Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Concienciación y educación en ciberseguridad para adultos mayores: una revisión sistemática de la literatura

Cybersecurity awareness and education for older adults: a systematic literature review

Klever E. Macas Chicaiza[1], José Baculima-Suárez[1], Andrea del Pilar Sánchez-Pinto[1]

[1]Universidad Católica de Cuenca. Ecuador
klever.macas.81@est.ucacue.edu.ec
https://orcid.org/0009-0002-4442-4502

jbaculima@ucacue.edu.ec
https://orcid.org/0000-0002-6695-665X

andrea.sanchez@ucacue.edu.ec
https://orcid.org/0000-0002-3826-0321

Correspondence: jbaculima@ucacue.edu.ec

Recibido: 19/04/2026
Aceptado: 21/06/2026
Publicado: 23/07/2026

Resumen

Objetivo: La investigación analizó la evidencia científica disponible sobre los programas de concienciación, educación y entrenamiento en ciberseguridad dirigidos a adultos mayores, con el propósito de identificar los enfoques más efectivos y las principales brechas existentes en este campo, especialmente en contextos latinoamericanos. **Metodología:** Se realizó una revisión sistemática de la literatura siguiendo las directrices del protocolo PRISMA 2020. La búsqueda se efectuó en las bases de datos Scopus y Web of Science, considerando publicaciones entre 2015 y 2026. De los 282 registros identificados inicialmente, se eliminaron 84 duplicados y, tras el proceso de cribado, evaluación de elegibilidad y valoración de calidad metodológica mediante criterios del Joanna Briggs Institute (JBI), se conformó un corpus final de 53 estudios. **Resultados:** Los hallazgos evidenciaron que los adultos mayores presentaron una vulnerabilidad significativa frente a amenazas digitales como phishing, fraude en línea e ingeniería social. Las intervenciones activas, personalizadas e intergeneracionales mostraron

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

mejores resultados que los enfoques basados únicamente en materiales informativos. Asimismo, los modelos multinivel OSICSAM y SCSAM-Elderly demostraron avances relevantes, aunque su validación permaneció limitada a contextos específicos. **Conclusiones:** La revisión permitió establecer la necesidad de desarrollar programas contextualizados, culturalmente adaptados y sustentados en evidencia, además de fortalecer la investigación latinoamericana, generar instrumentos validados en español y promover políticas públicas de ciberseguridad que incorporen de manera explícita a los adultos mayores.

Palabras clave: Ciberseguridad; adultos mayores; alfabetización digital; concienciación; phishing.

Abstract

Objective: The research analyzed the available scientific evidence on cybersecurity awareness, education, and training programs aimed at older adults, with the purpose of identifying the most effective approaches and the main existing gaps in this field, especially in Latin American contexts. **Methodology:** A systematic literature review was conducted following the guidelines of the PRISMA 2020 protocol. The search was conducted in the Scopus and Web of Science databases, considering publications between 2015 and 2026. Of the 282 records initially identified, 84 duplicates were removed, and after the screening process, eligibility assessment, and methodological quality evaluation using Joanna Briggs Institute (JBI) criteria, a final corpus of 53 studies was formed. **Results:** The findings revealed that older adults exhibited significant vulnerability to digital threats such as phishing, online fraud, and social engineering. Active, personalized, and intergenerational interventions showed better results than approaches based solely on informational materials. Likewise, the OSICSAM and SCSAM-Elderly multilevel models demonstrated significant advances, although their validation remained limited to specific contexts. **Conclusions:** The review highlighted the need to develop contextualized, culturally adapted, and evidence-based programs, in addition to strengthening Latin American research, generating validated instruments in Spanish, and promoting public cybersecurity policies that explicitly include older adults.

Keywords: Cybersecurity; older adults; digital literacy; awareness; phishing.

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Introducción

Un poco más de diez años, los adultos mayores han pasado a ser un grupo significativo de personas que usan Internet. La Unión Internacional de Telecomunicaciones informó que el acceso de las personas mayores de 60 años se duplicó entre 2012 y 2022, alcanzando más del 45 % en zonas de ingresos medios y altos [1]. La pandemia de la COVID-19 aceleró esta tendencia, ya que la telemedicina y las videollamadas se convirtieron en algo esencial para muchos. Sin embargo, esta rápida adopción no incluyó formación en ciberseguridad, lo que dejó a las personas mayores en una situación de vulnerabilidad, ya que siguen utilizando criterios obsoletos para evaluar la confianza en Internet, lo que puede acarrear riesgos.

Los ciberdelincuentes lo saben y se aprovechan constantemente de ello. Según el FBI, las personas mayores de 60 años en Estados Unidos denunciaron pérdidas por valor de más de 3.1 mil millones de dólares a causa de delitos cibernéticos en 2022, más que cualquier otro grupo de edad [2]. La Organización de los Estados Americanos señaló que la falta de educación en ciberseguridad para las personas mayores constituye una laguna significativa en las políticas públicas de América Latina [3].

En respuesta a este problema, diversas instituciones han desarrollado programas de sensibilización y formación en ciberseguridad dirigidos a esta población [4], [5], [6]. El inconveniente es que estos programas varían considerablemente en cuanto a su diseño, marcos teóricos y contextos de implementación, lo que dificulta determinar cuáles funcionan y por qué [7], [8]. A esto se suma que los ámbitos de la ciberseguridad, la gerontología y las ciencias de la educación rara vez mantienen un diálogo estructurado y continuo entre sí.

Dado este contexto, esta investigación busca examinar los programas de concientización y formación en ciberseguridad dirigidos a personas mayores. El objetivo es identificar cómo están diseñados, en qué se basan teóricamente y cuán efectivos son frente al aumento del riesgo cibernético que enfrenta este grupo.

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Revisión de la literatura

La relación entre ciberseguridad y envejecimiento digital ha sido abordada desde distintos ángulos, aunque los primeros estudios surgieron de forma poco articulada en la primera mitad del 2010 y el campo se consolidó a partir de 2020. El trabajo acumulado hasta hoy puede agruparse en tres líneas principales.

Vulnerabilidad digital de los adultos mayores

La primera línea de investigación se ha dedicado a entender por qué los adultos mayores son víctimas de los fraudes digitales y qué factores lo explican. Lo que esta literatura deja claro es que no se trata simplemente de personas con falta de manejo tecnológico: El envejecimiento trae consigo una menor velocidad de procesamiento y una tendencia más marcada a tomar la información al pie de la letra; a eso se suman condiciones sociales como el aislamiento o la dependencia de terceros para manejar dispositivos. Sarno et al. [9] evidenciaron, a través de estudios experimentales, que los adultos mayores presentan mayores problemas para reconocer correos electrónicos de phishing en comparación con personas jóvenes. Posteriormente, [10] interpretaron este fenómeno desde la Fuzzy Trace Theory, señalando que los adultos mayores suelen basarse más en interpretaciones generales de la información que en detalles específicos al momento de tomar decisiones.

Investigaciones nuevas han indagado en esta problemática. [11] indicaron que muchos delincuentes informáticos escogen premeditadamente a los adultos mayores como víctimas, aprovechando factores asociados a la vejez, a causa de la confianza en personas que aparentan tener autoridad, el aislamiento social y la menor tendencia a denunciar los fraudes. Por otra parte, [12] destacaron un aspecto poco considerado en las políticas de ciberseguridad: las consecuencias emocionales y psicológicas que deja la victimización, entre ellas ansiedad, depresión y pérdida de confianza. En una línea similar, [13] hallaron que la vulnerabilidad no es uniforme entre grupos de edad, sino que varía según el tipo específico de conducta de ciberseguridad analizada.

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Alfabetización digital, autoeficacia y comportamiento protector

La segunda línea de investigación explora qué factores median entre saber sobre riesgos digitales y actuar de forma segura En este sentido, la autoeficacia en ciberseguridad juega un papel central: no es suficiente conocer amenazas como el phishing, también es necesario sentirse capaz de reconocerlas y actuar de manera adecuada. [14] concluyeron que esta confianza en las propias capacidades influye más en las conductas de protección que la experiencia tecnológica previa. [15] también afirmaron que, según el Health Belief Model, la percepción de ser víctima de un ataque digital promueve la implementación de acciones preventivas.

Por otro lado, las investigaciones demuestran que un exceso de confianza puede constituir un riesgo considerable. [16] comprobaron que algunos longevos sobreestimaban sus destrezas y a pesar de contar con nociones de ciberseguridad, no siempre prestaban atención a ciertos riesgos particulares. Además, [17] concluyeron que una preocupación desmedida por el fraude no a menudo promueve conductas preventivas, sino que en algunos casos genera rechazo o miedo hacia el uso de internet, limitando de este modo la autonomía y la participación social de los ancianos. Un estudio fenomenológico [18] con adultos mayores en India identificó que la percepción del riesgo, las reacciones emocionales ante él y el apoyo familiar influyen directamente en la adopción de conductas seguras en línea.

Programas educativos y enfoques de concienciación

Diversas investigaciones se dedicaron a examinar la efectividad de programas e intervenciones particulares. En este sentido, revisiones como las de [19] y [7] coinciden en que las estrategias fundamentadas únicamente en la teoría tienen efectos limitados. En cambio, las actividades prácticas, interactivas y ajustadas a las necesidades de los usuarios presentan resultados más efectivos y duraderos. Sin embargo, muchos de estos estudios demandan un seguimiento prolongado y se realizaron en países anglosajones o asiáticos.

En el plano teórico, los modelos OSICSAM [4] y SCSAM-Elderly [20] ofrecen los marcos más completos para comprender la concienciación acerca de la ciberseguridad en los adultos mayores. Ambos trabajan desde una lógica de múltiples niveles: individual,

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

social e institucional, con resultados alentadores, aunque su validación ha sido comprobada en Malasia.

Metodología

Tipo de revisión y protocolo. Se realizó una revisión sistemática de la literatura (RSL) siguiendo las directrices de la declaración PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Este protocolo permite establecer criterios transparentes para la identificación, selección, evaluación y síntesis de estudios científicos, reduciendo posibles sesgos durante el proceso de revisión [21].

La revisión tuvo como finalidad analizar la evidencia disponible sobre la concienciación, educación y entrenamiento en ciberseguridad dirigidos a adultos mayores, considerando tanto los factores asociados a su vulnerabilidad digital como las características de las intervenciones educativas desarrolladas para fortalecer sus competencias de seguridad en línea.

La búsqueda consideró publicaciones realizadas entre 2015 y 2026. Aunque se estableció este periodo como criterio de búsqueda, los estudios finalmente incluidos en la revisión correspondieron al periodo comprendido entre 2016 y 2026.

Marco PICOC y preguntas de investigación. Para delimitar el alcance de la revisión, se utilizó el marco PICOC (Population, Intervention, Comparison, Outcome, Context), una estructura empleada para definir los elementos centrales de una revisión sistemática. La Tabla 1 presenta los componentes considerados.

Tabla 1

Marco PICOC

Componente	Descripción
Población	Adultos mayores (≥60 años): older adults, elderly, seniors, aging population
Intervención	Programas de alfabetización digital, educación en ciberseguridad, entrenamiento en seguridad en línea, formación en habilidades digitales y TIC.
Comparación	Adultos mayores con baja alfabetización digital, personas sin formación en ciberseguridad, grupos sin intervención educativa, adultos jóvenes
Resultado	Reducción de riesgos digitales, adopción de comportamientos seguros, mayor confianza digital, prevención del fraude, mejora de competencias digitales, concienciación en ciberseguridad.

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Contexto	Entorno digital, uso de internet, redes sociales, banca en línea, TIC, dispositivos móviles

Usando el marco PICOC, se crearon seis preguntas de investigación (Tabla 2). Estas preguntas buscan identificar los principales riesgos digitales, los factores que influyen en un comportamiento seguro, las características de los programas educativos, los modelos teóricos utilizados y las brechas en el área de estudio.

Tabla 2

Preguntas de investigación

RQ	Pregunta de investigación
RQ1	¿Cuáles son los principales riesgos y amenazas cibernéticas que afectan a los adultos mayores, y qué factores cognitivos, individuales y contextuales explican su mayor vulnerabilidad?
RQ2	¿En qué medida la alfabetización digital y la autoeficacia tecnológica se asocian con la adopción de comportamientos seguros en línea?
RQ3	¿Qué características metodológicas y pedagógicas tienen los programas de educación en ciberseguridad para adultos mayores, y qué evidencia existe sobre su efectividad?
RQ4	¿Qué barreras y facilitadores cognitivos, emocionales, sociales, tecnológicos e institucionales condicionan la participación en programas de ciberseguridad?
RQ5	¿Qué marcos teóricos y modelos de concienciación han sido aplicados a los adultos mayores, y qué validación empírica tienen?
RQ6	¿Qué vacíos de investigación existen en ciberseguridad para adultos mayores, especialmente en contextos no anglosajones?

Estrategia de búsqueda. La búsqueda bibliográfica se realizó en dos bases de datos internacionales: Scopus y Web of Science, seleccionadas por su cobertura científica y relevancia en áreas relacionadas con informática, ciencias sociales, educación y comportamiento humano.

La estrategia de búsqueda se diseñó a partir de tres bloques temáticos relacionados con el objetivo de investigación: (B1) Ciberseguridad, (B2) población adulta mayor y (B3) intervención educativa o concienciación. Los términos dentro de cada bloque se combinaron mediante el operador booleano OR, mientras que los bloques temáticos se relacionaron mediante el operador AND. Asimismo, se empleó el símbolo (*) como truncador para recuperar variaciones de los términos utilizados.

La ecuación de búsqueda se adaptó a las características de cada base de datos y aplicada en los campos de título, resumen y palabras clave. Los términos empleados para cada bloque se presentan en la Tabla 3.

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Tabla 3

Cadena de búsqueda por bloques

Bloque	Términos de búsqueda
B1 Ciberseguridad	"cybersecurity" OR "cyber security" OR "information security" OR "online safety" OR "internet safety" OR "digital security" OR "cyber hygiene" OR "phishing awareness"
B2 Población	"older adult*" OR "elderly" OR "senior*" OR "older people" OR "aging population" OR "ageing population" OR "aged people" OR "older user*"
B3 Intervención	"awareness" OR "education" OR "training" OR "digital literacy" OR "digital competence" OR "program*" OR "intervention" OR "digital skills"

La búsqueda permitió identificar inicialmente 282 registros. Los resultados obtenidos fueron posteriormente procesados para la eliminación de duplicados y la aplicación de los criterios de selección establecidos.

Criterios de selección. Los estudios se seleccionaron mediante criterios de inclusión y exclusión definidos previamente, con el propósito de garantizar la pertinencia temática y calidad metodológica de la evidencia analizada (Tabla 4).

Se incluyeron investigaciones publicadas entre 2015 y 2026, en inglés, español o chino, con resumen disponible en inglés, publicadas en revistas científicas o memorias de congresos académicos revisados por pares. Además, los estudios debían abordar la ciberseguridad, alfabetización digital, riesgos digitales, fraude, phishing o programas de concienciación dirigidos a adultos mayores.

Para mantener coherencia con el objetivo de investigación, se consideraron estudios enfocados en adultos mayores definidos como personas de 60 años o más. Los estudios que incluyeran rangos de edad amplios se consideraron únicamente cuando presentaban resultados diferenciados para esta población.

Se excluyeron artículos de opinión, editoriales, literatura sin revisión por pares, investigaciones centradas exclusivamente en estudiantes o jóvenes, estudios de ciberseguridad técnica u organizacional sin relación con usuarios adultos mayores, así como trabajos que no abordaran la dimensión educativa o conductual de la seguridad digital.

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Tabla 4

Criterios de selección

Criterios de inclusión	Criterios de exclusión
Artículos publicados en inglés, español o chino que incluyan resumen en inglés.	Se excluyen artículos de opinión, editoriales y literatura que no cuente con revisión por pares.
Publicaciones indexadas en revistas científicas o memorias de conferencias académicas.	Estudios que no presenten una diferenciación etaria explícita.
Investigaciones enfocadas en adultos mayores (≥55 años) como población principal de estudio.	Trabajo centrado en estudiantes, jóvenes o población universitaria.
Estudios relacionados con riesgos digitales, fraude, phishing, alfabetización digital o concienciación en ciberseguridad.	Investigación de ciberseguridad técnica u organizacional sin énfasis en usuarios adultos mayores.
Publicaciones realizadas entre 2015 y 2026.	Estudios que pretendan al área de salud o medicina que no aborden la ciberseguridad educativa como tema principal, así como artículos retractados.

Proceso de selección: protocolo PRISMA 2020. El proceso de selección siguió las cuatro fases establecidas por PRISMA 2020: identificación, cribado, elegibilidad e inclusión.

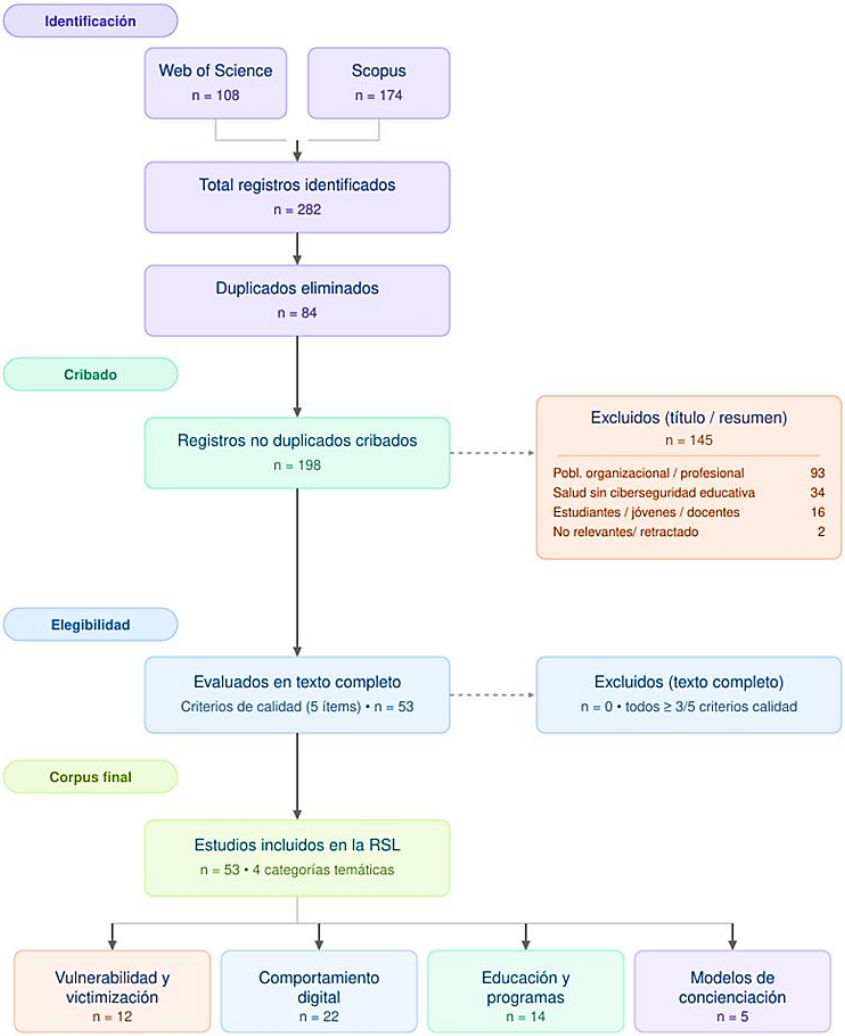
En la fase inicial se identificaron 282 registros procedentes de las bases de datos seleccionadas. Posteriormente, se eliminaron 84 registros duplicados. Los documentos restantes se evaluaron mediante la revisión de títulos y resúmenes, descartando aquellos que no cumplían con los criterios establecidos. Finalmente, se llevó a cabo la evaluación del texto completo de los estudios potencialmente relevantes.

Como resultado del proceso de selección, se obtuvo un corpus final de 53 estudios, los cuales se incluyeron para la síntesis narrativa. El proceso completo se presenta en la Figura 1 mediante el diagrama de flujo PRISMA 2020.

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Figura 1

Diagrama de flujo PRISMA 2020



Evaluación de calidad. Los estudios incluidos se evaluaron mediante criterios de calidad metodológica basados en las listas de evaluación crítica del Joanna Briggs Institute (JBI), seleccionadas de acuerdo con las características metodológicas de los estudios analizados.

Para facilitar la comparación entre investigaciones con diferentes diseños, la evaluación consideró cinco aspectos comunes: (C1) Claridad del objetivo del estudio; (C2) definición de la población analizada; (C3) adecuación del diseño metodológico; (C4) presentación de resultados sustentados en evidencia; (C5) coherencia entre resultados y conclusiones.

Los estudios que alcanzaron un puntaje igual o superior a 3 de 5 criterios se consideraron adecuados para la síntesis final. De los 53 estudios incluidos, 46 alcanzaron una valoración alta (5/5) y 7 una valoración media-alta (4/5).

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Extracción y síntesis de datos

Para la extracción de información se diseñó una matriz de análisis que recopiló las siguientes variables: autores, año de publicación, base de datos, país, diseño metodológico, población, muestra, instrumentos empleados, marcos teóricos, tipo de intervención, principales hallazgos y relación con las preguntas de investigación.

El análisis de la información se realizó mediante una síntesis narrativa, organizando los resultados en categorías temáticas relacionadas con las preguntas de investigación. Estas categorías permitieron analizar la vulnerabilidad digital de los adultos mayores, los factores asociados al comportamiento seguro, las características de las intervenciones educativas, las barreras de implementación, los modelos teóricos utilizados y las principales brechas de investigación.

Resultados

Visión general del corpus

El corpus quedó conformado por 53 investigaciones publicadas entre 2016 y 2026. El 85 % de ellos (n=45) se publicaron entre 2021–2026, lo que evidencia el interés de investigación que despertó la pandemia de COVID-19 en torno a la seguridad digital de adultos mayores. La cobertura entre bases de datos se equilibra: Scopus aportó 28 estudios y Web of Science 25. El enfoque cuantitativo fue el más recurrente (53 %), incluyendo encuestas y modelos de ecuaciones estructurales, mientras que los diseños mixtos representaron el 21 %, los cualitativos el 15 % y las revisiones teóricas el 11 %. La Tabla 5 desglosa la distribución por categoría temática y período.

Tabla 5

Distribución del corpus por categoría y período (n=53)

Categoría temática	2016–2019	2020–2022	2023–2024	2025–2026
Vulnerabilidad y victimización (n=12)	3	3	1	5
Comportamiento digital (n=22)	2	4	4	12
Educación y programas (n=14)	2	2	2	8
Modelos de concienciación (n=5)	0	1	1	3
TOTAL	**7**	**10**	**8**	**28**

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Distribución geográfica

El corpus se centra en Asia y en el mundo anglosajón. En Asia, el 28% de los datos provienen de países como Malasia, China, Tailandia e India. En cuanto al mundo anglosajón, los Estados Unidos aportan el 17% de los datos, mientras que Europa contribuye con el 24%. Los estudios internacionales o multinacionales suman el 15 %. El dato más significativo para el campo: América Latina no tiene representación, ni un solo estudio primario. Los únicos trabajos en contexto hispanohablante son dos de España [22], [23], que abordan una realidad muy diferente a la latinoamericana.

Hallazgos por pregunta de investigación

Riesgos y amenazas cibernéticas (RQ1)

Las amenazas más documentadas en el corpus son el phishing, el fraude en línea, el robo de identidad y la ingeniería social. Lo que distingue a la literatura más reciente no es la naturaleza de esas amenazas, conocida desde hace años, sino la descripción de cómo los atacantes las adaptan específicamente a los adultos mayores. [11] analizaron comunidades del foro Dread en la darknet y encontraron que los delincuentes seleccionan a sus víctimas a partir de rasgos concretos: mayor confianza en figuras de autoridad, aislamiento social y baja probabilidad de denuncia. La vergüenza y el desconocimiento de los canales de denuncia son, de hecho, tan importantes para la cifra negra del cibercrimen contra mayores como la propia efectividad del ataque [24].

Cognitivamente, los longevos tienen dificultades a la hora de reconocer fraudes digitales. [9] descubrieron que, a diferencia de los jóvenes, los adultos mayores tienen más dificultades para reconocer los correos electrónicos de phishing, especialmente si el contenido parecía provenir de una organización conocida y confiable. Según [10], se puede entender a través de la Fuzzy Trace Theory: a medida que las personas envejecen, sus cerebros tienden a procesar la información de forma más literal y cuidadosa, lo que, irónicamente, hace que sea más difícil detectar amenazas ocultas en mensajes phishing. Este enfoque detallado, a diferencia de un enfoque que se centra en el significado general del mensaje, facilita la comprensión intuitiva y facilita la identificación de contradicciones. [25], [26] amplían esta perspectiva utilizando la ingeniería social: los

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

ancianos aplican al mundo digital los mismos estándares de confianza que les han sido útiles a lo largo de su vida, creando áreas de vulnerabilidad que los estafadores saben reconocer y aprovechar. Entre los últimos descubrimientos más recientes, hay uno que merece especial mención. [17] llegaron a una conclusión inesperada: el temor al fraude no conduce a que los adultos mayores tomen precauciones, sino que provoca un efecto contrario. Muchos eligen simplemente desconectarse de internet para evitar cualquier peligro, una actitud que, aunque lógica, acaba perjudicando su autonomía y su calidad de vida. Por otro lado, [12] documentaron metódicamente las consecuencias emocionales y mentales de las víctimas de estos delitos, incluyendo ansiedad, depresión y estrés postraumático, que muchas veces están fuera del alcance de las políticas públicas de atención y respuesta.

Alfabetización digital y autoeficacia (RQ2)

Una creencia común en el desarrollo de software es que las personas que navegan más en internet estarán más dispuestas a protegerse. Sin embargo, [27] indican lo contrario: el tiempo que una persona pasa conectada no determina si será víctima de un delito digital. El factor determinante es el grado de conocimiento específico sobre seguridad en línea, el cual puede ser sorprendentemente corto incluso en personas que usan la tecnología a diario.

La autoeficacia destaca como la variable más determinante. Esta se entiende como la convicción propia de actuar con seguridad en entornos digitales. [14] encontraron que esta creencia anuncia los procedimientos de protección con mayor solidez que la experiencia tecnológica acumulada a lo largo del tiempo. [28] extiende una conclusión al sector financiero: los adultos mayores con mayor confianza en sus habilidades digitales tienen más probabilidad de utilizar la banca en línea, y gestionar trámites gubernamentales digitalmente. En banca digital específicamente, la edad y el nivel educativo condicionan de forma directa las prácticas de ciberseguridad de los usuarios mayores [29]. Sin embargo, esa certeza también puede convertirse en un peligro potencial. [30] distinguen entre la confianza racional y establecida, que promueve una situación segura, y la confianza excesiva, que puede poner a la persona en riesgo. En esta dirección, [16] hallaron que muchos adultos mayores tienden a sobreestimar sus

ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

conocimientos sobre seguridad digital mientras subestiman los riesgos reales que afrontan. Pensar que se tiene todo controlado puede ser tan peligroso como ignorar por completo el problema. Desde un aspecto diferente, [15] proponen un enfoque complementario basado en el modelo de creencias en salud: sentirse personalmente vulnerable ante una amenaza específica es importante para adoptar conductas de prevención. No basta con informar a las personas sobre las acciones que deben tomar; es importante que entiendan y acepten que este riesgo puede afectarles directamente. Finalmente, [31] destaca una variable que está empezando a ganar importancia: la dependencia excesiva de los teléfonos celulares se asocia con una capacidad reducida para evaluar críticamente situaciones de riesgo digital, lo que plantea nuevas preguntas sobre hasta qué punto el uso diario de la tecnología afecta la atención y la prudencia ante posibles amenazas.

Diseño y efectividad de intervenciones educativas (RQ3)

Las metodologías tradicionales como folletos, charlas y campañas masivas tienen un impacto limitado en la transformación del comportamiento a largo plazo [32]. Los métodos efectivos son aquellos que sitúan a los individuos como actores de su propio aprendizaje, los conectan con experiencias definidas que se adaptan a sus situaciones específicas. La experiencia acumulada por proyectos europeos de alfabetización digital dirigidos a personas mayores confirma la importancia de este enfoque práctico y situado [33]. En este sentido, [6] presentaron SmartICST, un sistema de aprendizaje adaptativo que combina principios de andragogía, diseño universal e inteligencia artificial, mostrando resultados iniciales prometedores en la comprensión y satisfacción de los participantes. Por otro lado, [34] demostraron que los mensajes que apelan al miedo pueden ser efectivos, pero solo si se les proporcionan directrices claras sobre afrontar la amenaza identificada. Sin una solución concreta, el miedo tiende a llevar a la parálisis en lugar de alentar la acción. Esto se fundamenta en el modelo de proceso paralelo extendido (Extended Parallel Process Model) y tiene implicaciones directas en el diseño de campañas de concientización sobre seguridad digital. El aprendizaje entre generaciones funciona de manera diferente a la enseñanza tradicional. [35] encontraron que pedir ayuda de una persona más joven en un programa estructurado reducía la ansiedad tecnológica y mejoraba las habilidades de manera más sostenida que el aprendizaje autónomo. El

ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

componente relacional, transferencia de confianza entre generaciones, parece ser tanto o más importante que el contenido técnico.

La medición sigue siendo un déficit importante del campo. [23] avanzaron con una escala basada en el marco DigComp validada en contexto hispanohablante. [36] diseñaron la escala DIQ adaptada al contexto tailandés. Tanto este instrumento como otros similares permiten realizar comparaciones antes y después de las intervenciones; sin embargo, se necesitan más herramientas de este tipo en distintos idiomas. [37] incorpora un diseño frecuente ignorado: en WeChat, la coherencia entre la fuente del mensaje y su formato incrementa significativamente la intención de los adultos mayores chinos de adoptar conocimientos de ciberseguridad, evidenciando que el canal de comunicación y la credibilidad de la fuente son tan importantes como el contenido de este.

Barreras y facilitadores de implementación (RQ4)

Lo que los estudios han encontrado es que el mayor obstáculo para aprender tecnología no tiene que ver con la inteligencia de las personas, sino con cómo se sienten frente a ella. [7] mostraron que el miedo a cometer errores, la sensación de no ser suficiente o la desconfianza hacia lo digital pueden bloquear a alguien incluso antes de que empiece a intentarlo. En otras palabras, un programa de formación que ignora las barreras emocionales desde el principio tiene pocas posibilidades de éxito, sin importar cuán capaz sea el alumno.

[8] ofrecen otra perspectiva diferente: navegar por internet no se limita a la capacidad de utilizar tecnologías, sino que también incluye el acceso a recursos, una sensación de confianza y recibir apoyo de otros. En América Latina, donde son muchas las personas que tienen dificultades económicas, los desafíos materiales de habilidades digitales no pueden verse como problemas aislados, son manifestaciones de desigualdades estructurales. Por lo tanto, las decisiones tomadas sin coordinación y apoyo institucional son inútiles para lograr un cambio duradero.

En la misma línea, [38] señalaron que la continuidad del aprendizaje depende más de cómo se percibe la utilidad práctica del contenido que de su calidad, así como de la falta de exigencias abrumadoras. Asimismo, [39] indican que las formas de aprendizaje de

ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

cada persona están influenciadas por su situación económica, educación y su ubicación geográfica, por lo que es difícil encontrar una solución que sea universalmente aplicable.

Un tema que la investigación reciente ha comenzado a abordar reconoce, aunque todavía no ha recibido suficiente atención en las políticas públicas, el papel de los trabajadores asistenciales. [40] evidencian que los cuidadores de adultos mayores con discapacidades intelectuales asumen la responsabilidad de proteger a estas personas en el entorno digital, a pesar de no haber recibido capacitación específica para ello. La pandemia exacerbó esta situación: [41] documentaron que el confinamiento llevo al uso de dispositivos y plataformas sin la supervisión adecuada para manejarlo.

En este contexto, iniciativas como el modelo [4] o el [20] sugieren intervenciones que miran más allá del individuo para incluir su red de apoyo y el contexto institucional en el que está inserto; los resultados demuestran que este enfoque sistémico es mucho más eficaz que el sistema centrado exclusivamente en el individuo. [42], en una revisión sistemática de 62 estudios, encontraron que valorar las tecnologías del pasado, la preocupación por la privacidad y la seguridad, la ansiedad, el deterioro cognitivo, la motivación y la confianza son las principales barreras que enfrentan los adultos mayores al interactuar con servicios digitales gubernamentales. Incluso en población con mayor riesgo de demencia, las intervenciones educativas han mostrado mejoras significativas en la capacidad de detectar riesgos digitales [43].

Marcos teóricos y modelos de concienciación (RQ5)

El corpus muestra una considerable diversidad teórica y los enfoques a menudo son inconsistentes entre sí, como suele ocurrir en el campo que aún está en desarrollo.

En términos de procesos cognitivos, la Teoría del Fuzzy Trace, estudiada por [10] y [9], explica por qué los adultos mayores son más susceptibles al phishing: no se trata de desatención, sino de la manera en que procesan la información según el tipo de mensaje que reciben. Desde una perspectiva más centrada en la motivación, el Modelo de Creencias en Salud se establece como el marco más frecuentemente empleado en este campo [15], [17], y esto no es fortuito: permite establecer una conexión bastante directa

ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

entre la percepción que una persona tiene del riesgo y la amenaza en una situación, y su disposición real para llevar a cabo acciones preventivas.

En el área del diseño de mensajes y comunicación, el modelo de proceso paralelo extendido, utilizado por [34], propone una distinción que es particularmente útil para la aplicación práctica: existe una clara distinción entre las personas que responden ante una amenaza queriendo protegerse de inmediato y aquellos que, de otro modo, ignoran el problema para reducir la ansiedad. Esta distinción es relevante cuando se trata de crear intervenciones. En este mismo sentido, [44] se apoyaron en la Teoría de Motivación de Protección para investigar cómo la percepción de amenaza afecta la decisión de los adultos mayores de adoptar o no el uso del smartphone en su vida diaria.

Finalmente, cabe mencionar dos modelos diseñados específicamente para esta población: el [4] y el [20]. Ambos organizan sus variables en varios niveles: individual, social e institucional, y muestran resultados alentadores, aunque su principal debilidad radica en que únicamente han sido probados en el contexto malayo. El propio [5] reconocen esta limitación y plantean la necesidad de marcos más integrales que se verifiquen en distintos contextos culturales y geográficos. A esto se suma el hallazgo de [19], quien señala que las aplicaciones de seguridad móvil no han sido desarrolladas teniendo en cuenta a los usuarios mayores, y que esa brecha de diseño no puede resolverse únicamente a través de la formación. Como alternativa desde el ámbito técnico, [45] propuso un sistema de monitoreo de ciberseguridad instalado en el hogar, orientado a personas mayores que viven sin acompañamiento.

Vacíos de investigación y brechas geográficas (RQ6)

Una de las ausencias más notorias en esta literatura es la geográfica: América Latina prácticamente no existe en estos estudios. No hace falta profundizar demasiado para comprobarlo; basta con mirar de dónde vienen las investigaciones revisadas. En el ámbito hispanohablante, apenas se localizan dos trabajos, ambos desarrollados en España, un país cuya realidad educativa y social tiene poco que ver con lo que sucede en esta región. Algunos investigadores, como [39] y [46], coinciden en que el entorno cultural y económico de una comunidad juega un papel crucial en la efectividad de cualquier intervención. Una habilidad que funcione bien en Finlandia puede no ser apropiada

ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

cuando se aplica en el Ecuador rural o en zonas populares de Lima, porque transferir decisiones entre diferentes contextos sin adaptar significa desestimar las realidades materiales y simbólicas que caracterizan la vida cotidiana de las personas.

Además, existen límites de tiempo: la mayoría de los estudios existentes solo analizan los resultados. Los efectos inmediatos de la intervención, sin considerar lo que sucederá en el mediano plazo. Aún no hay pruebas concluyentes sobre si las habilidades adquiridas se mantienen seis meses o un año después del final de la intervención [25], [12]. Sin un seguimiento adecuado en el tiempo, cualquier estrategia de ciberseguridad basada en estos resultados se basa en supuestos que no han demostrado ser viables.

A estas limitaciones se les suma un vacío metodológico: no existen herramientas validadas en español para evaluar las competencias de ciberseguridad en los adultos mayores. Aunque la escala creada por [23] representa un avance, su capacidad se limita para reflejar la variedad de realidades presentes en América Latina. Como señalan [5], el problema principal va más allá de las herramientas: los marcos teóricos existentes se han desarrollado y probado en contextos culturales específicos. Esto requiere desarrollar modelos más adecuados y probarlos previamente en diferentes entornos antes de intentar aplicar sus resultados de forma general.

Discusión

Hay tres aspectos del análisis que merecen especial atención. El primero está relacionado con un aspecto previo a cualquier tipo de programa o herramienta: el estado emocional del alumno. Muchos adultos mayores desconfían de la tecnología, y si esto no se aborda desde el principio, todo lo demás es inútil. Los programas que ignoran este malestar o no tienen en cuenta la resistencia provocada por el cambio suelen tener poco éxito [7]. Es fundamental generar confianza antes de transferir conocimientos. En esta línea, [47] plantean que los objetivos de aprendizaje de los programas de educación digital para personas mayores deben redefinirse para responder a sus necesidades específicas, en lugar de replicar los diseñados para poblaciones más jóvenes. Asimismo, los resultados de esta revisión refuerzan la necesidad de considerar las diferencias generacionales en los conocimientos, percepciones y prácticas de seguridad digital al diseñar estrategias

educativas dirigidas a esta población, ya que estos factores condicionan la adopción de comportamientos seguros y la efectividad de las intervenciones [48]. Estudios recientes refuerzan esta evidencia al demostrar que las dificultades cognitivas para discriminar correos electrónicos seguros de los maliciosos son significativamente mayores en edades avanzadas [49], mientras que factores psicosociales como la soledad o la menor reserva cognitiva amplifican la vulnerabilidad a estafas financieras [50].

En segundo lugar, el entorno del individuo no es un detalle menor, sino un factor que debe influir en el diseño desde el principio. La manera en la que una persona aprende, los dispositivos disponibles para ella, el apoyo que dispone y la relevancia que le otorga al contenido varían considerablemente en función de su situación económica, su cultura y el lugar en el que reside [39], [8]. Un programa que funciona bien en una ciudad con ingresos medios o altos puede resultar inaccesible o directamente irrelevante en una zona rural de América Latina. Investigaciones en contextos nórdicos, como las entrevistas realizadas a adultos mayores suecos, subrayan que la formación en ciberseguridad debe abordar simultáneamente la exclusión digital y los miedos asociados para ser efectiva [51], mientras que las revisiones sistemáticas sobre percepciones de privacidad confirman que estas varían sustancialmente según el entorno sociotécnico del usuario [52].

La tercera es de carácter institucional: quienes cuidan a los adultos mayores y quienes conforman sus redes de apoyo informal cumplen, en la práctica, un papel relevante en la protección de su seguridad digital, por lo que requieren capacitación especializada. Excluirlos de los programas de intervención equivale a desaprovechar uno de los canales más eficientes y de fácil acceso para implementar acciones preventivas [40], [41]. En esta línea, iniciativas que promueven la formación de “guardianes digitales” en comunidades de mayores han demostrado ser un mecanismo eficaz para extender la protección más allá del individuo [53], al mismo tiempo que la incorporación de una perspectiva generacional permite que los adultos mayores se apropien de su identidad digital con mayor seguridad y autonomía [54].

Revista Ingenio Global
ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

Conclusiones

Esta revisión sistemática de la literatura se basó en 53 estudios publicados entre 2016 y 2026, obteniendo cuatro conclusiones significativas.

Los adultos mayores presentan una vulnerabilidad en el mundo digital, esta vulnerabilidad no solo se debe a los cambios cognitivos que vienen con la edad, sino que también está influenciada por factores generacionales, educativos y contextuales. Por ejemplo, la forma en que las personas mayores transfieren su confianza del mundo analógico al digital, su falta de conocimientos específicos en ciberseguridad y su aislamiento social son factores clave.

Las intervenciones que funcionan mejor tienen tres características: son activas y experienciales, incluyen acompañamiento personalizado o intergeneracional, y se adaptan a la cultural y tecnología del usuario. Los programas genéricos o de una sola sesión no tienen un impacto significativo. Los modelos multinivel OSICSAM y SCSAM-Elderly son más efectivos que los enfoques que solo se conectan en el individuo.

La falta de investigación en América Latina. Las situaciones socioeconómicas, los patrones culturales en esta región son muy diferentes a los de otros lugares donde se han realizados estudios. Es fundamental desarrollar investigación propia en la región; es necesaria para diseñar políticas y programas que funcionen en este entorno.

Este campo necesita mejorar en dos áreas técnicas importantes: estudios a largo plazo que evalúen cómo cambian los comportamientos con el tiempo, y herramientas de medición estandarizadas que permitan comparar diferentes programas. Sin esta información, las decisiones sobre políticas públicas seguirán basándose en evidencia que no es relevante o transferible para el contexto local.

Referencias

[1] International Telecommunication Union (ITU), "Measuring digital development: Facts and Figures 2022," ITU, Geneva, Switzerland, 2022. [Online]. Available: https://www.itu.int/itu-d/reports/statistics/facts-figures-2022/

[2] Internet Crime Complaint Center (IC3), "2022 IC3 Elder Fraud Report," Federal Bureau of Investigation, Washington, DC, USA, 2022. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf

[3] Inter-American Development Bank and Organization of American States, "Cybersecurity: Risks, Progress, and the Way Forward in Latin America and the Caribbean," IDB/OAS, 2020, doi: 10.18235/0002513.

[4] A. G. Buja, S. D. M. Wahid, T. F. A. Rahman, N. A. Deraman, M. N. H. H. Jono, and A. A. Aziz, "Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly," *Int. J. Adv. Technol. Eng. Explor.*, vol. 8, no. 76, pp. 511–519, 2021, doi: 10.19101/IJATEE.2020.762185.

[5] N. A. Azam, A. G. Buja, N. M. Sahri, R. Ahmad, N. F. Habidin, S. F. Abdul Latip, M. Y. Darus, M. S. Hussin, and S. Saat, "A light review on cyber security awareness models for the elderly," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 44, no. 1, pp. 31–45, 2025, doi: 10.37934/araset.44.1.3145.

[6] D. Fujs, S. Vrhovec, T. Hovelja, and D. Vavpotič, "SmartICST: A smart information and cyber security training approach for older adults," *Educ. Inf. Technol.*, vol. 30, no. 14, pp. 19911–19932, 2025, doi: 10.1007/s10639-025-13564-y.

[7] B. Morrison, L. Coventry, and P. Briggs, "How do older adults feel about engaging with cyber-security?," *Hum. Behav. Emerg. Technol.*, vol. 3, no. 5, pp. 1033–1049, 2021, doi: 10.1002/hbe2.291.

[8] E. M. Glowacki, Y. Zhu, J. M. Bernhardt, and K. Magsamen-Conrad, "Technological capital within aging United States-based populations: Challenges and recommendations for online intervention uptake," *J. Appl. Commun. Res.*, vol. 49, no. 3, pp. 347–367, 2021, doi: 10.1080/00909882.2021.1885051.

[9] D. M. Sarno, J. E. Lewis, C. J. Bohil, and M. B. Neider, "Which phish is on the hook? Phishing vulnerability for older versus younger adults," *Hum. Factors*, vol. 62, no. 5, pp. 704–717, 2020, doi: 10.1177/0018720819855570.

[10] C. White, M. Gummerum, S. Wood, and Y. Hanoch, "Internet safety and the silver surfer: The relationship between gist reasoning and adults' risky online behavior," *J. Behav. Decis. Mak.*, vol. 30, no. 4, pp. 819–827, 2017, doi: 10.1002/bdm.2003.

[11] K. Logie and S. Das, "Lessons learned from Dread darknet communities: How and why are fraudsters targeting the elderly to be victims or accomplices?," *Criminol. Public Policy*, vol. 24, no. 2, pp. 237–271, 2025, doi: 10.1111/1745-9133.12684.

[12] R. Gautam and S. Yadav, "Psychological impact of cyber-crime on victims," *Curr. Psychol.*, vol. 45, art. 240, 2026, doi: 10.1007/s12144-025-08873-x.

[13] D. Branley-Bell, L. Coventry, M. Dixon, A. Joinson, and P. Briggs, "Exploring age and gender differences in ICT cybersecurity behaviour," *Hum. Behav. Emerg. Technol.*, vol. 2022, art. 2693080, 2022, doi: 10.1155/2022/2693080.

[14] C. Blackwood-Brown, Y. Levy, and J. D'Arcy, "Cybersecurity awareness and skills of senior citizens: A motivation perspective," *J. Comput. Inf. Syst.*, vol. 61, no. 3, pp. 195–206, 2021, doi: 10.1080/08874417.2019.1579076.

[15] M. Dodel and G. Mesch, "Cyber-victimization preventive behavior: A health belief model approach," *Comput. Hum. Behav.*, vol. 68, pp. 359–367, 2017, doi: 10.1016/j.chb.2016.11.044.

[16] M. Kyytsönen, J. Ikonen, A.-M. Aalto, and T. Vehko, "The self-assessed information security skills of the Finnish population: A regression analysis," *Comput. Secur.*, vol. 118, art. 102732, 2022, doi: 10.1016/j.cose.2022.102732.

[17] S. Kemp, E. Sitges Maciá, and N. Erades-Pérez, "Worry about online fraud and older adults: Avoidant and protective responses," *J. Criminol.*, 2025, doi: 10.1177/26338076241293144.

[18] R. S. Datti, N. Mishra, M. Sirisety, and A. Tewari, "Risk perceptions and safe behaviours on the internet among older adults in India," *Secur. J.*, vol. 38, art. 41, 2025, doi: 10.1057/s41284-025-00480-6.

[19] C. Gupta, M. Hassan, and O. M. Adedayo, "Mobile privacy and security for older adults: A systematic review of concerns, risks, usability, and pathways for support," *J. Appl. Gerontol.*, 2026, doi: 10.1177/07334648261416184.

[20] N. A. Azam, A. G. Buja, M. Y. Darus, and N. M. Sahri, "SCSAM-Elderly: A new synergistic cyber security model for the elderly for IR4.0 readiness in Malaysia," in *Proc. 2022 IEEE 12th Symp. Comput. Appl. Ind. Electron. (ISCAIE)*, May 2022, pp. 117–122, doi: 10.1109/ISCAIE54458.2022.9794521.

[21] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, D. Ghersi, G. H. Guyatt, and D. Moher, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, art. n71, 2021, doi: 10.1136/bmj.n71.

[22] C. Llorente-Barroso, M. Sánchez-Valle, and M. Viñarás-Abad, "The role of the internet in later life autonomy: Silver surfers in Spain," *Humanit. Soc. Sci. Commun.*, vol. 10, art. 56, 2023, doi: 10.1057/s41599-023-01536-x.

[23] F. P. Rodríguez-Miranda, R. Illanes-Segura, Y. Ceada-Garrido, and J. C. Infante-Moro, "Validation of a scale based on the DigComp framework on internet navigation and cybersecurity in older adults," *Front. Educ.*, vol. 10, art. 1520929, 2025, doi: 10.3389/feduc.2025.1520929.

[24] V. Karagiannopoulos, A. Kirby, S. Oftadeh-Moghadam, and L. Sugiura, "Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study," *Comput. Law Secur. Rev.*, vol. 43, art. 105615, 2021, doi: 10.1016/j.clsr.2021.105615.

[25] S. Rathor, M. Zhang, and R. Goutam, "Cybersecurity challenges for the elderly: Vulnerabilities and risks," *IT Prof.*, vol. 27, no. 6, pp. 53–57, 2025, doi: 10.1109/MITP.2025.3571254.

[26] K.-L. Tan *et al.*, "Cybercrime vulnerability among older adults in Malaysia in the context of digital deception," *Arch. Tech. Sci.*, vol. 33, no. 2, pp. 154–164, 2025.

[27] N. Erades Pérez, M. C. Segura Cuenca, and E. Sitges Maciá, "ICT use and cyber-victimisation of older adults: An exploratory study," *Rev. Gen. Derecho Penal*, no. 38, 2022.

[28] S. Kim, "Impact of cybersecurity self-efficacy on digital economic behaviors among older adults," *INQUIRY*, vol. 62, art. 00469580251370933, 2025, doi: 10.1177/00469580251370933.

[29] M. Bukovec and K. Antoliš, "The impact of age and education on cyber security in digital banking," *Medijska Istraž.*, vol. 30, no. 2, pp. 129–152, 2024, doi: 10.22572/mi.30.2.6.

[30] A. K. Yadav, M. Ahmed, and B. Bansal, "Trust and safety perception in digital platforms among older populations," *TPM Test. Psychom. Methodol. Appl. Psychol.*, 2025.

[31] Y. Lu, R. Zhang, and W. Dai, "Digital risk perception among middle-aged and older adults in China: A perspective from mobile phone dependence within the I-PACE model," *Front. Psychiatry*, vol. 17, art. 1746285, 2026, doi: 10.3389/fpsyt.2026.1746285.

[32] J. Miljković, L. Manić, and B. Ljujić, "Educating older people: From victimisation to safety on the internet," *Temida*, vol. 27, no. 2, pp. 201–219, 2024, doi: 10.2298/TEM2402201M.

[33] X. Liu and R. Xie, "The practical experience and enlightenment of European digital literacy projects for senior citizens," *Doc. Inf. Knowl.*, vol. 40, no. 2, pp. 117–130, 2023, doi: 10.13366/j.dik.2023.02.117.

[34] K. Huang, X. Wang, J. Zhou, and B. Liang, "From fear to act: Enhancing older adults' cybersecurity practices by elderly-oriented fear appeal messages design," *Inf. Technol. People*, vol. 39, no. 4, pp. 1626–1652, 2026, doi: 10.1108/ITP-04-2024-0548.

[35] D. L. LoBuono, S. N. Leedahl, and E. Maiocco, "Older adults learning technology in an intergenerational program: Qualitative analysis of areas of technology requested for assistance," *Gerontechnology*, vol. 18, no. 2, pp. 97–107, 2019, doi: 10.4017/gt.2019.18.2.004.00.

[36] S. Wiroonrath, K. Na-Nan, S. Inmor, and V. Thammarakkitanon, "Enhancing digital intelligence among Thai seniors: Developing and validating the digital intelligence quotient scale," *Kybernetes*, vol. 55, no. 2, pp. 1015–1036, 2026, doi: 10.1108/K-08-2024-2062.

[37] Y. Zhang and Q. Zhang, "The effects of consistency and inconsistency in the source features of WeChat tweets on older Chinese adults' intentions to adopt personal information security knowledge," *Soc. Media Soc.*, vol. 10, no. 4, 2024, doi: 10.1177/20563051241306318.

[38] J. Kim and J. A. Gray, "Qualitative evaluation of an intervention program for sustained internet use among low-income older adults," *Ageing Int.*, vol. 41, no. 3, pp. 240–253, 2016, doi: 10.1007/s12126-015-9235-1.

[39] K. Parti, S. Abdelhamid, and T. Ladancsik, "Designing for life: A socioeconomic view of digital learning preferences in cybersecurity, with emphasis on older adults," *Societies*, vol. 15, no. 12, art. 342, 2025, doi: 10.3390/soc15120342.

[40] J. N. Rocheleau, H. Chalghoumi, J. Jutai, S. Farrell, Y. Lachapelle, and V. Cobigo, "Caregivers' role in cybersecurity for aging information technology users with intellectual disabilities," *Cyberpsychol. Behav. Soc. Netw.*, vol. 24, no. 9, pp. 624–629, 2021, doi: 10.1089/cyber.2020.0572.

[41] T. Vandecar-Burdin and M. Akpinar-Elci, "A qualitative exploration of dual vulnerability: Cybersecurity and social isolation risks for Alzheimer's caregivers during the COVID-19 pandemic," *Crim. Justice Stud.*, vol. 36, no. 3, pp. 292–310, 2023, doi: 10.1080/1478601X.2023.2254100.

[42] D. Brown, U. Butt, B. Naqvi, and S. Farag, "Bridging the digital gap: Security, privacy and challenges for older adults in governmental digital services," *Inf. Comput. Secur.*, early access, 2026, doi: 10.1108/ICS-09-2025-0352.

[43] R. de O. Ferreira, I. G. de O. Karnikowski, E. N. Costa, A. G. de Oliveira, M. S. Cruz, I. B. dos S. Brandão, and M. G. de O. Karnikowski, "Ability to detect digital risks: Effects of an educational intervention and dementia risk level," *Int. J. Environ. Res. Public Health*, vol. 23, no. 1, art. 58, 2026, doi: 10.3390/ijerph23010058.

[44] P. Pucer, B. Žvanut, and S. Vrhovec, "Adoption of smartphones among older adults and the role of perceived threat of cyberattacks," *Int. J. Inf. Secur.*, vol. 24, art. 101, 2025, doi: 10.1007/s10207-025-01014-2.

[45] M.-Y. Chen, "Establishing a cybersecurity home monitoring system for the elderly," *IEEE Trans. Ind. Inform.*, vol. 18, no. 7, pp. 4838–4845, 2022, doi: 10.1109/TII.2021.3114296.

[46] K. Tipayalai, N. Chittavimongkhon, and P. Sattayanurak, "Not over the hill: Exploring the digital divide among vulnerable older adults in Thailand," *J. Aging Soc. Policy*, 2026, doi: 10.1080/08959420.2026.2630920.

[47] L. Tomczyk and N. Edisherashvili, "Learning objectives in older adult digital education: Redefining digital inclusion," *Int. J. Cogn. Res. Sci. Eng. Educ.*, vol. 12, no. 3, pp. 507–520, 2024, doi: 10.23947/2334-8496-2024-12-3-507-520.

[48] M. Jiang, H.-Y. S. Tsai, S. R. Cotten, N. J. Rifon, R. LaRose, and S. Alhabash, "Generational differences in online safety perceptions, knowledge, and practices," *Educ. Gerontol.*, vol. 42, no. 9, pp. 621–634, 2016, doi: 10.1080/03601277.2016.1205408.

[49] M. D. Grilli, K. S. McVeigh, and R. C. Wilson, "Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails," *PsyArXiv Preprints*, 2020, doi: 10.31234/osf.io/upf6c.

[50] S. Beach, S. Czaja, R. Schulz, D. Loewenstein, and P. Lichtenberg, "Vulnerability to financial scams among older adults: Cognitive and psychosocial factors," *Innovation in Aging*, vol. 4, no. Suppl. 1, pp. 440–441, 2020, doi: 10.1093/geroni/igaa057.1447.

[51] J. Kävrestad, D. Lindvall, and M. Nohlberg, "Combating digital exclusion with cybersecurity training – an interview study with Swedish seniors," in *Proceedings of the 17th IFIP WG 11.12 International Symposium on Human Aspects of Information Security Assurance (HAISA 2023)*, S. Furnell and N. Clarke, Eds., Cham, Switzerland: Springer, 2023, vol. 1, pp. 3–12, doi: 10.1007/978-3-031-38530-8_1.

[52] T. Knight, X. Yuan, and D. M. B. Gayle, "Privacy and security concerns: A systematic review of older adults' perceptions surrounding the use of technology," *Journal of Data Protection and Privacy*, vol. 5, no. 4, pp. 388–400, 2023.

[53] J. Nicholson, B. Morrison, M. Dixon, J. Holt, L. Coventry, and J. McGlasson, "Training and embedding cybersecurity guardians in older communities," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama, Japan: Association for Computing Machinery, 2021, Art. no. 86, pp. 1–15, doi: 10.1145/3411764.3445078.

ISSN: 3028-8800
Julio - diciembre, 2026
Vol. 5 - No. 2
DOI: https://doi.org/10.62943/rig.v5n2.2026.572

[54] C. Zanchetta, H. Schiff, C. Novo, S. Cruz, and C. Vaz de Carvalho, "Generational inclusion: Getting older adults ready to own safe online identities," *Education Sciences*, vol. 12, no. 10, Art. no. 715, 2022, doi: 10.3390/educsci12100715.

Los autores no tienen conflicto de interés que declarar. La investigación fue financiada por los autores.