurso para consumar el delito.

Phishing: es una técnica de ingeniería social utilizada para obtener información confidencial de manera fraudulenta, con el objetivo de cometer delitos financieros. El término deriva del inglés *fishing* (pescar), haciendo alusión a la práctica de “pescar” víctimas mediante cebos engañosos. En términos técnicos, el phishing consiste en el uso de medios electrónicos tales como correo electrónico, mensajes de texto (SMS), llamadas telefónicas o sitios web falsificados, para engañar al usuario y hacer que revele datos sensibles como

contraseñas, números de tarjetas de crédito, información bancaria o credenciales de acceso a plataformas financieras. El proceso típico de phishing se inicia con un mensaje que aparenta provenir de una entidad legítima, como un banco, una empresa de tecnología o un organismo gubernamental, soliendo incluir logotipos, lenguaje y formatos visuales similares a los de las instituciones que suplantan, y contienen enlaces a páginas web falsas (clonadas o simuladas) que solicitan al usuario introducir sus datos personales. Una vez que la víctima proporciona la información, ésta es recolectada por los ciberdelincuentes y utilizada para realizar transferencias no autorizadas, compras fraudulentas o incluso suplantaciones de identidad más complejas.

El desarrollo de las inteligencias artificiales ha permitido que se vaya sofisticando la modalidad, haciendo que la "pesca" sea cada vez más verosímil, pasando de modalidades muy primitivas como la imitación de sitios web a versiones como la sinterización de voz y robo de tarjeta SIM. Algunos indicios de alerta acerca de este tipo de estafa son la existencia de direcciones de correo electrónico o URL sospechosas, mal escritas, o con caracteres poco comunes; orografía y gramática errada o poco natural en el mensaje; solicitudes urgentes y perentorias, especialmente si vienen acompañadas de una amenaza de bloqueo inmediato de la cuenta; peticiones inusuales de información confidencial, especialmente si ésta ya se ha proporcionado antes a la entidad financiera; y, especialmente, la presencia de archivos adjuntos con extensiones extrañas o enlaces acortados (Moncada-Vargas, 2020).

Pirámides (Ponzi): son esquemas fraudulentos de captación de dinero que prometen altos rendimientos económicos con poco o ningún esfuerzo, cuya liquidez se sustenta en la incorporación continua de nuevos participantes. Técnicamente, se trata de un modelo insostenible en el que los pagos a los inversores más antiguos se financian con el dinero aportado por los nuevos, sin que exista una actividad económica real que respalde las ganancias prometidas. Desde el punto de vista financiero, estas estafas no generan valor real ni retorno legítimo de inversión, y el modelo colapsa inevitablemente cuando se agota la capacidad de reclutar nuevos miembros, dejando a la mayoría de los participantes con pérdidas significativas. Con el tiempo se han ido sofisticando, partiendo desde modalidades de membresía a un fondo de inversión, hasta la instalación de pseudonegocios con

productos ficticios o sobrevaluados y, más recientemente, la inclusión de plataformas digitales de inversión pseudocríptica que facilitan la estafa al tokenizar la participación de las víctimas.

Algunas claras señales de alerta son el requerimiento de una membresía para pertenecer a un nivel específico de privilegio en el negocio; un énfasis extremo en el reclutamiento de nuevos miembros como fuente principal de bonificaciones y ascensos en la estructura del negocio; promesas de ganancias muy por encima del mercado, asegurando utilidades veloces y garantizadas; información reservada acerca de la actividad económica o la forma en la que el dinero brinda su rendimiento; ausencia de registros legales por parte de las autoridades y, muy frecuentemente, una especial presión para que la inversión sea lo más inmediata posible ya que la oportunidad es permanentemente efímera (Gayubas-Fernández, 2022; Parejo-Pizarro, 2017).

Pump and dump (inflar y tirar): es una estrategia fraudulenta que consiste en manipular artificialmente el precio de un activo financiero mediante la difusión de información engañosa o exagerada, con el objetivo de provocar una subida rápida del precio (*pump*). Una vez que el valor ha aumentado gracias al interés especulativo generado, los promotores del esquema venden sus activos a precios inflados (*dump*), obteniendo ganancias a expensas de los inversores incautos, quienes sufren pérdidas cuando el precio colapsa. Desde el punto de vista técnico, el *pump and dump* es una forma de manipulación de mercado y constituye una violación de las normativas de transparencia y equidad de los mercados financieros. El esquema se apoya en el volumen bajo y la volatilidad alta de ciertos activos que pueden ser fácilmente influenciados por campañas coordinadas de compra y promoción. Desde luego, la tecnología ha facilitado su proliferación, especialmente cuando se involucran redes sociales muy poco reguladas como Telegram, Discord o Reddit, coordinándose desde ahí unas campañas muy bien estructuradas para que el fraude sea creíble, desde la idea de “si muchos lo creen, es que debe ser cierto”, ignorando que la mayor parte de esas opiniones son el producto de *bots* o *spam* dedicado a manipular la percepción colectiva.

La alerta debe saltar cuando se identifican características altamente especulativas en un negocio, teniendo en cuenta elementos como el increminto súbito y no justificado en el precio de cotización de un activo poco conocido; promoción agresiva del activo en redes sociales, foros o canales sin respaldo institucional; presión para una inversión inmediata e irreflexiva, justificándose en un patrón de precios en forma de pico abrupto seguido de una caída inmediata, por lo que no se debe desaprovechar la oportunidad de aparente ganancia asegurada (Friedhelm & Hagemann, 2019).

Rug pulls (tirón de alfombra): es una forma de estafa financiera en el ecosistema de los criptoactivos y las finanzas descentralizadas, en la que los desarrolladores de un proyecto retiran repentinamente los fondos aportados por los inversores, abandonando el proyecto y dejando a los usuarios sin acceso a sus activos. Se trata de una modalidad de *exit scam* altamente sofisticada que aprovecha la falta de regulación y la complejidad técnica del entorno *blockchain*. Ocurre comúnmente en proyectos de tokens nuevos o plataformas pseudocripto, donde los desarrolladores crean un token, lo listan en un *exchange* descentralizado, y ofrecen altos rendimientos para atraer liquidez. Una vez que una cantidad significativa de fondos ha sido depositada por usuarios confiados, los desarrolladores retiran el fondo de liquidez, eliminan el sitio web, bloquean las redes sociales y desaparecen con los activos digitales. Este tipo de estafa suele combinarse con el *pump and dump*, haciendo que exista un halo de confianza acompañando el crecimiento del capital acumulado.

Si bien esta modalidad resulta obvia por sus características, es necesario que se identifiquen algunas señales de alerta fundamentales, las cuales incluyen la disponibilidad de realizar los tratos a través de *smart contracts* no supervisados, la operación por medio de equipos y asesores telemáticos, promesas de retornos más allá de los precios de mercado, ausencia de una obligatoriedad legal de reserva de liquidez (encaje financiero), falta de transparencia en la divulgación de la *tokenómica* (método de cálculo, resguardo y administración de los tokens) y, con especial ahínco, la falta posibilidad preferente de realizar las transferencias mediante plataformas pseudocriptológicas (Friedhelm & Hagemann, 2019).

Quioscos financieros: son entidades que ofrecen servicios de inversión sin estar autorizadas ni reguladas por las autoridades competentes. Estas organizaciones simulan ser intermediarios financieros legítimos, pero operan al margen del sistema legal, captando fondos de los inversores bajo falsas promesas de rentabilidad, sin ninguna garantía ni supervisión. A menudo, el objetivo final es apropiarse del capital invertido, en lugar de gestionarlo de manera legítima. Para obtener la confianza de las víctimas, suelen adoptar la apariencia de una entidad formal que dispone de páginas web bien diseñadas, documentación con terminología financiera sofisticada y personal que simula ser asesor certificado. Sin embargo, estas entidades no figuran en los registros oficiales de instituciones financieras autorizadas y carecen de los requisitos legales para operar en los mercados. Este tipo de fraude aprovecha el desconocimiento del público y se disfraza de oportunidad de inversión, especialmente en contextos de alta inflación, incertidumbre económica o búsqueda de rentabilidad rápida.

Algunas alertas a considerarse son referentes a las promesas de rentabilidades fijas, elevadas con respecto al mercado y garantizadas; presión para la inversión de forma inmediata so riesgo de perder la oportunidad favorable que da el mercado; ausencia de registro o licencia ante las autoridades nacionales, normalmente aduciendo que todo lo legal se gestiona en la casa matriz en un país lejano; contratos ambiguos; dificultades crecientes para realizar el retiro de fondos invertidos; así como la propensión a preferir el pago mediante plataformas pseudocritpológicas (Gayubas-Fernández, 2022).

Habiendo, pues, tantas señales de alerta para la detección oportuna y preventiva de las estafas financieras, resulta poco comprensible que éstas siempre encuentran víctimas para perpetrar delitos, por lo que vale la pena explorar las relaciones en la psique de las víctimas potenciales.

Situación de fraudes financieros en El Salvador

La Superintendencia del Sistema Financiero (SSF) de El Salvador reporta que se tienen identificadas diversas modalidades de estafas financieras que suponen una amenaza creciente para los usuarios, especialmente por vías digitales. En consonancia con la

tendencia global, destacan las promesas falsas de recuperación de dinero mediante cuentas que generan confianza y buscan atraer incautos; la oferta de inversiones ficticias que simulan ser financiadas por entidades serias mediante el uso de imágenes y sonido, a veces producto del uso de inteligencias artificiales, especialmente aprovechando la popularidad del Gobierno en algunos sectores de la población (Villeda, 2025); y la suplantación de instituciones bancarias mediante correos electrónicos o SMS que solicitan datos personales (Palma, 2025; Superintendencia del Sistema Financiero, 2025c).

También se documentan estafas vinculadas a falsos programas gubernamentales de inversión con promesas de elevadas ganancias a corto plazo, así como créditos sin garantía ni fiador ofrecidos por plataformas no registradas y que exigen pagos por adelantado (Villeda, 2025). Además, circulan estafas laborales que utilizan logos oficiales para ofrecer empleos desde casa con pago inmediato, al igual que sitios fraudulentos que simulan subsidios estatales y plataformas falsas de venta de equipaje o boletos aéreos que buscan sustraer tanto datos como dinero. Tal como puede observarse, la ingeniería social se constituye en la principal herramienta para cometer la estafa financiera en El Salvador (Superintendencia del Sistema Financiero, 2025b), muy probablemente por que explota la vulnerabilidad de la ciudadanía al identificar las múltiples carencias educativas al respecto de las finanzas y la seguridad cibernética (Fundación Salvadoreña para el Desarrollo, 2021; González-Portillo, 2021).

Pese a la relevancia del tema y a que el Gobierno Central ha dispuesto un canal de denuncias especializado (Superintendencia del Sistema Financiero, 2025a), la Fiscalía General de la República ha declarado que no cuenta con ningún tipo de estadística acerca de las denuncias, comisiones de delitos, fraudes e investigaciones sobre estafas financieras (Ávalos, 2025; Fiscalía General de la República de El Salvador, 2025), lo cual dificulta en gran medida tener un abordaje integral del problema en aras de la persecución del delito y prevención de riesgos entre la población, pese a la reforma de la Ley Especial Contra los Delitos Informáticos y Conexos, la cual incluyó un inciso para que quien use las tecnologías para insertar instrucciones fraudulentas que resulten en un provecho para sí o para un tercero será sancionado hasta con 10 años de prisión (Jordán, 2025).

Perfil de las víctimas de fraude financiero

La creciente sofisticación de los fraudes financieros plantea un desafío no solo en términos legales y económicos, sino también desde una perspectiva psicológica, por lo que comprender qué características personales y sociodemográficas hacen que ciertos individuos sean más propensos a caer en estos esquemas es esencial para el diseño de estrategias preventivas y políticas públicas eficaces.

Un factor relevante para el análisis es la edad de las víctimas, tomando en cuenta que la mayor incidencia de estafas radica sobre las personas mayores de 41 años en un porcentaje del 51 %, seguido de personas menores de 30 años las cuales componen un 38 % de la muestra europea para 2023 (Pérez Martínez & López Pérez, 2023). En el mismo año, pero en Estados Unidos, se registró un aumento del 14 % (6.6 billones de dólares) en las estafas perpetradas contra personas mayores de 40 años (Internet Crime Complaint Center, 2023b), siendo la principal vía de *phishing* mediante fingimiento de soporte técnico (Morgan & Tapp, 2024), valiéndose de la credulidad propia de la generación objetivo y sus características psicosociales (Ebner et al., 2023).

Aunado a eso, el nivel educativo de la víctima potencial es un factor interviniente. Si bien las personas con menor educación formal suelen ser más vulnerables a fraudes tradicionales, los individuos con niveles medios o altos de formación no están exentos de caer en esquemas sofisticados en razón del exceso de confianza derivado de la sensación de adecuada educación financiera, lo cual puede llevar a una sobreestimación de la capacidad personal para detectar fraudes (Céspedes-López, 2018; Herrera-Guzmán & Raccanello, 2014), especialmente en ámbitos financieros complejos, tomando como factor relevante el que la educación formal no siempre corresponde con una educación financiera adecuada (Angulo-Rangel et al., 2023; Lusardi & Mitchel, 2011). En tal sentido, una intervención educativa intencionada e institucionalizada tienen la capacidad de proveer a los individuos de herramientas de gestión de riesgos y prevención de fraudes (Burke et al., 2022), pudiéndose establecer una relación proporcional entre la propensión a ser víctima

de fraude financiero y la calidad de vida, expresada en función de la educación financiera a la que se ha tenido acceso (Rodríguez-Rodríguez et al., 2020).

Otro elemento a tomarse en cuenta es la situación económica de la víctima potencial, a sabiendas de que de que la vulnerabilidad financiera de las personas de cara a la insatisfacción de necesidades básicas o en el afrontar responsabilidad es adquiridas pueden condicionar su toma de decisiones, especialmente cuando existen promesas de altas rentabilidades sin invertir montos fuera de órbita (Anguita-López, 2022; Wang et al., 2021). En contra posición, aquellos que se encuentran en una condición económica estable pueden padecer frente a estafas mucho mejor elaboradas, que evoquen a una rentabilidad alta para un futuro planificado (Castagno et al., 2025; Ricci & Carateli, 2017), por lo que la estrategia cambia de acuerdo a la condición de la víctima potencial.

La evidencia apunta a que conocer a profundidad los pormenores estadísticos de la comisión de fraudes financieros permite que se diseñen estrategias de prevención más efectivas; sin embargo, es imposible establecer un perfil de la víctima para el caso específico de El Salvador, siendo que, como se ha dicho, la Fiscalía General de la República carece en su totalidad de datos que permitan hacer un análisis mínimo para la gestión del riesgo financiero en el campo de las estafas y fraudes (Ávalos, 2025; Fiscalía General de la República de El Salvador, 2025).

Pese a la carencia de data, resulta evidente que la población salvadoreña cumple con una cantidad importante de características que le colocan como posibles víctimas de fraudes financieros, verificándose un deficiente nivel educativo en el término tecnológico, financiero y de ciberseguridad (Fuentes-Monroy, 2019; González-Portillo, 2021; Ibáñez, 2020); y una situación económica apremiante que sirve de catalizador para que la población se convierta en víctima potencial en virtud de sus vulnerabilidades (Alemán, 2025).

La psicología de la víctima de fraude financiero

El engaño y la mentira han sido comportamientos presentes en la historia de los seres humanos por mucho tiempo, habiéndose utilizado regularmente como estrategias de enfrentamiento y supervivencia ante entornos hostiles. En la historia, fueron empleados

para obtener recompensas y evitar consecuencias negativas en diferentes situaciones como enfrentamientos violentos, acuerdos políticos, negociaciones comerciales, entre otras. Esto indica que dichos comportamientos han ido evolucionando con el tiempo, ajustándose a los cambios en la sociedad humana (Ashby, 2020; Burnes et al., 2017; Caneppele & Aebi, 2019a).

Tomando en cuenta lo anterior, realizar un estudio completo de las estafas debe ser interdisciplinario, desde la perspectiva de la jurisprudencia, la criminología y la psicología forense. Esta última se encarga del análisis de patrones comportamentales del ser humano en actos de índole legal, asesorando a profesionales del área jurídica con bases teóricas fuertemente aceptadas por la comunidad científica (Camacho-Espinosa, 2023).

De acuerdo a la teoría de los cincos grandes factores de la personalidad (Big Five), una de las principales características psicológicas de las víctimas de estafa es la baja estabilidad emocional (van de Weijer & Leukfeldt, 2017). Según la neurociencia, el ser humano es un ser emocional que tiene la capacidad de razonar; y, por su parte, a nivel neurofisiológico se dice que la actividad racional se lleva a cabo en el córtex, mientras que la actividad emocional se encuentra en el sistema límbico. La toma de decisiones es el resultado de la interacción entre estas dos regiones del cerebro, por lo que las emociones interfieren directamente (Padilla-Madera, 2024). Esto indica que, al no poseer una estabilidad emocional adecuada, las decisiones que se toman suelen ser impulsivas e inestables, teniendo como intervinientes externos las causales esgrimidas en apartados anteriores.

Además de lo anterior, en estudios anteriores (Caneppele & Aebi, 2019b; Chen et al., 2017; DeLiema et al., 2020; Jones et al., 2019; Mueller et al., 2020; Winsor & Mueller, 2020), se ha encontrado que otras de las características psicológicas que vuelven vulnerables a las víctimas de fraudes o estafas son las siguientes:

La impulsividad: se entiende como la tendencia a reaccionar de manera rápida y sin una reflexión previa, dando como resultado comportamientos agresivos o la incapacidad de accionar utilizando la atención sostenida (Haro et al., 2004; Pinal-Fernández & Pérez-Bravo, 2003).

El neuroticismo: se define como un rasgo de la personalidad que se caracteriza por una tendencia a experimentar diversos efectos negativos (emocionalidad negativa) de manera intensa y/o recurrente (Costa & McCrae, 2014; Goldberg et al., 2006). Este rasgo de la personalidad suele estar relacionado con la ansiedad y la depresión.

El bajo locus de control: define el locus de control como la capacidad del ser humano de analizar los acontecimientos relacionados a sí mismo y sus diferentes componentes, para identificar si dichos acontecimientos son resultado de factores propios o del entorno (Rotter, 1966). Un bajo locus de control implica entonces una deficiencia en este tipo de análisis.

La baja reflexión cognitiva: Hace referencia a la dificultad que existe en la inhibición de respuestas instintivas incorrectas y la búsqueda de una respuesta correcta a través de la profundización de la reflexión (Frederick, 2005).

También se habla de la búsqueda de nuevas sensaciones y de la falta de habilidad para el manejo de la presión del tiempo. La primera suele relacionarse con la etapa del adulto joven que busca experimentar cosas nuevas que le permitan salir de la casilla de niño o adolescente y entrar al mundo de la independencia, la estabilidad y la madurez. La segunda se refiere a la habilidad que se va adquiriendo con el tiempo y la experiencia de la gestión del tiempo. Esta no necesariamente se relaciona con una etapa del desarrollo en específico, ya que depende de las vivencias de cada ser humano.

Para el caso de El Salvador, el tema de la salud mental es a penas incipiente en la agenda nacional, habiéndose establecido algunas políticas públicas que buscan dar atención a la población desde el enfoque de la profilaxis (Molina-Aguilar, 2021). Sin embargo, la Encuesta Nacional de Salud Mental 2022 reveló que la población adulta (entre los 18 y los 59 años, siendo la más propensa a ser estafada por su capacidad adquisitiva) se encuentra en una condición de vulnerabilidad, registrándose que el 10.3 % tiene síntomas de estrés postraumático; el 19.3 % presenta trastornos de ansiedad; y que el 21 % presenta algún grado de depresión; desembocando un preocupante 2.3 % de personas que presentan riesgo moderado-alto de ideación suicida (Armero-Guardado & Domínguez, 2023). En tal sentido, el manejo emocional de la población salvadoreña es claramente un

factor de riesgo en cuanto a su vulnerabilidad multidimensional, exponiéndole directamente a los factores ya expuestos como agravantes ante las estafas financieras.

CONCLUSIONES

La evolución de los fraudes financieros revela una constante adaptación a los avances tecnológicos y a los contextos socioeconómicos de las víctimas potenciales, teniendo por característica un incremento en la sofisticación de los esquemas y una mayor capacidad para valerse de la manipulación emocional como herramienta de control. Esta evolución ha trascendido las simples cuestiones técnicas, insertándose en la comprensión cognitiva y emocional de las víctimas, cuyo perfil psicológico y sociodemográfico influye significativamente en su vulnerabilidad. Ciertos atributos, como baja estabilidad emocional, exceso de confianza derivado de una sobreestimación de la educación financiera, y condiciones socioeconómicas precarias, crean un sustrato en el que los mecanismos de confianza, ilusión y necesidad de validación pueden ser explotados por los estafadores.

Desde una perspectiva psicológica, la vulnerabilidad no es meramente el resultado de la ignorancia o falta de información, sino que se alimenta de procesos cognitivos como la heurística de disponibilidad, la tendencia al optimismo irracional y la propensión al efecto de confirmación; además, las emociones producto de la avaricia y la ansiedad por resolver problemas económicos urgentes, refuerzan decisiones irracionales. En tal sentido, la existencia de sesgos cognitivos, combinada con la percepción distorsionada del riesgo, facilita que las víctimas acepten propuestas que, bajo un análisis racional, serían claramente riesgosas o engañosas. De esta forma, la psicología de la estafa se configura como un entramado complejo donde el conocimiento emocional y cognitivo del potencial víctima interactúa con las técnicas manipulativas del estafador, generándose un ciclo donde la víctima se vuelve más susceptible a nuevas formas de engaño.

El entendimiento profundo de estas relaciones permite fundamentar medidas de gestión de riesgo personal, que van mucho más allá de la mera educación financiera técnica. Es imperativo desarrollar intervenciones que aborden directamente los sesgos cognitivos y las emociones implicadas en la toma de decisiones económicas, promoviendo capacidades

metacognitivas que faciliten la identificación de señales de alerta y la adopción de conductas precautorias. La incorporación de enfoques psicológicos en programas preventivos tales como entrenamiento en gestión emocional, reconocimiento de sesgos y deliberación racional, puede reducir significativamente la vulnerabilidad individual frente a probables fraudes financieros. Además, la generación de conciencia sobre la propia psicología en relación con la toma de decisiones financieras ayuda a evitar caer en trampas que, explotando la confianza o el miedo, aumentan la probabilidad de victimización.

En conclusión, la integración de un análisis analítico del desarrollo de los fraudes, perfil psicológico y mecanismos de decisión no solo permite entender las causas subyacentes de la vulnerabilidad, sino que también fundamenta estrategias de prevención individualizadas y contextualizadas, las cuales idealmente deberían incorporarse en las políticas públicas de educación. Este enfoque multidisciplinario resulta en una gestión del riesgo proactiva, que fortalece la capacidad del individuo para detectar y combatir tácticas de manipulación, generando una resistencia cognitiva y emocional frente a las técnicas cada vez más elaboradas de los estafadores.

REFERENCIAS

Aguilar-Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de Estudios En Seguridad Internacional*, *6*(2), 17–43. https://doi.org/10.18847/1.12.2

Alemán, U. (2025, August 5). CEPAL reduce por segunda vez la proyección de crecimiento de El Salvador, a 2.4 % en 2025. *Diario El Mundo*. https://diario.elmundo.sv/economia/cepal-reduce-por-segunda-vez-la-proyeccion-de-crecimiento-de-el-salvador-a-2-4-en-2025

Allende, M. (2024, April 3). Financial Inclusion in Latin America Grew by 30 Percentage Points. *Mexico Business News*. https://mexicobusiness.news/finance/news/financial-inclusion-latin-america-grew-30-percentage-points

Amro, B. (2018). Phishing Techniques in Mobile Devices. *Journal of Computer and*

Communications, *06*(02), 27–35. https://doi.org/10.4236/jcc.2018.62003

Anguita-López, D. (2022). *Euforia colectia y burbujas especulativas* [Universidad de Valladolid]. https://uvadoc.uva.es/bitstream/handle/10324/54407/TFG-N.1791.pdf?sequence=1&isAllowed=y

Angulo-Rangel, F., Rodríguez-Márquez, R. L., & Figueroa-Royero, L. (2023). Auditoría forense: detención del fraude financiero en organizaciones Latinoamericanas. *Misión Jurídica*, *16*(25), 277–289. https://doi.org/10.25058/1794600X.2264

Armero-Guardado, J., & Domínguez, R. L. (2023). *Encuesta Nacional de Salud Mental 2022*. https://tinyurl.com/24hzk6w6

Ashby, M. P. J. (2020). Initial evidence on the relationship between the coronavirus pandemic and crime in the United States. *Crime Science*, *9*(1), 6. https://doi.org/10.1186/s40163-020-00117-6

Ávalos, J. (2025, August 8). Fiscalía sin estadísticas sobre estafas digitales, pese al auge de casos. *El Diario de Hoy*. https://www.elsalvador.com/noticias/nacional/fiscalia-sin-estadisticas-sobre-estafas-digitales/1235240/2025/

Bermúdez Pacheco, D., Guarín Avella, N., & Rojas Camargo, S. (2021). *Avances e impacto generado tras la circulación de las criptomonedas en la negociación de los mercados financieros* [Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/bitstream/20.500.12494/36440/3/2021_avances_impacto_generado.pdf

Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? *Journal of Economic Behavior & Organization*, *198*, 250–266. https://doi.org/10.1016/j.jebo.2022.03.028

Burnes, D., Henderson, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of Financial Fraud and Scams Among Older Adults in the United States: A Systematic Review and Meta-Analysis. *American Journal of Public Health*, *107*(8), e13–e21. https://doi.org/10.2105/AJPH.2017.303821

Camacho-Espinosa, G. (2023). Criminología forense: concepto y aplicaciones en el sistema de justicia penal. *Archivos de Criminología, Seguridad Privada y Criminalística*,

10(20), 82–91. https://bit.ly/3f8OliL

Caneppele, S., & Aebi, M. F. (2019a). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66–79. https://doi.org/10.1093/police/pax055

Caneppele, S., & Aebi, M. F. (2019b). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66–79. https://doi.org/10.1093/police/pax055

Casanova-Villalba, C. I., & Casanova-Villalba, L. A. (2024). Uso de análisis de datos avanzados para la detección de fraudes financieros. *Revista Científica Ciencia y Método*, *2*(3), 1–12. https://doi.org/10.55813/gaea/rcym/v2/n3/44

Castagno, E., Caretta, A., Giacomel, E., & Rossi, M. (2025). The importance of pension and financial knowledge for pension plan participation in Italy. *Journal of Pension Economics and Finance*, 1–31. https://doi.org/10.1017/S1474747224000143

Castillo-Tapuy, A. Y., & Montenegro-Ramírez, A. F. (2022). Evolución del uso de plataformas digitales para la adquisición de bienes y servicios Postcovid19. *593 Digital Publisher CEIT*, *7*(4–1), 567–578. https://doi.org/10.33386/593dp.2022.4-1.1280

Castro-Badillo, F., Londoño-Avellaneda, D., & Medina-Cifuentes, F. (2022). Transacciones en línea y bienestar financiero. *Coyuntura Económica*, *2*, 127–151. https://www.repository.fedesarrollo.org.co/bitstream/handle/11445/4354/Co_Eco_Diciembre_2022_Castro_Londoño_y_Medina.pdf?sequence=1&isAllowed=y

Céspedes-López, J. B. (2018). Análisis de la necesidad de la educación financiera en la formación colegial. *Pensamiento Crítico*, *22*(2), 97. https://doi.org/10.15381/pc.v22i2.14333

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Costa, P., & McCrae, R. (2014). *The Oxford Handbook of the Five Factor Model* (2nd ed.). Routledge.

Cox, L. A., Babayev, D., & Huber, W. (2005). Some Limitations of Qualitative Risk Rating Systems. *Risk Analysis*, *25*(3), 651–662. https://doi.org/10.1111/j.1539-6924.2005.00615.x

De La Torre Lascano, C. M., & Quiroz Peña, J. I. (2023). Ciberdelito 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/10.52080/rvgluz.28.102.11

DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2020). Financial Fraud Among Older Americans: Evidence and Implications. *The Journals of Gerontology: Series B*, *75*(4), 861–868. https://doi.org/10.1093/geronb/gby151

Ebner, N., Pehlivanoglu, D., & Shoenfelt, A. (2023). Financial Fraud and Deception in Aging. *Advances in Geriatric Medicine and Research*, *5*(3). https://doi.org/10.20900/agmr20230007

Fiscalía General de la República de El Salvador. (2025). *Informe de Labores 2024 – 2025*. https://www.fiscalia.gob.sv/informe-de-labores-2024-2025/

Flores-Álava, S., & Mena-Hernández, L. (2023). Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras. *593 Digital Publisher CEIT*, *8*(4), 159–173. https://doi.org/10.33386/593dp.2023.4.1652

Frederick, S. (2005). Cognitive Reflection and Decision Making. *Journal of Economic Perspectives*, *19*(4), 25–42. https://doi.org/10.1257/089533005775196732

Friedhelm, V., & Hagemann, T. (2019). Cryptocurrency Pump and Dump Schemes: Quantification and Detection. *2019 International Conference on Data Mining Workshops (ICDMW)*, 244–251. https://doi.org/10.1109/ICDMW.2019.00045

Fuentes-Monroy, C. (2019). *La educación financiera en los programas educativos de El Salvador* [Universidad de El Salvador]. https://repositorio.ues.edu.sv/items/bc560066-2e76-474c-bc3b-9c3ae8ab67e9

Fundación Salvadoreña para el Desarrollo. (2021). Cerrar la brecha digital en educación:

¿qué debemos mirar más allá de la entrega de computadoras? *Nota de Política Pública*, *11*, 1–7. https://tinyurl.com/28ejmfqv

Gayubas-Fernández, L. (2022). *Las estafas financieras piramidales* [Universidad de Valladolid]. https://doi.org/10.19230/jonnpr.1237

Goldberg, L. R., Johnson, J. A., Eber, H. W., Hogan, R., Ashton, M. C., Cloninger, C. R., & Gough, H. G. (2006). The international personality item pool and the future of public-domain personality measures. *Journal of Research in Personality*, *40*(1), 84–96. https://doi.org/10.1016/j.jrp.2005.08.007

González-Portillo, A. D. (2021). *La ciberseguridad: una visión nacional y regional frente a las ciberamenazas en el siglo XXI* [Universidad de El Salvador]. https://tinyurl.com/23tz27ue

Haro, G., Castellanos, M., Pérez-Gálvez, B., Rodríguez, E., Cervera, G., & Valderrama, J. C. (2004). Revisión histórica de la impulsividad desde una perspectiva artística, filosófica y psicopatológica. *Salud Mental*, *27*(5), 23–28. https://tinyurl.com/29manmxh

Herrera-Deyta, M. (2025). *Esquema Ponzi y piramidales: un enfoque de psicopatía* [Universidad Autónoma del Estado de Hidalgo]. https://tinyurl.com/23thvyx6

Herrera-Guzmán, E., & Raccanello, K. (2014). Educación e inclusión financiera. *Revista Latinoamericana de Estudios Educativos*, *64*(2), 119–141. https://tinyurl.com/27wakt8g

Ibáñez, M. (2020). *La Educación financiera en El Salvador*. https://www.iefweb.org/ca/la-educacion-financiera-en-el-salvador/

Internet Crime Complaint Center. (2023a). *Elder Fraud Report*.

Internet Crime Complaint Center. (2023b). *Elder Fraud Report*. https://tinyurl.com/2yxol8wh

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLOS ONE*, *14*(1), e0209684. https://doi.org/10.1371/journal.pone.0209684

Jordán, L. (2025, July 4). Reforma a ley de delitos informáticos entró en vigencia. *La Prensa*

Gráfica. https://www.laprensagrafica.com/elsalvador/Reforma-a-ley-de-delitos-informaticos-entro-en-vigencia-20250704-0096.html

Kemp, S., & Moneva, A. (2020). Fraude online vs. offline: factores predictores de victimización y su impacto. *InDret*, *1*, 424–444. https://dugi-doc.udg.edu/bitstream/handle/10256/17693/FraudeOnline.pdf?sequence=1

López-Pincay, P. R., Mendoza-Lino, K. M., Yagual-Tomalá, E. M., & Blum-Alcívar, H. M. (2024). Mecanismos de control para evitar el aumento del cibercrimen financiero. *MQRInvestigar*, *8*(3), 1802–1818. https://doi.org/10.56048/MQR20225.8.3.2024.1802-1818

Lusardi, A., & Mitchel, O. (2011). Financial literacy around the world: an overview. *Journal of Pension Economics and Finance*, *10*(4), 497–508. https://doi.org/10.1017/S1474747211000448

Maldonado-Guñido, C., Sánchez-Puga, A., Ramírez-Flores, D., & Hallo-Silva, K. (2024). El delito de fraude financiero en el Ecuador: un análisis de las transacciones digitales. *Dilemas Contemporáneos: Educación, Política y Valores*, *12*(87), 1–19. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/download/4491/4323/

Manoharan, A., & Sarker, M. (2024). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/IRJMETS32644

Mena Roa, M. (2021). Los pagos de rescate con criptomonedas por ataques ransomware se dispararon en 2020. *Statista*. https://es.statista.com/grafico/25240/valor-total-de-las-criptomonedas-recibidas-por-direcciones-de-ransomware–en-mill-de-dolares-%252A/

Molina-Aguilar, J. (2021). La salud mental en El Salvador: los costos invisibles de un problema olvidado. Un abordaje desde las Ciencias Sociales. *Análisis Socioeconómico de El Salvador*. https://tinyurl.com/245kgybe

Moncada-Vargas, A. (2020). Comparación de técnicas de machine learning para detección

de sitios web de phishing. *Interfases*, 77–103. https://doi.org/10.26439/interfases2020.n013.4886

Morgan, R., & Tapp, S. (2024). Análisis del fraude financiero contra adultos mayores. *National Institute of Justice*. https://nij.ojp.gov/topics/articles/examining-financial-fraud-against-older-adults

Mueller, E. A., Wood, S. A., Hanoch, Y., Huang, Y., & Reed, C. L. (2020). Older and wiser: age differences in susceptibility to investment fraud: the protective role of emotional intelligence. *Journal of Elder Abuse & Neglect*, *32*(2), 152–172. https://doi.org/10.1080/08946566.2020.1736704

Orellana-Osorio, I., Reyes, M. A., & Cevallos-Rodríguez, E. (2019). Evolución de los modelos para la medición del riesgo financiero. *UDA AKADEM*, *3*, 7–34. https://doi.org/10.33324/udaakadem.v1i3.201

Padilla-Madera, B. (2024). *Toma de decisiones: cuando la emoción supera la razón* (K. Sandoval-Balcazar (ed.)). Colegio Nacional de Educación Profesional Técnica. https://tinyurl.com/22h6ulvs

Palma, M. (2025, July 22). ¡Cuidado! Estas son las 8 estafas más comunes que circulan en El Salvador. *El Diario de Hoy*. https://www.laprensagrafica.com/Cuidado-Estas-son-las-8-estafas-mas-comunes-que-circulan-en-El-Salvador-t202507220001.html

Parejo-Pizarro, I. (2017). La estafa piramidal: Un estudio exploratorio de la víctima. *Journal of Negative and No Positive Results*, *2*(2), 62–68. https://doi.org/10.19230/jonnpr.1237

Pérez Martínez, A., & López Pérez, R. (2023). Análisis del delito de estafa desde la psicología forense: una propuesta interdisciplinaria. *Behavior & Law Journal*. https://doi.org/10.47442/blj.2023.95

Pinal-Fernández, B., & Pérez-Bravo, A. (2003). Impulsividad: revisión histórica y conceptual. *Actas Españols de Psiquiatría*, *1*(4), 220–230. https://actaspsiquiatria.es/index.php/actas/article/download/1116/1807/1838

Ricci, O., & Carateli, M. (2017). Financial literacy, trust and retirement planning. *Journal of Pension Economics and Finance*, *16*(1), 43–64.

https://doi.org/10.1017/S1474747215000177

Rivera-Díaz, N. E. (2022). Grado de riesgo en el uso de criptoactivos para usuarios sin un nivel de educación especializado en el ramo: aspectos a priorizar en la mitigación. *Revista Minerva*, *5*(4), 5–22. https://minerva.sic.ues.edu.sv/index.php/Minerva/article/view/197/195

Rodríguez-Martínez, H. (2024, December 19). Suben 26,1% los intentos de fraude electrónico durante el fin de año. *Portafolio*. https://www.portafolio.co/economia/finanzas/suben-26-1-los-intentos-de-fraude-electronico-durante-el-fin-de-ano-620033

Rodríguez-Rodríguez, V., Pérez-Garín, D., Recio-Saboya, P., & Rico-Gómez, A. (2020). Fraudes financieros, salud y calidad de vida: un estudio cualitativo. *Gaceta Sanitaria*, *34*(3), 268–275. https://doi.org/10.1016/j.gaceta.2019.11.006

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, *80*(1), 1–28. https://doi.org/10.1037/h0092976

Secretaría General de INTERPOL. (2020). *Ciberdelincuencia: efectos de la COVID-19*. https://www.interpol.int/es/content/download/15526/file/COVID-19 Cybercrime Analysis Report-Design_02_SP.pdf

Superintendencia del Sistema Financiero. (2025a). *¿A dónde puedes interponer tu denuncia?* SSF. https://ssf.gob.sv/preguntas-frecuentes/a-donde-puedes-interponer-tu-denuncia/

Superintendencia del Sistema Financiero. (2025b). *¿Cómo operan los ciberdelincuentes?* SSF. https://ssf.gob.sv/estafas/identifica-una-estafa/

Superintendencia del Sistema Financiero. (2025c). *Modalidades de fraude*. SSF. https://ssf.gob.sv/estafas/modalidades-de-fraudes/

van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Villeda, J. (2025, June 26). MINEC denuncia suplantación de identidad de ministra de

Economía para estafa de programas de inversión. *Diario El Mundo*. https://diario.elmundo.sv/economia/minec-denuncia-suplantacion-de-identidad-de-ministra-de-economia-para-estafa-de-programas-de-inversion

Wang, W., Lan, Y., & Wang, X. (2021). Impact of livelihood capital endowment on poverty alleviation of households under rural land consolidation. *Land Use Policy*, *109*, 105608. https://doi.org/10.1016/j.landusepol.2021.105608

Winsor, D. L., & Mueller, C. E. (2020). Depression, suicide, and the gifted student: A primer for the school psychologist. *Psychology in the Schools*, *57*(10), 1627–1639. https://doi.org/10.1002/pits.22416