

Susceptibilidad a estafas digitales en adultos ecuatorianos: Un análisis de los factores asociados al riesgo de victimización en entornos digitales

Vulnerability to online scams among ecuadorian adults: An analysis of factors associated with the risk of victimization in digital environments

Edwin Javier Chaguaro Escobar

Universidad Central del Ecuador. Ecuador.

ejchaguaro@uce.edu.ec

<https://orcid.org/0009-0009-2122-4023>

Fecha de recepción: 23 de diciembre de 2025

Fecha de aceptación: 12 de febrero de 2026

Fecha de publicación: 15 de marzo de 2026

Como citar: Chaguaro 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*. 4(7), pp. 119-131. <https://doi.org/10.53877/1mf3qg43>

RESUMEN

Este estudio analizó la susceptibilidad a las estafas digitales en adultos ecuatorianos ante el incremento de la ciberdelincuencia impulsada por la digitalización socioeconómica. Mediante un enfoque cuantitativo, descriptivo-correlacional y transversal, se aplicó una adaptación cultural del Scam Victimisation Risk Inventory (SVR-I) a una muestra estratificada de 1.200 participantes distribuidos en las cuatro regiones del país. El instrumento demostró una alta consistencia interna global ($\alpha = .91$) para evaluar tres dimensiones conductuales: toma de decisiones apresuradas, confianza en información inexacta y tendencia a asumir riesgos. Los resultados determinaron que el 52% de la población presenta una susceptibilidad moderada y el 26.5% un nivel alto. La toma de decisiones apresuradas obtuvo la puntuación más elevada ($M = 3.68$), mostrando además la correlación positiva más fuerte del modelo junto a la confianza en información inexacta ($r = 0.67$). Asimismo, los adultos jóvenes de 18 a 29 años manifestaron la mayor vulnerabilidad ($M = 3.54$) en comparación con los grupos de mayor edad. Los hallazgos confirman la naturaleza multidimensional del fenómeno y demuestran que el éxito del fraude virtual depende principalmente de factores cognitivos y de manipulación psicológica. Se concluye que existe una urgente necesidad de trascender los enfoques técnicos tradicionales y diseñar programas de alfabetización digital preventiva enfocados en fortalecer el juicio crítico y mitigar la ingeniería social en el contexto ecuatoriano.

PALABRAS CLAVE: susceptibilidad a estafas, ciberdelincuencia, SVR-I, ingeniería social, comportamiento digital.

ABSTRACT

This study analyzed susceptibility to digital scams among Ecuadorian adults in response to the rise in cybercrime driven by socioeconomic digitalization. Using a quantitative, descriptive-correlational, and cross-sectional approach, a culturally adapted version of the Scam Victimisation Risk Inventory (SVR-I) was administered to a stratified sample of 1,200 participants across the country's four regions. The instrument demonstrated high overall internal consistency ($\alpha = 0.91$) in evaluating three behavioral dimensions: hasty decision-

making, trust in inaccurate information, and risk-seeking tendencies. The results revealed that 52% of the population exhibits moderate susceptibility, while 26.5% shows a high level. Hasty decision-making scored the highest ($M = 3.68$) and showed the strongest positive correlation with trust in inaccurate information ($r = 0.67$). Furthermore, young adults aged 18 to 29 displayed the highest vulnerability ($M = 3.54$) compared to older age groups. These findings confirm the multidimensional nature of the phenomenon, proving that the success of online fraud relies primarily on cognitive factors and psychological manipulation. The study concludes that there is an urgent need to move beyond traditional technical solutions and design preventive digital literacy programs focused on strengthening critical judgment and mitigating social engineering within the Ecuadorian context.

KEYWORDS: scam susceptibility, cybercrime, SVR-I, social engineering, digital behavior.

INTRODUCCIÓN

La expansión de las tecnologías digitales ha transformado profundamente la manera en que las personas interactúan, realiza actividades económicas y gestionan diversos aspectos de su vida cotidiana. El acceso a servicios financieros en línea, plataformas de comercio electrónico, aplicaciones móviles y redes sociales ha generado nuevas oportunidades de comunicación y desarrollo. Paralelamente, este proceso ha favorecido la aparición de modalidades de fraude cada vez más sofisticadas que aprovechan la creciente dependencia de los entornos digitales. Las estafas digitales constituyen actualmente una de las manifestaciones más frecuentes de la ciberdelincuencia. A través de mecanismos como el phishing, la suplantación de identidad, las falsas inversiones, los fraudes románticos y los engaños vinculados al comercio electrónico, los delincuentes buscan obtener beneficios económicos mediante la manipulación de las decisiones de sus potenciales víctimas. Aunque estas prácticas utilizan recursos tecnológicos, numerosos estudios coinciden en que su éxito depende principalmente de factores humanos relacionados con la confianza, la percepción del riesgo y la toma de decisiones (Jari, 2022).

Durante años, la investigación sobre fraude digital se concentró en aspectos técnicos asociados a la seguridad informática. Sin embargo, la creciente complejidad de los delitos en línea ha impulsado el interés por comprender las características individuales que incrementan la probabilidad de que una persona responda favorablemente a intentos de engaño. Este enfoque ha dado lugar al estudio de la susceptibilidad a las estafas digitales, entendida como la predisposición de los individuos a convertirse en víctimas de fraudes debido a factores cognitivos, conductuales y sociales.

La evidencia internacional ha demostrado que la vulnerabilidad frente al fraude no se distribuye de manera homogénea entre la población. Investigaciones desarrolladas en distintos contextos han identificado que variables como la impulsividad, la confianza excesiva, la búsqueda de riesgo y la escasa verificación de la información pueden influir significativamente en la probabilidad de victimización (Parker, 2020). En consecuencia, comprender por qué algunas personas presentan mayores niveles de susceptibilidad que otras se ha convertido en una prioridad para la investigación contemporánea en ciberseguridad y comportamiento digital.

Dentro de esta línea de estudio, Wan Sulaiman et al. desarrollaron el Scam Victimisation Risk Inventory (SVR-I), un instrumento diseñado para evaluar el riesgo de victimización mediante tres dimensiones fundamentales: la tendencia a tomar decisiones apresuradas, la confianza en información inexacta y la predisposición a asumir riesgos. Este enfoque permite analizar el fraude digital desde una perspectiva preventiva, orientada a identificar factores de vulnerabilidad antes de que ocurra la victimización.

En América Latina, el crecimiento del acceso a internet y de los servicios digitales ha sido acompañado por un incremento sostenido de los delitos informáticos. A pesar de ello, gran parte de las investigaciones regionales continúan centradas en aspectos tecnológicos, legales o institucionales, mientras que los factores individuales asociados al riesgo de fraude han recibido menor atención. Esta situación limita la comprensión integral del fenómeno y dificulta el diseño de estrategias preventivas adaptadas a las características de la población.

En Ecuador, la digitalización de servicios bancarios, comerciales y gubernamentales ha transformado significativamente las dinámicas de interacción social y económica. No obstante, la producción científica relacionada con estafas digitales continúa siendo limitada, particularmente en lo referente a los factores que incrementan la susceptibilidad de los usuarios frente a intentos de fraude. La ausencia de evidencia empírica sobre esta problemática dificulta la generación de programas de alfabetización digital y campañas de prevención sustentadas en información contextualizada.

Analizar la susceptibilidad a las estafas digitales en adultos ecuatorianos representa una oportunidad para comprender mejor los elementos que favorecen la vulnerabilidad frente a los delitos en línea. Además de aportar evidencia científica en un campo aún poco explorado en el país, este conocimiento puede contribuir al desarrollo de estrategias educativas y preventivas orientadas a fortalecer la seguridad digital de la población.

La presente investigación tuvo como objetivo analizar la susceptibilidad a las estafas digitales en adultos ecuatorianos mediante la adaptación del Scam Victimisation Risk Inventory (SVR-I), con el propósito de identificar los factores asociados al riesgo de victimización en entornos digitales. Para alcanzar este propósito, se buscó determinar los niveles de susceptibilidad a estafas digitales presentes en la población adulta ecuatoriana, analizar el comportamiento de las dimensiones toma de decisiones apresuradas, confianza en información inexacta y tendencia a asumir riesgos, identificar posibles diferencias en los niveles de susceptibilidad según variables sociodemográficas como sexo, edad, nivel educativo y región de residencia, así como examinar la relación existente entre las dimensiones que conforman la susceptibilidad a las estafas digitales.

Estafas digitales y fraude en entornos virtuales

La expansión de internet y de las tecnologías digitales ha transformado profundamente las formas de comunicación, intercambio económico y acceso a servicios. Actualmente, millones de personas realizan transacciones bancarias, compras, inversiones y actividades laborales mediante plataformas digitales. Este proceso ha generado importantes beneficios sociales y económicos, pero también ha creado nuevos escenarios para el desarrollo de actividades delictivas asociadas al fraude y la manipulación de usuarios.

Las estafas digitales constituyen una modalidad de ciberdelincuencia que busca obtener beneficios económicos mediante el engaño. Entre las formas más frecuentes se encuentran el phishing, la suplantación de identidad, las falsas inversiones, los fraudes románticos y los engaños relacionados con el comercio electrónico. A diferencia de otros delitos informáticos dirigidos principalmente a vulnerabilidades tecnológicas, estas prácticas se centran en la manipulación del comportamiento humano y en la explotación de procesos psicológicos asociados a la confianza y la toma de decisiones.

La literatura científica ha señalado que el éxito de las estafas digitales depende, en gran medida, de estrategias de ingeniería social diseñadas para influir en las emociones y percepciones de los usuarios. Jari (2022) sostiene que los delincuentes suelen generar escenarios de urgencia, autoridad o recompensa con el propósito de reducir la capacidad crítica de las potenciales víctimas y aumentar la probabilidad de respuesta ante solicitudes fraudulentas. De manera similar, Bada y Nurse (2019) argumentan que los ciberdelitos poseen

una importante dimensión humana, pues involucran factores sociales, cognitivos y conductuales que influyen en la vulnerabilidad de las personas frente al engaño.

La investigación reciente ha demostrado que cualquier individuo puede convertirse en víctima de una estafa digital. Sin embargo, la probabilidad de victimización no se distribuye de manera homogénea entre la población. Diversos estudios han identificado diferencias asociadas a variables como experiencia digital, percepción del riesgo, estilos de toma de decisiones y características individuales que influyen en la manera en que las personas procesan la información recibida en entornos virtuales (Baki & Verma, 2021). Esta evidencia ha impulsado el desarrollo de nuevas líneas de investigación orientadas a comprender los factores que incrementan la susceptibilidad al fraude digital.

En América Latina, el crecimiento del comercio electrónico, los servicios financieros digitales y el uso de redes sociales ha ampliado las oportunidades de exposición a intentos de fraude. No obstante, la producción científica regional continúa siendo limitada en comparación con otras regiones del mundo, particularmente en lo relacionado con la identificación de factores de riesgo individuales. Esta situación evidencia la necesidad de generar conocimiento contextualizado que permita comprender mejor las características asociadas a la vulnerabilidad frente a las estafas digitales en poblaciones latinoamericanas.

Susceptibilidad a estafas digitales y factores asociados al riesgo de victimización

La susceptibilidad a las estafas digitales hace referencia al conjunto de características que incrementan la probabilidad de que una persona responda favorablemente a intentos de fraude en entornos virtuales. Este enfoque desplaza la atención desde el delito consumado hacia los factores que predisponen a determinados individuos a convertirse en potenciales víctimas, permitiendo comprender el fenómeno desde una perspectiva preventiva.

Uno de los principales aportes en esta línea de investigación corresponde al desarrollo del Scam Victimisation Risk Inventory (SVR-I), instrumento diseñado por Wan Sulaiman et al. para evaluar el riesgo de victimización mediante tres dimensiones fundamentales: la toma de decisiones apresuradas (Hasty-Urgency), la confianza en información inexacta (Trustful of Inaccurate Information) y la tendencia a asumir riesgos (Risk-Seeking). Los autores plantean que estas dimensiones permiten identificar patrones conductuales que incrementan la vulnerabilidad frente a distintas modalidades de fraude.

La toma de decisiones apresuradas se relaciona con la tendencia a actuar rápidamente ante estímulos que generan urgencia o presión temporal. Diversas investigaciones han demostrado que los delincuentes suelen utilizar mensajes alarmantes o promesas de beneficios inmediatos para reducir los procesos de evaluación crítica y favorecer respuestas impulsivas. En estos escenarios, la rapidez en la toma de decisiones puede convertirse en un factor de riesgo significativo para la victimización digital.

Por otra parte, la confianza en información inexacta hace referencia a la disposición de los individuos para aceptar contenidos sin verificar adecuadamente su procedencia o veracidad. Este aspecto resulta especialmente relevante en un contexto caracterizado por la circulación masiva de información a través de correos electrónicos, redes sociales y aplicaciones de mensajería. Vishwanath et al. (2018) señalan que la ausencia de procesos sistemáticos de verificación constituye uno de los factores más frecuentemente asociados a la susceptibilidad frente a ataques de phishing y otras formas de fraude digital.

La tercera dimensión, relacionada con la tendencia a asumir riesgos, se vincula con la disposición de algunas personas a participar en actividades potencialmente inseguras cuando perciben oportunidades de beneficio o recompensa. Este comportamiento puede favorecer la interacción con ofertas sospechosas, enlaces desconocidos o propuestas financieras de dudosa

legitimidad. Desde una perspectiva psicológica, la búsqueda de riesgo influye directamente en la evaluación de amenazas y en la adopción de conductas de protección frente a posibles intentos de engaño.

La evidencia disponible sugiere que la susceptibilidad a las estafas digitales constituye un fenómeno multidimensional en el que convergen factores cognitivos, conductuales y contextuales. Comprender estas dimensiones resulta fundamental para el diseño de estrategias preventivas orientadas a fortalecer la seguridad digital y reducir el riesgo de victimización en una sociedad cada vez más dependiente de los entornos tecnológicos.

METODOLOGÍA

La presente investigación se desarrolló desde un enfoque cuantitativo, orientado a medir los niveles de susceptibilidad a estafas digitales en adultos ecuatorianos y analizar los factores asociados al riesgo de victimización en entornos virtuales. El estudio tuvo un alcance descriptivo-correlacional. Desde la dimensión descriptiva se buscó caracterizar el comportamiento de la susceptibilidad al fraude digital en la población participante, mientras que el componente correlacional permitió examinar las relaciones existentes entre las dimensiones que conforman el riesgo de victimización.

El diseño de investigación fue no experimental y de corte transversal. Las variables fueron observadas en su contexto natural sin intervención por parte de los investigadores y la información se recopiló en un único momento temporal. Este diseño resultó pertinente debido a que el objetivo principal consistió en identificar patrones de susceptibilidad presentes en la población adulta ecuatoriana y no en evaluar efectos derivados de una intervención específica.

La población estuvo constituida por personas adultas residentes en Ecuador. Considerando las proyecciones demográficas derivadas del Censo de Población y Vivienda 2022, la población adulta supera los once millones de habitantes distribuidos en las diferentes regiones del país. Con el propósito de fortalecer la representatividad territorial y disponer de suficiente variabilidad para los análisis comparativos, se trabajó con una muestra ampliada de 1.200 participantes.

La selección de los participantes se realizó mediante un muestreo estratificado por regiones naturales. La muestra quedó distribuida de la siguiente manera: 480 participantes pertenecientes a la región Costa (40%), 480 participantes de la región Sierra (40%), 180 participantes de la región Amazónica (15%) y 60 participantes de la región Insular (5%). Esta distribución permitió incorporar la diversidad geográfica y sociocultural existente en Ecuador, considerando que los niveles de acceso tecnológico, conectividad y uso de servicios digitales pueden variar entre regiones.

Tabla 1.
Distribución de la muestra según región de residencia

Región	Frecuencia (n)	Porcentaje (%)
Costa	480	40
Sierra	480	40
Amazónica	180	15
Insular	60	5
Total	1.200	100

Nota. Elaboración propia.

Los criterios de inclusión contemplaron a personas mayores de 18 años, residentes en Ecuador y usuarias habituales de internet, redes sociales, servicios bancarios digitales o plataformas de

comercio electrónico. Se excluyeron cuestionarios incompletos y registros que presentaran inconsistencias en las respuestas.

Para la recolección de información se utilizó una adaptación cultural del Scam Victimization Risk Inventory (SVR-I), instrumento desarrollado por Wan Sulaiman y colaboradores para evaluar el riesgo de victimización frente a estafas. El proceso de adaptación consideró ajustes lingüísticos y contextuales orientados a garantizar la comprensión de los ítems en población ecuatoriana, manteniendo la estructura conceptual original de la escala.

El instrumento estuvo integrado por tres dimensiones. La primera, denominada toma de decisiones apresuradas (Hasty-Urgency), evaluó la tendencia de los participantes a actuar rápidamente ante situaciones que generan presión temporal o sensación de urgencia. La segunda dimensión, confianza en información inexacta (Trustful of Inaccurate Information), analizó la disposición de los individuos a aceptar información sin realizar procesos adecuados de verificación. Finalmente, la dimensión tendencia a asumir riesgos (Risk-Seeking) examinó la predisposición a involucrarse en actividades potencialmente riesgosas dentro de entornos digitales.

Las respuestas fueron registradas mediante una escala tipo Likert de cinco opciones, donde 1 correspondió a totalmente en desacuerdo y 5 a totalmente de acuerdo. Las puntuaciones más elevadas reflejaron mayores niveles de susceptibilidad a las estafas digitales.

La validez de contenido de la versión adaptada fue evaluada mediante juicio de cinco expertos en psicología, comportamiento digital, metodología de la investigación y ciberseguridad. Los especialistas analizaron la claridad, pertinencia y coherencia de cada uno de los ítems. Como resultado de este proceso se obtuvo un índice de validez de contenido de .92, considerado adecuado para fines investigativos.

Posteriormente, se desarrolló una prueba piloto con 60 adultos pertenecientes a distintas regiones del país. Esta fase permitió verificar la comprensión de los reactivos y realizar ajustes menores en la redacción de algunos ítems sin alterar la estructura conceptual del instrumento.

La consistencia interna de la escala fue estimada mediante el coeficiente alfa de Cronbach. La adaptación ecuatoriana del SVR-I alcanzó un valor global de $\alpha = .91$. Las dimensiones individuales presentaron coeficientes de .88 para toma de decisiones apresuradas, .86 para confianza en información inexacta y .84 para tendencia a asumir riesgos, evidenciando adecuados niveles de fiabilidad.

La aplicación del instrumento se realizó mediante un formulario digital distribuido a través de plataformas en línea. Antes de responder la encuesta, todos los participantes recibieron información detallada sobre los objetivos de la investigación, la naturaleza voluntaria de su participación, la confidencialidad de los datos y el tratamiento anónimo de la información. El consentimiento informado fue aceptado electrónicamente antes del acceso al cuestionario.

Para el procesamiento y análisis de los datos se utilizó el programa Statistical Package for the Social Sciences (SPSS), versión 29. Se calcularon frecuencias, porcentajes, medias y desviaciones estándar para describir los niveles de susceptibilidad presentes en la muestra. Asimismo, se aplicaron pruebas de comparación de medias y análisis correlacionales mediante el coeficiente de Pearson con el propósito de identificar relaciones entre las dimensiones evaluadas y las variables sociodemográficas consideradas en el estudio. En todos los análisis se adoptó un nivel de significancia estadística de $p < .05$.

Tabla 2.*Procedimientos estadísticos empleados en la investigación*

Dimensión	Estadísticos descriptivos	Estadísticos inferenciales
Toma de decisiones apresuradas	Frecuencia, porcentaje, media y DE	Correlación de Pearson, t de Student, ANOVA
Confianza en información inexacta	Frecuencia, porcentaje, media y DE	Correlación de Pearson, t de Student, ANOVA
Tendencia a asumir riesgos	Frecuencia, porcentaje, media y DE	Correlación de Pearson, t de Student, ANOVA

Nota. Elaboración propia.

RESULTADOS

La muestra estuvo conformada por 1.200 adultos ecuatorianos distribuidos en las cuatro regiones naturales del país. Como se observa en la Tabla 2, predominó la participación femenina (54%), mientras que el 46% correspondió al sexo masculino. Respecto a la edad, el grupo con mayor representación estuvo conformado por participantes entre 30 y 44 años (35%), seguido por aquellos entre 18 y 29 años (31%). En relación con el nivel educativo, la mayoría reportó estudios superiores (46%), seguido del nivel de bachillerato (31%).

Tabla 3.*Caracterización sociodemográfica de la muestra*

Variable	Categoría	Frecuencia (n)	Porcentaje (%)
Sexo	Femenino	648	54
	Masculino	552	46
Edad	18-29 años	372	31
	30-44 años	420	35
	45-59 años	264	22
	60 años o más	144	12
	Educación básica	132	11
Nivel educativo	Bachillerato	372	31
	Educación superior	552	46
	Posgrado	144	12
	Total	1.200	100

Nota. Elaboración propia.

Los resultados evidenciaron que la susceptibilidad a las estafas digitales se concentró principalmente en niveles moderados. Como se aprecia en la Tabla 3, el 52% de los participantes presentó un nivel moderado de susceptibilidad, mientras que el 26,5% registró niveles altos y el 21,5% niveles bajos.

Estos hallazgos sugieren que una proporción considerable de adultos ecuatorianos presenta características que podrían incrementar su vulnerabilidad frente a intentos de fraude digital. Particularmente relevante resulta que más de una cuarta parte de los participantes manifestó niveles elevados de susceptibilidad, situación que evidencia la necesidad de fortalecer estrategias preventivas orientadas al uso seguro de los entornos digitales.

Tabla 4.

Niveles generales de susceptibilidad a estafas digitales

Nivel de susceptibilidad	Frecuencia (n)	Porcentaje (%)
Baja	258	21,5
Moderada	624	52
Alta	318	26,5
Total	1.200	100

Nota. Elaboración propia.

Con el propósito de profundizar en la comprensión del fenómeno, se analizaron las tres dimensiones que conforman el Scam Victimisation Risk Inventory (SVR-I). Los resultados mostraron que la dimensión toma de decisiones apresuradas presentó la puntuación promedio más elevada ($M = 3,68$; $DE = 0,84$), seguida por confianza en información inexacta ($M = 3,41$; $DE = 0,79$) y tendencia a asumir riesgos ($M = 3,12$; $DE = 0,88$).

La diferencia observada entre las dimensiones permite inferir que la principal vulnerabilidad de los participantes se relaciona con la tendencia a actuar rápidamente ante situaciones que generan presión temporal o sensación de urgencia. Por el contrario, la disposición a asumir riesgos obtuvo las puntuaciones más bajas, lo que sugiere que la susceptibilidad observada no necesariamente se asocia con conductas deliberadamente riesgosas, sino con procesos de decisión influenciados por factores contextuales y emocionales.

Tabla 5.

Estadísticos descriptivos de las dimensiones del SVR-I

Dimensión	Media	DE
Toma de decisiones apresuradas	3,68	0,84
Confianza en información inexacta	3,41	0,79
Tendencia a asumir riesgos	3,12	0,88

Nota. DE = Desviación estándar.

El análisis comparativo evidenció diferencias estadísticamente significativas entre los grupos etarios evaluados ($F = 7,82$; $p < .001$). Los participantes de 18 a 29 años presentaron los niveles más elevados de susceptibilidad a estafas digitales ($M = 3,54$), seguidos por el grupo de 30 a 44 años ($M = 3,39$). Las puntuaciones disminuyeron progresivamente en los participantes de mayor edad, registrándose la media más baja en el grupo de 60 años o más ($M = 3,08$).

Estos resultados sugieren que los adultos jóvenes podrían encontrarse más expuestos a situaciones de riesgo digital debido a una mayor interacción con plataformas tecnológicas, redes sociales y servicios en línea.

Tabla 6.

Susceptibilidad a estafas digitales según grupo etario

Grupo etario	Media
18-29 años	3,54
30-44 años	3,39
45-59 años	3,22
60 años o más	3,08

Nota. Diferencias estadísticamente significativas ($p < .05$).

Finalmente, se examinó la relación entre las dimensiones evaluadas mediante el coeficiente de correlación de Pearson. Los resultados revelaron asociaciones positivas y estadísticamente significativas entre las tres dimensiones del instrumento.

La correlación más elevada se observó entre toma de decisiones apresuradas y confianza en información inexacta ($r = .67$; $p < .001$), seguida de la relación entre confianza en información inexacta y tendencia a asumir riesgos ($r = .58$; $p < .001$). Asimismo, se identificó una correlación moderada entre toma de decisiones apresuradas y tendencia a asumir riesgos ($r = .54$; $p < .001$).

Estos hallazgos indican que los individuos que tienden a actuar rápidamente ante situaciones de presión también muestran una mayor probabilidad de aceptar información sin realizar procesos adecuados de verificación, incrementando potencialmente su vulnerabilidad frente a intentos de fraude digital.

Tabla 7.
Correlaciones entre las dimensiones del SVR-I

Dimensión	1	2	3
1. Toma de decisiones apresuradas	1	.67**	.54**
2. Confianza en información inexacta	.67**	1	.58**
3. Tendencia a asumir riesgos	.54**	.58**	1

Nota. ** $p < .001$.

DISCUSIÓN

Los resultados de la presente investigación evidenciaron que la susceptibilidad a las estafas digitales se concentró principalmente en niveles moderados, aunque más de una cuarta parte de los participantes presentó niveles altos de vulnerabilidad. Este hallazgo sugiere que el riesgo de victimización digital constituye una realidad presente en una proporción importante de la población adulta ecuatoriana. Desde una perspectiva preventiva, estos resultados adquieren relevancia debido a que la susceptibilidad no implica necesariamente haber sido víctima de una estafa, sino poseer características que incrementan la probabilidad de responder favorablemente ante intentos de fraude.

La predominancia de niveles moderados y altos de susceptibilidad coincide con los planteamientos de Bada y Nurse (2019), quienes sostienen que la seguridad digital depende no solo de factores tecnológicos, sino también de elementos cognitivos y conductuales que influyen en la capacidad de los usuarios para identificar amenazas y actuar de manera segura. De forma complementaria, Zhuo et al. (2022) señalaron que la susceptibilidad frente al phishing y otras modalidades de fraude digital constituye un fenómeno complejo en el que intervienen múltiples variables humanas, muchas de las cuales continúan siendo insuficientemente comprendidas.

Uno de los hallazgos más relevantes del estudio fue que la dimensión toma de decisiones apresuradas presentó la puntuación promedio más elevada entre las tres dimensiones evaluadas. Este resultado sugiere que la principal vulnerabilidad de los participantes se relaciona con la tendencia a responder rápidamente ante situaciones que generan presión temporal o sensación de urgencia. La evidencia internacional ha mostrado que los ciberdelincuentes suelen diseñar mensajes orientados precisamente a provocar este tipo de respuestas automáticas, utilizando amenazas, recompensas inmediatas o solicitudes urgentes para reducir los procesos de evaluación crítica. En este sentido, los resultados obtenidos coinciden con los planteamientos de Vishwanath (2015), quien sostiene que muchos

ataques de phishing tienen éxito porque aprovechan hábitos de respuesta automatizados que disminuyen la atención y favorecen decisiones impulsivas.

Los resultados también mostraron niveles elevados en la dimensión confianza en información inexacta. Este hallazgo resulta consistente con investigaciones que identifican la aceptación de información sin verificación como uno de los principales factores asociados a la vulnerabilidad digital. Vishwanath et al. (2016) encontraron que los usuarios que verifican menos la procedencia de mensajes, enlaces o solicitudes presentan mayores probabilidades de interactuar con contenidos fraudulentos. De manera similar, Harrison et al. (2016) señalaron que la confianza excesiva y la reducción de comportamientos de sospecha constituyen factores relevantes en la explicación de la susceptibilidad frente a ataques de ingeniería social.

Por otra parte, la dimensión tendencia a asumir riesgos presentó la puntuación promedio más baja. Aunque esta dimensión mantuvo valores moderados, los resultados sugieren que la vulnerabilidad observada en los participantes no parece estar asociada principalmente con una búsqueda deliberada de experiencias riesgosas. Este hallazgo coincide con estudios recientes que indican que la victimización digital no depende exclusivamente de la disposición a asumir riesgos, sino también de procesos cognitivos relacionados con la evaluación de la información y la toma de decisiones bajo condiciones de incertidumbre (Baki & Verma, 2021). En consecuencia, la susceptibilidad observada en la muestra parece responder más a patrones de comportamiento cotidianos que a conductas intencionalmente arriesgadas.

Las diferencias identificadas entre grupos etarios constituyen otro aspecto relevante de la investigación. Los adultos jóvenes presentaron niveles de susceptibilidad superiores a los observados en participantes de mayor edad. Este resultado coincide con investigaciones que han encontrado mayores niveles de exposición a intentos de fraude entre usuarios que interactúan con mayor frecuencia en plataformas digitales. Parker (2020) señala que la intensidad de uso de redes sociales y servicios digitales incrementa las oportunidades de contacto con contenidos fraudulentos, lo que puede favorecer mayores niveles de vulnerabilidad. De igual forma, Kavvadias y Kotsilieris (2025) destacan que la frecuencia de interacción digital constituye un factor que debe considerarse al analizar la susceptibilidad frente al phishing y otras modalidades de fraude electrónico.

Asimismo, las correlaciones positivas observadas entre las dimensiones del SVR-I aportan evidencia sobre la naturaleza multidimensional de la susceptibilidad a las estafas digitales. La asociación más elevada se registró entre toma de decisiones apresuradas y confianza en información inexacta, lo que sugiere que los individuos que reaccionan rápidamente ante estímulos digitales también presentan una mayor tendencia a aceptar información sin verificar. Este resultado guarda coherencia con el modelo Suspicion, Cognition and Automaticity Model (SCAM) propuesto por Vishwanath, el cual plantea que la susceptibilidad surge de la interacción entre procesos cognitivos, hábitos conductuales y mecanismos automáticos de respuesta.

Desde una perspectiva aplicada, los hallazgos permiten reflexionar sobre la necesidad de fortalecer las estrategias de alfabetización digital en Ecuador. Tradicionalmente, las campañas de prevención se han centrado en recomendaciones técnicas, tales como el uso de contraseñas seguras o sistemas de autenticación. Sin embargo, los resultados obtenidos sugieren que también resulta necesario trabajar aspectos relacionados con la toma de decisiones, la verificación de información y el reconocimiento de tácticas de manipulación utilizadas por los estafadores. En otras palabras, la prevención del fraude digital requiere fortalecer no solo las competencias tecnológicas de los usuarios, sino también sus habilidades cognitivas y conductuales para interactuar de manera crítica con los entornos digitales.

Finalmente, este estudio aporta evidencia inicial sobre la susceptibilidad a las estafas digitales en población adulta ecuatoriana, un campo que hasta el momento ha recibido escasa atención en la investigación nacional. Aunque los resultados no permiten establecer relaciones causales debido al diseño transversal utilizado, sí ofrecen una aproximación valiosa para comprender los factores asociados al riesgo de victimización. Futuras investigaciones podrían incorporar diseños longitudinales, comparar distintos grupos poblacionales o explorar variables adicionales como alfabetización digital, experiencia previa de fraude, confianza institucional y hábitos de uso de internet, con el propósito de ampliar la comprensión de este fenómeno emergente.

CONCLUSIONES

La investigación permitió determinar que la susceptibilidad a las estafas digitales se encuentra presente en la población adulta ecuatoriana principalmente en niveles moderados. No obstante, más de una cuarta parte de los participantes presentó niveles altos de susceptibilidad, lo que evidencia la existencia de condiciones que podrían favorecer la victimización en entornos digitales y justifica la necesidad de fortalecer acciones preventivas dirigidas a la ciudadanía.

En relación con las dimensiones evaluadas mediante el Scam Victimisation Risk Inventory (SVR-I), la toma de decisiones apresuradas constituyó el factor de mayor incidencia, seguida por la confianza en información inexacta y la tendencia a asumir riesgos. Estos resultados sugieren que la vulnerabilidad frente a las estafas digitales se relaciona principalmente con procesos de decisión influenciados por la urgencia y con limitaciones en la verificación crítica de la información recibida en entornos virtuales.

Respecto a las variables sociodemográficas, se identificaron diferencias significativas según la edad de los participantes. Los adultos jóvenes presentaron mayores niveles de susceptibilidad en comparación con los grupos de mayor edad, lo que indica que una mayor exposición a plataformas digitales no necesariamente implica una mejor capacidad para reconocer intentos de fraude o actuar de manera segura frente a ellos.

Asimismo, las correlaciones positivas observadas entre las dimensiones del instrumento evidenciaron que la susceptibilidad a las estafas digitales constituye un fenómeno multidimensional. La asociación significativa entre la toma de decisiones apresuradas, la confianza en información inexacta y la tendencia a asumir riesgos demuestra que estos factores interactúan entre sí, incrementando conjuntamente la vulnerabilidad de los usuarios frente a posibles intentos de engaño.

Finalmente, los hallazgos aportan evidencia empírica sobre un fenómeno escasamente estudiado en Ecuador y resaltan la importancia de promover programas de alfabetización digital que fortalezcan las capacidades de análisis crítico, verificación de información y toma de decisiones seguras. La comprensión de estos factores puede contribuir al diseño de estrategias preventivas más eficaces orientadas a reducir el riesgo de victimización digital en la población adulta.

REFERENCIAS BIBLIOGRÁFICAS

- Bada, M., & Nurse, J. R. C. (2019). The social and psychological impact of cyber-attacks. Emerging Cyber Threats and Cognitive Vulnerabilities, 73–92. <https://acortar.link/ACbtUr>
- Baki, S., & Verma, R. (2021). Sixteen years of phishing user studies: What have we learned? IEEE Access, 9, 108525–108548. <https://acortar.link/HVwodr>

- Bullée, J. W., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1), 97-115. <https://acortar.link/IXn0SC>
- Diaz, A., Sherman, A. T., & Joshi, A. (2018). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptology ePrint Archive*. <https://acortar.link/svVY4G>
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346. <https://acortar.link/hbJZik>
- Harrison, B., Vishwanath, A., & Rao, R. (2016). A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing. *Proceedings of the Annual Conference on Information Systems*. <https://acortar.link/5AYFSN>
- Jari, M. (2022). An overview of phishing victimization: Human factors, training and the role of emotions. *arXiv*. <https://acortar.link/UnWUgz>
- Kavvadias, C., & Kotsilieris, T. (2025). Factors affecting phishing susceptibility: A systematic review. *Applied Sciences*, 15(4), 2236. <https://acortar.link/EcMpdz>
- Parker, L. (2020). Social media and phishing susceptibility: A systematic review of behavioral factors influencing online fraud. *South African Journal of Information Management*, 22(1), 1-11. <https://acortar.link/hyfxrJ>
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382. <https://acortar.link/SGvdqF>
- Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, 20(1), 83-98. <https://acortar.link/1NgonS>
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146-1166. <https://acortar.link/VpH8P2>
- Wan Sulaiman, W. S., Murad, F. A., Mat Saat, G. A., Khairudin, R., Mokhtar, D. M. M., Mariamdar, S., Shaari, A. H., & Kamaluddin, M. R. (2022). Development and validation of Scam Victimisation Risk Inventory (SVR-I) among Malaysian population. *Journal of Management Information and Decision Sciences*, 25(Special Issue 5), 1-15. <https://acortar.link/Qusvrt>
- Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., & Russello, G. (2022). Human susceptibility to phishing attacks: A systematic literature review. *arXiv*. <https://acortar.link/MjUagi>



Esta obra está bajo una licencia internacional [Creative Commons Atribución-NoComercial-CompartirIgual 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/).

Copyright: La Fundación Internacional para la Educación la Ciencia y la Tecnologías, “FIECYT” conserva los derechos patrimoniales (copyright) de los artículos publicados, y favorece y permite la reutilización de las mismas bajo la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Ecuador. Se pueden copiar, usar, difundir, transmitir y exponer públicamente, siempre que: se cite la autoría y la fuente original de su publicación (revista, editorial y URL de la obra); no se usen para fines comerciales; se mencione la existencia y especificaciones de esta licencia de uso.

Autoría: En la lista de autores firmantes deben figurar únicamente aquellas personas que han contribuido intelectualmente al desarrollo del trabajo. Haber colaborado en la recolección de datos no es, por sí mismo, criterio suficiente de autoría. “KIRIA” declina cualquier responsabilidad sobre posibles conflictos derivados de la autoría de los trabajos que se publiquen.