NEXUS
Revista Científica

ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

MÁS ALLÁ DE LA TECNOLOGÍA: FACTORES PSICOLÓGICOS Y ALFABETIZACIÓN DIGITAL ASOCIADOS A LA VULNERABILIDAD FRENTE A LAS ESTAFAS DIGITALES

BEYOND TECHNOLOGY: PSYCHOLOGICAL FACTORS AND DIGITAL LITERACY ASSOCIATED WITH VULNERABILITY TO DIGITAL SCAMS

Autores: [1] Stalin Patricio Songor Illescas, [2] Patricio Sebastián Rosas Villagómez y [3] Mark Anderson Uriarte Guzmán

[1]ORCID ID: https://orcid.org/0009-0005-7059-0178
[2]ORCID ID: https://orcid.org/0009-0001-5973-1401
[3]ORCID ID: https://orcid.org/0009-0005-1723-1248
[1]E-mail de contacto: ssongor4000@upse.edu.ec
[2]E-mail de contacto: prosas7845@upse.edu.ec
[3]E-mail de contacto: marck.uriarte@ueb.edu.ec
Afiliación: [1*2*] Universidad Estatal Península de Santa Elena (Ecuador) [3*] Universidad Estatal de Bolívar (Ecuador)
Artículo recibido: 14 de septiembre del 2026
Artículo revisado: 16 de octubre del 2026
Artículo aprobado: 19 de noviembre del 2026
[1] Psicólogo clínico, adquirido de la Universidad Católica de Cuenca (Ecuador). Máster Universitario en Dirección e Intervención Sociosanitaria, adquirido de la Universidad Internacional de la Rioja (España).
[2] Psicólogo clínico, adquirido de la Universidad Politécnica Salesiana (Ecuador). Magíster en Política Comparada, adquirido de la Facultad Latinoamericana de Ciencias Sociales (Ecuador).
[3] Licenciado en Psicología, adquirido de Pontificia Universidad Católica del Ecuador (Ecuador). Magíster en Psicología clínica, mención en Psicoterapia, obtenido en la Universidad Particular de Especialidades Espíritu Santo (Ecuador).

Resumen

Las estafas digitales están convirtiéndose cada vez más en un problema relevante en el mundo actual debido al aumento de las plataformas para el uso de la tecnología y la implementación de nuevas tácticas que emplean los ciberdelincuentes para engañar. La investigación tiene como objetivo identificar los elementos psicológicos y la alfabetización digital que determinan la susceptibilidad de las personas a las estafas digitales. La investigación se llevará a cabo de acuerdo con una metodología cualitativa de naturaleza bibliográfica y documental y con una perspectiva descriptiva, la cual supone el proceso de búsqueda, selección, análisis y revisión de fuentes científicas entre los años 2021 y 2026. Se considerarán cinco aspectos relacionados con el problema: estafas digitales e ingeniería social, aspectos psicológicos, emociones y sesgos cognitivos, alfabetización digital y prevención. A partir de los antecedentes científicos se comprende que la vulnerabilidad no es solamente un aspecto relacionado con la tecnología, sino que también está vinculada al conocimiento, al comportamiento y al proceso de toma de decisiones de los usuarios. Además, se comprende la importancia del pensamiento crítico y la alfabetización digital como herramientas para la identificación de amenazas y la verificación de la información. En resumen, para prevenir el cibercrimen es necesario combinar los enfoques tecnológicos y psicológicos.

Palabras clave: Estafas digitales, Factores psicológicos, Alfabetización digital, Ingeniería social, Vulnerabilidad.

Abstract

Digital scams are increasingly becoming a relevant problem in today's world due to the

NEXUS
Revista Científica
ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

growth of technology-based platforms and the implementation of new tactics used by cybercriminals to deceive individuals. This research aims to identify the psychological factors and digital literacy elements that determine people's susceptibility to digital scams. The study will follow a qualitative, bibliographic, and documentary methodology with a descriptive approach, involving the search, selection, analysis, and review of scientific sources published between 2021 and 2026. Five aspects related to the problem will be considered: digital scams and social engineering, psychological factors, emotions and cognitive biases, digital literacy, and prevention. Based on previous scientific research, vulnerability is understood not only as a technology-related issue but also as something linked to users' knowledge, behavior, and decision-making processes. Moreover, the significance of critical thinking and digital literacy as means to detect threats and verify information is noted. In conclusion, stopping cybercrimes needs a combination of technological and psychological methods.

Keywords: Digital scams, Psychological factors, Digital literacy, Social engineering, Vulnerability.

Sumário

Os golpes digitais estão se tornando cada vez mais um problema relevante no mundo atual devido ao aumento das plataformas tecnológicas e à implementação de novas táticas utilizadas pelos cibercriminosos para enganar as pessoas. A pesquisa tem como objetivo identificar os fatores psicológicos e os elementos da alfabetização digital que determinam a suscetibilidade das pessoas aos golpes digitais. O estudo será desenvolvido por meio de uma metodologia qualitativa, bibliográfica e documental, com abordagem descritiva, envolvendo a busca, seleção, análise e revisão de fontes científicas publicadas entre 2021 e 2026. Serão considerados cinco aspectos relacionados ao problema: golpes digitais e engenharia social, fatores psicológicos, emoções e vieses cognitivos, alfabetização digital e prevenção. Com base nos estudos científicos anteriores, compreende-se que a vulnerabilidade não está relacionada apenas à tecnologia, mas também ao conhecimento, ao comportamento e ao processo de tomada de decisões dos usuários. Além disso a necessidade do pensamento crítico e da alfabetização digital para ajudarem a reconhecer ameaças e verificar informações é apreciada. No geral a prevenção do crime cibernético requer um misto de intervenções tanto técnicas quanto psicológicas.

Palavras-chave: Golpes digitais, Fatores psicológicos, Alfabetização digital, Engenharia social, Vulnerabilidade.

Introducción

El aumento del uso de Internet y de los dispositivos digitales ha ayudado a lograr la comunicación, la información y la realización de las actividades diarias, pero también se ha convertido en un terreno fértil para los ciberdelitos los cuales incluyen el fraude digital y los estafas y que emplean técnicas como el phishing, el robo de identidad y la manipulación de las personas para obtener sus datos personales y financieros.

En este sentido el ingenio social se convierte en uno de los riesgos ya que manipula la confianza y las reacciones de los usuarios para engañarlos

ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

(Garzón Ibarra et al., 2024). Ser susceptible a estas amenazas no es solo un problema de la conciencia técnica, sino que también depende de otros factores como el miedo, la urgencia, la confianza excesiva y la impulsividad.

Estos aspectos pueden afectar la percepción que tenga un usuario y la forma en que actúe ante un mensaje sospechoso en relación a cualquier estafa (Desolda et al., 2021). Además, la alfabetización digital juega un papel importante porque permite la adquisición de las habilidades necesarias para la identificación de riesgos, la evaluación de la información y el uso seguro de los medios digitales (Hernández-Marín et al., 2024).

Las estafas digitales se han ido desarrollando con la ayuda de mensajes, correos electrónicos, llamadas telefónicas y sitios web de redes sociales. Pueden ser bastante difíciles de detectar particularmente cuando los delincuentes emplean datos personales o situaciones cotidianas comunes para ganar la confianza de sus posibles víctimas.

Por lo tanto, el peligro no sólo se limita a la funcionalidad de los dispositivos tecnológicos, sino que también depende de la capacidad de las personas para detectar comportamientos engañosos (Candanedo Yau, 2025).
Los aspectos psicológicos que pueden jugar un papel en este tipo de escenarios incluyen la presión del tiempo, el miedo a perderse una oportunidad, la curiosidad y las respuestas rápidas a algunos mensajes en particular.

El ritmo de las acciones de las personas puede resultar en la toma de decisiones impulsivas sin evaluar adecuadamente la información recibida. De esta manera, el análisis del comportamiento de los usuarios permite explicar cómo ciertas personas se convierten en víctimas de las tácticas de manipulación empleadas en los fraudes cibernéticos (Baki & Verma, 2023). Sin embargo, la alfabetización digital va más allá del uso de herramientas tecnológicas y espacios virtuales.

Es la capacidad de investigar, analizar y juzgar la información, identificar información falsa y proteger la información personal. La adquisición de estas competencias permite al individuo tomar una postura más crítica ante la información recibida y no difundirlos sin antes verificar su confiabilidad (López-González et al., 2023).

Así la educación y la capacitación digital se han convertido en recursos claves en el proceso de prevención. La verificación de enlaces, la identificación de remitentes sospechosos, la verificación de la información y la implementación de medidas de seguridad pueden disminuir los peligros que plantean los estafas.

Por otro lado, el pensamiento crítico permite poner a prueba la veracidad de la información antes de actuar sobre ella y compartirla, especialmente en aquellas plataformas donde la información puede ser falsa o alterada (Aceituno Silva, 2024).

En este contexto, el presente artículo analiza, mediante una revisión bibliográfica de trabajos académicos recientes, los factores psicológicos y de alfabetización digital involucrados en la susceptibilidad a las estafas digitales.

Las estafas digitales y la ingeniería social como mecanismos de manipulación

NEXUS
Revista Científica
ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

Los fraudes digitales se refieren a diferentes formas de conducta delictiva creada a través de medios como dispositivos, plataformas y otros servicios asociados a Internet. La razón de este tipo de fraude es defraudar a la víctima para obtener ganancias financieras o para obtener acceso a su información privada o a sus cuentas en plataformas digitales.

Los fraudes digitales incluyen el phishing, el robo de identidad, mensajes falsos, promociones fraudulentas y fraudes en el comercio electrónico. Una característica distintiva de los fraudes digitales es que no siempre implican el hackeo de los sistemas informáticos de la víctima ya que pueden explotar a las víctimas a través de la confianza y la falta de conocimiento.

El Ingeniería Social es una forma de técnicas de manipulación en las cuales una persona utiliza los medios de mensajes, identidades falsas y situaciones para manipular a otra persona para que realice acciones.

En relación a Ecuador Campos Gallegos y otros (2025) también hablan sobre la detección de ataques de ingeniería social, fraude y estafas lo cual permite asociarlo con el requisito del reconocimiento de las tácticas de engaño en el mundo cibernético.

Garzón Ibarra y otros (2024) en su estudio sobre ataques de ingeniería social en Ecuador hablaron sobre cómo los atacantes manipulan a las personas y los efectos que esto puede traer a diferentes áreas de la sociedad. Es crucial destacar la importancia de implementar medidas preventivas contra estos riesgos.

Por su parte Pazmiño-Quiñonez et al. (2024) realizaron un análisis sobre la eficiencia del phishing automatizado demostrando el efecto que el uso de procedimientos automatizados tiene sobre este tipo de ataques. Este precedente ayuda a comprender que los mecanismos engañosos siguen evolucionando con la tecnología haciéndolos complicados de detectar.

Según su investigación documental descriptiva la Inteligencia Artificial Generativa permite automatizar y personalizar el engaño haciendo que los mensajes fraudulentos sean más creíbles.

En ese sentido es necesario decir que el fraude digital puede verse como un fenómeno que combina los medios tecnológicos y las manipulaciones interpersonales. La eficiencia de esos métodos depende entre otras cosas de la capacidad de los delincuentes para crear un ambiente que fomente la confianza.

Factores psicológicos asociados a la vulnerabilidad frente a las estafas digitales

Uno de los aspectos más cruciales relacionados con los problemas psicológicos es que los factores psicológicos son el aspecto clave para comprender las razones por las cuales algunas personas reaccionan positivamente ante cualquier esfuerzo manipulador.

Las elecciones digitales no son necesariamente racionales ya que pueden verse afectadas por las emociones, la experiencia, las expectativas y los mecanismos de procesamiento de la información.

Los aspectos psicológicos que vale la pena considerar incluyen tales características como la

ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

impulsividad, la sobreconfianza, la percepción del riesgo, la búsqueda de beneficios instantáneos y las dificultades de la evaluación situacional. Estas cualidades pueden afectar cómo una persona percibe el mensaje y evalúa la legitimidad del mensaje.

En la revisión sistemática de Desolda et al. (2021) sobre la literatura científica de los factores humanos de los ataques de phishing se revelan diversos aspectos que contribuyen a la susceptibilidad del usuario.

Este estudio permite identificar que el conocimiento y la conciencia del riesgo, junto con el comportamiento individual, son aspectos importantes a tener en cuenta cuando se intenta comprender la efectividad de estos ataques.

De manera similar en el análisis de Baki y Verma (2023) sobre los estudios de la susceptibilidad del usuario al phishing los cuales fueron realizados durante un periodo de dieciséis años se discutieron las características de los participantes, así como los métodos para evaluar las reacciones e intervenciones.

La vulnerabilidad al fraude en línea se determina por numerosos factores psicológicos y de comportamiento incluyendo la impulsividad, demasiada confianza, la percepción del riesgo y el procesamiento de la información recibida.

Esta es la forma en la que se evidencia la importancia de incluir las características psicológicas en el proceso de prevención del fraude. En este sentido, los factores psicológicos no pueden verse como los rasgos que predestinan a alguien a convertirse en una víctima. Son simplemente las condiciones que pueden afectar la evaluación de la información y la percepción de la amenaza en la situación engañosa.

Emociones, confianza y sesgos cognitivos en la toma de decisiones digitales

Las emociones afectan la manera en la que los receptores procesan y reaccionan ante situaciones particulares. En cuanto al fraude digital los delincuentes emplean recursos de comunicación que buscan generar miedo, preocupación, emoción, curiosidad o un sentimiento de urgencia en sus víctimas.

Esto hace que el tiempo que se toma para verificar los detalles sea más corto y lleva a la toma de decisiones espontáneas. Una de las técnicas que se emplean es el uso de mensajes que alerten a los receptores de bloqueos de cuentas, transacciones bancarias desconocidas para ellos o problemas de servicios personales.

Estos mensajes buscan generar preocupación en los receptores antes de que verifiquen su autenticidad. Según Chaguaro Escobar (2026) tomar decisiones apresuradas y utilizar información inexacta están asociados a la vulnerabilidad de los adultos ecuatorianos a las estafas cibernéticas.

Mensajes que contienen logotipos, marcas, nombres institucionales o frases comunes pueden ser tomados como auténticos. Esto puede llevar al usuario a no verificar la autenticidad de los mensajes y a considerar el contenido como información fáctica a pesar de que sea engañosa.

El estudio realizado por Candanedo Yau (2025) ha estudiado el phishing y el spam en el contexto de la seguridad de los datos personales

NEXUS
Revista Científica
ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

como posibles peligros. Candanedo Yau ha puesto al descubierto las debilidades en la conciencia de los usuarios para detectar y manejar los mensajes fraudulentos, lo que significa que no existe una correlación entre la conciencia del peligro y tener las habilidades necesarias para prevenir el fraude.

Por lo tanto, para prevenir este tipo de fraudes es necesario desarrollar el hábito de reflexionar sobre las acciones antes de responder al mensaje o realizar cualquier otra acción.

Tabla 1

Factores psicológicos asociados a la vulnerabilidad frente a las estafas digitales

Factor psicológico	Característica	Posible consecuencia
Impulsividad	Actuar sin analizar suficientemente la información.	Acceder a enlaces fraudulentos.
Confianza excesiva	Aceptar comunicaciones sin comprobar su autenticidad.	Compartir información personal.
Temor	Reaccionar ante advertencias o amenazas.	Realizar acciones precipitadas.
Búsqueda de beneficios	Interesarse por recompensas u ofertas atractivas.	Caer en promociones engañosas.
Presión emocional	Experimentar dificultades para evaluar situaciones bajo tensión.	Disminuir la verificación de información.

Nota. Elaboración propia a partir de la síntesis de los aportes de Desolda et al. (2021), Baki y Verma (2023) y Chaguaro Escobar (2026). Los factores se presentan como categorías de análisis y no como una clasificación estadística de los usuarios.

Alfabetización digital y pensamiento crítico como mecanismos de prevención

Es imperativo que una persona tenga la alfabetización digital como un requisito previo para moverse con seguridad en los espacios tecnológicos. Esto no solo se limita al uso de dispositivos tecnológicos, aplicaciones o software, sino que también incluye la búsqueda, la evaluación y el uso de la información de manera responsable.

En el contexto de las estafas digitales esto le permitirá detectar direcciones de correo electrónico cuestionables, comunicaciones engañosas y confirmar las fuentes de los mensajes y de su información personal.

Hernández-Marín et al. (2024) revisaron varios instrumentos para evaluar las habilidades de alfabetización mediática, informacional y digital. Estos autores argumentan que las competencias involucran la combinación de conocimientos, habilidades y actitudes necesarias para el uso crítico de los medios y la información.

También es importante señalar que la evaluación no se basa solamente en las percepciones de las personas, sino que necesita incluir algunos instrumentos para identificar sus verdaderas habilidades.

Por otro lado, López-González et al. (2023), a través de una revisión sistemática de la educación mediática, informacional y del pensamiento crítico, destacaron la importancia de formar ciudadanos que puedan utilizar la información de manera reflexiva frente a los fenómenos de desinformación en los medios digitales.

En el estudio realizado por Rodríguez Cruz et al. (2025) los autores analizaron los obstáculos relacionados con la alfabetización mediática e

NEXUS
Revista Científica
ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

informacional en la era de la desinformación y destacaron la necesidad de desarrollar las habilidades necesarias para interpretar el contenido de manera crítica y crear una cultura de ciudadanos digitales responsables.

De manera similar Aceituno Silva (2024) en su estudio sobre la ciudadanía digital y la estrategia SIFT encontró los obstáculos relacionados con la lectura lateral y la verificación de la información entre los estudiantes de Chile.

Este estudio permite reconocer la necesidad de enseñar cómo verificar la información antes de compartirla. Asimismo, Castro-Montoya et al. (2024), en su investigación sobre profesores en formación de telesecundaria en México, analizaron la autopercepción de las habilidades de alfabetización mediática, informacional y digital.

Este estudio evidencia la importancia de desarrollar habilidades de alfabetización mediática, informacional y digital que permitan evaluar los contenidos, verificar las fuentes y utilizar la tecnología de manera crítica.

La alfabetización digital previene el fraude debido a su capacidad de cultivar habilidades que permitan a los usuarios detectar el fraude, autenticar fuentes, detectar enlaces sospechosos y salvaguardar la información personal.

Tabla 2

Competencias de alfabetización digital para prevenir las estafas digitales

Competencia	Aplicación preventiva
Verificación de información	Comprobar la autenticidad de mensajes y remitentes.
Pensamiento crítico	Analizar ofertas y solicitudes sospechosas.
Protección de datos	Evitar compartir contraseñas y códigos de seguridad.
Reconocimiento de amenazas	Identificar enlaces, perfiles y páginas fraudulentas.
Uso seguro de plataformas	Aplicar medidas de protección en cuentas y dispositivos.

Nota. Elaboración propia a partir de Hernández-Marín et al. (2024), López-González et al. (2023), Rodríguez Cruz et al. (2025) y Aceituno Silva (2024).

Vulnerabilidad digital y estrategias de prevención desde la educación

La susceptibilidad al fraude digital no es igual para todas las personas. El nivel de exposición a la tecnología, el conocimiento, la educación y el comportamiento de cada persona van a afectar la capacidad del usuario para detectar y manejar la amenaza.

Desde esta perspectiva, no sería justo asumir que las personas con una exposición limitada a la tecnología serán las únicas víctimas de estas estafas. Incluso los usuarios frecuentes de Internet pueden no detectar estafas, en especial si emplean técnicas persuasivas y son de fuentes creíbles.

En su revisión sistemática sobre el impacto de los factores humanos que afectan la vulnerabilidad a los ataques de phishing en profesores de universidades latinoamericanas, Ortega Correa et al. (2026) reconocieron la necesidad de un estudio sobre las prácticas de los usuarios y las brechas en la alfabetización digital.

Por el contrario, García Herrera y Quintero Ávila (2025) en su revisión sistemática sobre la

ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

educación digital y la prevención social de las estafas cibernéticas mencionaron la alfabetización digital, las campañas educativas, la capacitación y la gamificación como herramientas que podrían ayudar a disminuir la vulnerabilidad de los ciudadanos a las estafas digitales.

Por estas razones las acciones preventivas deben considerar factores individuales y ambientales. Capacitaciones consistentes, ejercicios prácticos para detectar fraudes, la difusión de información confiable y el desarrollo de buenas prácticas en cuanto a los procedimientos de verificación pueden ayudar a incrementar la seguridad de los usuarios.

También es necesario recordar que las tecnologías y la capacitación humana deben ir de la mano. La protección de los sistemas, la identificación de varios factores y los sistemas de detección de amenazas son útiles pero su efectividad se ve disminuida si la persona no está al tanto de las amenazas o no reconoce las señales de manipulación.

En general la lucha contra los fraudes digitales implica un enfoque integral que considere el conocimiento, las emociones, los comportamientos, las habilidades y las medidas tecnológicas de protección de los usuarios.

Materiales y métodos

La investigación actual se desarrolló siguiendo un enfoque metodológico cualitativo, mediante una revisión bibliográfica y documental descriptiva. Por lo tanto se utilizó esta metodología para analizar los factores psicológicos y las habilidades de alfabetización digital involucradas en la vulnerabilidad de las personas a las estafas digitales teniendo en cuenta las contribuciones científicas relativas a la ingeniería social, el comportamiento humano, la toma de decisiones y la prevención del fraude en espacios virtuales.

El diseño no es experimental porque la investigación no involucro la manipulación de ninguna variable ni la intervención de los sujetos. La información fue recolectada usando fuentes documentales secundarias, principalmente artículos científicos que abordan temas como la susceptibilidad al phishing, la manipulación psicológica, los sesgos cognitivos, la alfabetización digital y las acciones de prevención educativa contra el fraude.

Los materiales fueron publicaciones académicas relacionadas con el objeto de estudio, principalmente publicadas entre 2021 y 2026. Se tomaron en cuenta investigaciones empíricas, revisiones sistemáticas, estudios documentales y análisis sobre la seguridad digital y el comportamiento del usuario. Dichas fuentes proporcionan el marco teórico y el contexto científico que permitieron interpretar la relación entre los factores psicológicos, las habilidades digitales y la exposición de las personas a situaciones de fraude.

Para delimitar la revisión se tomó en cuenta la relevancia temática, la relación con el objetivo del estudio y la contribución de cada trabajo científico al conocimiento de las estafas digitales. Se priorizaron los trabajos científicos que tratan los factores humanos involucrados en el fraude, los métodos de ingeniería social, la percepción del riesgo, la respuesta emocional y las habilidades digitales para identificar el fraude. Además se tomaron en cuenta las investigaciones realizadas en Ecuador y otros

NEXUS
Revista Científica
ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

escenarios internacionales para aportar diferentes perspectivas al problema.

La información de la documentación fue sistematizada a través de una lectura analítica y comparativa de los trabajos científicos. De esta manera fue posible conocer el propósito, el enfoque metodológico, el contexto de la investigación y la contribución principal de cada publicación. Posteriormente se realizó una síntesis temática para determinar las similitudes, las diferencias y las relaciones entre los hallazgos científicos sin interpretarlos como resultados obtenidos en la investigación actual.

Para facilitar la organización de la información se definieron cinco categorías de análisis: estafas digitales e ingeniería social; factores psicológicos relacionados con la vulnerabilidad; emociones, confianza y sesgos cognitivos; alfabetización digital y pensamiento crítico; y acciones de prevención educativa. Dichas categorías permitieron establecer los vínculos entre el contexto científico

Análisis y resultados

La revisión de la literatura de la investigación científica desde el 2021 hasta el 2026 permite la distinción de diferentes formas de investigar la vulnerabilidad a las estafas digitales.

La investigación de fondo elegida incluye revisiones sistemáticas, la investigación documental y estudios empíricos que analizan el comportamiento del usuario, la ingeniería social, las habilidades digitales y las técnicas preventivas.

La investigación permite la organización de las evidencias a lo largo de tres dimensiones principales: elementos psicológicos que intervienen en el proceso de toma de decisiones, las habilidades digitales que permiten el reconocimiento de los riesgos digitales y los aspectos individuales y situacionales relacionados con el riesgo de ser víctima.

Tabla 3

Investigaciones científicas relacionadas con la vulnerabilidad frente a las estafas digitales

Autor y año	Contexto y metodología	Principales resultados o aportes
Desolda et al. (2021)	Revisión sistemática sobre factores humanos y phishing.	Destaca la importancia de los conocimientos, la conciencia y los comportamientos de los usuarios.
Baki y Verma (2023)	Revisión de investigaciones sobre susceptibilidad al phishing.	Examina las características de los usuarios y las estrategias de intervención.
López-González et al. (2023)	Revisión sistemática sobre alfabetización mediática y pensamiento crítico.	Destaca la importancia de formar ciudadanos capaces de evaluar críticamente la información.
Echeverría y Rodríguez Cano (2023)	Investigación sobre alfabetización digital y desinformación en México.	Analiza las actitudes y estrategias utilizadas para identificar noticias falsas.
Garzón Ibarra et al. (2024)	Estudio sobre ingeniería social en Ecuador.	Examina las tácticas de manipulación y las estrategias de prevención.
Pazmiño-Quiñonez et al. (2024)	Revisión de literatura sobre phishing automatizado.	Explica la evolución y sofisticación de los ataques de phishing.
Hernández-Marín et al. (2024)	Revisión exploratoria de instrumentos de alfabetización digital.	Identifica conocimientos, habilidades y actitudes como componentes de la competencia digital.

ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

Aceituno Silva (2024)	Investigación sobre razonamiento crítico y estrategia SIFT.	Identifica dificultades en la verificación de información digital.
Candanedo Yau (2025)	Estudio empírico sobre phishing y spam.	Identifica deficiencias en el reconocimiento y manejo de correos fraudulentos.
Rodríguez Cruz et al. (2025)	Análisis documental sobre alfabetización mediática e informacional.	Destaca la necesidad de fortalecer el pensamiento crítico frente a la desinformación.
García Herrera y Quintero Ávila (2025)	Revisión sistemática sobre educación digital y ciberestafas.	Reconoce la educación digital como estrategia de prevención social.
Chaguaro Escobar (2026)	Estudio cuantitativo con adultos ecuatorianos.	Identifica la toma de decisiones apresuradas y la confianza en información inexacta como dimensiones de susceptibilidad.
Ortega Correa et al. (2026)	Revisión sistemática sobre factores humanos y phishing en universidades latinoamericanas.	Destaca las brechas de conciencia digital y los comportamientos de los usuarios.

Nota. La tabla sintetiza los principales aportes de las investigaciones seleccionadas. Los resultados corresponden a sus respectivas poblaciones y metodologías, por lo que no representan datos obtenidos directamente en el presente artículo.

La investigación de fondo revisada permite observar que la vulnerabilidad a las estafas digitales es un problema multifacético. La revisión de la literatura no se limita a explorar las técnicas tecnológicas empleadas por los estafadores, sino que también considera los rasgos psicológicos, el conocimiento y las competencias que juegan un papel en la toma de decisiones de los consumidores.

En primer lugar, la investigación realizada por Desolda et al. (2021), Baki y Verma (2023) y Chaguaro Escobar (2026) permite reconocer la importancia de los factores humanos en la vulnerabilidad al phishing y las estafas digitales.

En segundo lugar, a partir del trabajo de Hernández-Marín et al. (2024), López-González et al. (2023), Aceituno Silva (2024) y Rodríguez Cruz et al. (2025), se comprende que la alfabetización digital es un aspecto importante para mejorar la capacidad de los usuarios para analizar, verificar y desarrollarse de manera crítica en un entorno digital.

De esta manera, se evidencia cómo las técnicas de engaño han evolucionado con la tecnología y tienen la capacidad de explotar el estado psicológico de los usuarios. Finalmente, los trabajos de García Herrera y Quintero Ávila (2025) y Ortega Correa et al. (2026), permiten identificar el papel de la educación y la capacitación institucional.

Uno de los antecedentes más relevantes corresponde al estudio de Chaguaro Escobar (2026), realizado con 1.200 adultos ecuatorianos, en el que se observó que el 52 % de los participantes presentaba una susceptibilidad moderada al fraude y el 26,5 % una susceptibilidad alta.

El estudio también identificó que la toma de decisiones apresuradas obtuvo una puntuación promedio de 3,68 y que esta variable presentó una correlación positiva de 0,67 con la confianza en información inexacta.

En otras palabras, mientras que las primeras pueden afectar la manera en la que las personas entienden los mensajes y manejan las

ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

situaciones que involucran el engaño, las segundas proporcionan el conocimiento necesario para evaluar los peligros.

Discusión

El análisis del contexto científico antes descrito permite comprender las estafas digitales no solo desde el punto de vista de sus características técnicas sino también desde el punto de vista de los componentes psicológicos y educativos de este fenómeno.

Al mismo tiempo, dado que las tecnologías de seguridad informática tienen que ser empleadas para reducir los posibles riesgos, también es considerar la influencia del comportamiento del usuario como un componente importante para evaluar la eficiencia del ataque.

Uno de los temas más importantes discutidos es la influencia de los factores psicológicos en el proceso de toma de decisiones. En otras palabras, la impulsividad, la sobre confianza y las emociones pueden influir en la comprensión de la información digital.

Este planteamiento se respalda en el estudio de Chaguaro Escobar (2026), quien determinó que la toma de decisiones apresuradas y la confianza en información inexacta están asociadas con la vulnerabilidad al fraude digital entre adultos ecuatorianos.

La convergencia de estos resultados permite comprender que la prevención implica considerar los procesos de pensamiento y comportamiento involucrados durante la recepción de un mensaje sospechoso. La alfabetización digital es un elemento importante que ayudaría a mejorar la capacidad de las personas para actuar.

Las teorías presentadas por Hernández-Marín et al. (2024) y López-González et al. (2023) permiten comprender que la competencia digital implica conocimientos, habilidades y actitudes que apoyan una interacción efectiva con la información.

Por lo tanto, una persona puede ser experimentada en el uso de dispositivos digitales y al mismo tiempo ser vulnerable al fraude. Este caso en particular también está relacionado con las teorías propuestas por Aceituno Silva (2024), quien señala los problemas asociados a la verificación de la información y al pensamiento crítico en Internet.

Es importante incluir la educación para desarrollar estas habilidades en la práctica. Desafíos como la automatización, el fraude de identidad y la inteligencia artificial representan una amenaza aún mayor.

Sin embargo, en cuanto al caso de Ecuador, los estudios de Garzón Ibarra y otros (2024) y de Chaguaro Escobar (2026) permiten revelar la importancia de analizar este desafío desde la perspectiva de las características del entorno nacional.

El estudio de Garzón Ibarra y otros (2024) analiza la ingeniería social mientras que el estudio de Chaguaro Escobar (2026) proporciona algunas evidencias empíricas sobre la vulnerabilidad de la población adulta de Ecuador al fraude digital.

NEXUS
Revista Científica
ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

Por consiguiente, dicha prevención no debe limitarse a la notificación de los posibles riesgos de Internet, sino que debe involucrar el desarrollo de habilidades que permitan reconocer y responder adecuadamente a estos peligros.

La educación digital debe incluir los casos prácticos de fraude, robo de identidad, ofrecimientos engañosos y solicitudes de información privada.

En definitiva, es necesario mencionar que los aspectos psicológicos y la alfabetización digital tienen que ser vistos como dos problemas interconectados. La competencia tecnológica no puede eliminar el riesgo de verse envuelto en un fraude igual que el conocimiento digital no puede garantizar una evaluación correcta de las amenazas. En este sentido se requiere un enfoque integral que integre medidas educativas y tecnológicas.

Conclusiones

El fenómeno de las estafas en línea es un problema que va más allá del lado técnico de la computación debido a que su efectividad está vinculada con las características psicológicas y de comportamiento de los usuarios también.

A partir de la revisión de la literatura, se evidencia que la impulsividad, el exceso de confianza, las emociones y la búsqueda de ganancias rápidas pueden afectar la toma de decisiones en la presencia de correos electrónicos fraudulentos.

Los aspectos psicológicos se convierten en una parte esencial para comprender las vulnerabilidades ya que afectan la percepción de los mensajes, la evaluación de la situación y las acciones que las personas toman cuando se enfrentan a riesgos potenciales.

Sin embargo, las características mencionadas no significan que una persona inevitablemente se convierta en una víctima, la alfabetización digital juega un papel clave como una herramienta efectiva para la prevención de estafas.

La adquisición de las habilidades necesarias para verificar la información, detectar mensajes fraudulentos, proteger los datos personales y evaluar la credibilidad de la fuente mejora la capacidad de los usuarios para enfrentar los riesgos en el entorno digital.

Además, la evidencia científica presentada también permite comprender que el uso constante de estos dispositivos y plataformas no implica necesariamente una preparación suficiente contra los riesgos.

Por lo tanto, es importante fomentar programas de capacitación que incorporen el conocimiento de la tecnología, el análisis y la comprensión de las técnicas de manipulación utilizadas en el fraude. Los estudios de Garzón Ibarra et al., (2024) y de Chaguaro Escobar (2026) provenientes del Ecuador hacen énfasis en la importancia de reforzar la educación digital y la prevención de estafas digitales.

La implementación de programas de alfabetización digital, campañas y entrenamiento práctico para identificar riesgos puede ayudar a construir una ciudadanía más consciente y preparada.

En definitiva, la revisión permite concluir que la prevención de los fraudes digitales requiere

ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

superar un enfoque exclusivamente tecnológico e incorporar estrategias de seguridad informática, conocimientos sobre los factores psicológicos involucrados y el desarrollo de habilidades de alfabetización digital. La capacidad para detectar estos engaños depende de la preparación de los usuarios y de la toma de decisiones críticas en entornos digitales.

Referencias bibliográficas

Baki, S., & Verma, R. M. (2022). Sixteen years of phishing user studies: What have we learned? *IEEE Transactions on Dependable and Secure Computing*, 1200-1212.

Campos Gallegos, M. G., Moreno Dillon, R. G., & Jiménez Espín, B. A. (2025). Detección de fraudes y estafas basadas en ingeniería social en Ecuador. *Revista InveCom*.

Correa, C. O., Ledezma, A., & Berbey, D. (2026). Factores humanos que influyen en la vulnerabilidad al phishing en docentes de universidades latinoamericanas. *Latitude*, 40-56.

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys*, 1-35.

Echeverría, M., & Cano, C. A. (2023). ¿ La alfabetización digital activa la incredulidad en noticias falsas? Eficacia de las actitudes y estrategias contra la desinformación en México. *Revista de Comunicación*, 79-95.

Escobar, E. J. (2026). Susceptibilidad a estafas digitales en adultos ecuatorianos: un análisis de los factores asociados al riesgo de victimización en entornos digitales. *KIRIA: Revista Científica Multidisciplinaria*, 119-131.

García Herrera, D. G., & Quintero Ávila, O. (2025). Educación digital como factor coadyuvante de la prevención social de ciberestafas: una revisión sistemática de literatura con la metodología PRISMA. *Revista Conrado*.

González, H. L., Sosa, L., Sánchez, L., & Carvallo, A. F. (2023). Educación mediática e informacional y pensamiento crítico: Una revisión sistemática. *Revista Latina de Comunicación Social*, 19.

Hernández-Marín, J. L., Castro-Montoya, M. D., & Figueroa-Rodríguez, S. (2024). Alfabetización Mediática, Informacional y Digital: análisis de instrumentos de evaluación. *Investigación bibliotecológica*, 55-73.

Hernández-Marín, J. L., Castro-Montoya, M. D., & Figueroa-Rodríguez, S. (2024). Alfabetización mediática, informacional y digital: Autopercepción de los docentes en formación de telesecundaria en México. *Revista Interamericana de Bibliotecología*.

Ibarra, C. S., Tapia, C. A., Tene, A. M., Toapanta, R. J., & Ormaza, G. S. (2024). Análisis de los Ataques de Ingeniería Social en Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, 4354-4367.

Quiñonez, J. P., De la Cueva, M. S., & Mendoza, L. Y. (2024). Análisis de la efectividad de phishing automático. *Revista Científica Élite*, 1-8.

Rodríguez Cruz, Y., Medina-González, V., & Almansa-Martínez, A. (2025). Alfabetización Mediática e Informacional (AMI) en tiempos de Desinformación: perspectivas en Iberoamérica. *Chasqui*, 189.

Silva, D. A. (2024). Ciudadanía digital, fake news y la desinformación. Uso de la estrategia SIFT y el desarrollo del razonamiento cívico online en la escuela. *European Public & Social Innovation Review*, 1-22.

NEXUS
Revista Científica
ISSN - L: 3103-1048 ISSN - E: 3091-2032
VOL. 2 NO. 6
Mes de Noviembre-Diciembre

Yau, R. M. (2026). Phishing y Spam: Un correo malintencionado. Seguridad digital de tu información ante el robo de datos. *Acción y reflexión educativa*, 235-254.

Más allá de la tecnología: Factores psicológicos y alfabetización digital asociados a la vulnerabilidad frente a las estafas digitales © 2026 by Stalin Patricio Songor Illescas, Patricio Sebastián Rosas Villagómez y Mark Anderson Uriarte Guzmán is licensed under Creative Commons Attribution-NonCommercial 4.0 International. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/4.0/