

Marco estratégico para el desarrollo de competencias en ciberseguridad para adultos mayores mediante Context-Based Micro-Training

Strategic Framework for Developing Cybersecurity Competencies in Older Adults through Context-Based Micro-Training

 Dayhan Vázquez-Torres¹;   Juan Carlos Pérez-Arriaga^{1,2};
 Martha Elizabet Domínguez-Bárcenas¹;  Xavier Limón¹

¹Universidad Veracruzana, Xalapa - México

²Universidad de Alcalá, Alcalá de Henares - España

Correspondencia: juaperez@uv.mx

Recibido: 31 Julio 2025

Aceptado: 14 Julio 2026

Disponible: 23 Julio 2026

Cómo citar / How to cite

D. Vázquez-Torres, J. C. Pérez-Arriaga, M. E. Domínguez-Bárcenas, and X. Limón, "Marco estratégico para el desarrollo de competencias en ciberseguridad para adultos mayores mediante Context-Based Micro-Training" *TecnoLógicas*, vol. 29, no. 66, e3593, 2026.

<https://doi.org/10.22430/22565337.3593>



Resumen

La inclusión digital de los adultos mayores es un factor clave para garantizar su participación segura en una sociedad digitalizada. Este grupo enfrenta desafíos en la adopción de una cultura de ciberseguridad derivados de su exposición a amenazas como la suplantación de identidad, el robo de información confidencial y el fraude digital. Derivado de un análisis de los hallazgos identificados en una revisión de la literatura previa, se identificaron estrategias que fomentan el desarrollo de competencias digitales en esta población, así como competencias digitales para la presencia digital segura de esta población, como el reconocimiento de sitios web seguros, la gestión de contraseñas y la protección de la privacidad en línea. A partir de lo anterior, se planteó el objetivo de diseñar un marco estratégico para el desarrollo de competencias en la gestión de contraseñas y en el reconocimiento de información veraz, acompañado de un instrumento de evaluación de competencias CCAM para adultos mayores. El marco se fundamentó en la metodología Context-Based Micro-Training (CBMT) y en el marco de competencias DigComp. Las actividades del marco incluyeron el diseño de módulos orientados al desarrollo de competencias mediante la impartición de un taller presencial. La validez del marco y del instrumento CCAM se evaluó mediante el juicio de expertos, lo que confirmó su pertinencia conceptual. Finalmente, se considera que la propuesta puede servir de base para futuras implementaciones que contribuyan a la inclusión digital de los adultos mayores, contemplando aspectos de ciberseguridad. El trabajo presenta como limitación la necesidad de confirmación mediante estudios empíricos con la población objetivo. Además de que requiere de un proceso de adaptación que considere características socioculturales de los participantes, de acuerdo con su contexto.

Palabras clave

Alfabetización digital, ciberseguridad para adultos, context-based micro-training, inclusión digital, información falsa.

Abstract

Digital inclusion for older adults is a key factor in ensuring their safe participation in a digitalized society. This population faces challenges in adopting a cybersecurity culture due to its exposure to threats such as identity theft, theft of confidential information, and digital fraud. Based on findings from a previous literature review, several strategies to foster the development of digital competencies among older adults were identified, including peer support, personalized educational materials, and strengthening voluntary community networks. Building on these findings, the objective of this study was to design a strategic framework to develop competencies in password management and in recognizing trustworthy information, accompanied by a CCAM competency assessment instrument for older adults. The framework was grounded in the Context-Based Micro-Training (CBMT) methodology and the DigComp competence framework. The proposed activities include designing competency-oriented modules delivered through an in-person workshop. The validity of both the framework and the CCAM instrument was evaluated through expert judgment, confirming their conceptual relevance. Finally, the proposed framework is considered a potential foundation for future implementations that promote the digital inclusion of older adults while incorporating cybersecurity considerations. As a limitation, the proposal requires validation through empirical studies involving the target population. Furthermore, it requires an adaptation process that considers sociocultural characteristics of the participants in their specific context.

Keywords

Digital literacy, cybersecurity for adults, context-based micro-training, digital inclusion, misinformation.

1. INTRODUCCIÓN

El presente estudio es una versión extendida del trabajo “Cybersecurity Strategies for the Digital Inclusion of Older Adults: A Systematic Literature Review”, presentado en las XI Jornadas Iberoamericanas de Interacción Humano-Computadora (IJIHC'25) [1]. En el estudio inicial se presentan hallazgos derivados de una revisión de la literatura de 57 estudios primarios, en donde se identifican las bases para diseñar la propuesta presentada en este trabajo.

La rápida transición digital ha cambiado significativamente la forma en que las personas interactúan, se comunican y utilizan los servicios. Sin embargo, este acelerado proceso ha incrementado la necesidad de adquirir competencias digitales básicas en ciberseguridad para participar en la sociedad digital actual. No obstante, los adultos mayores enfrentan desafíos para adaptarse a estas nuevas tecnologías, lo que amplía la brecha digital. Esta brecha se extiende a áreas como la ciberseguridad, donde la limitada alfabetización de los adultos mayores los expone a ciber-amenazas, como el fraude, el robo de identidad y la extorsión.

Diferentes estudios han documentado la brecha que afecta a este grupo, señalando la necesidad de promover procesos de alfabetización digital con un enfoque inclusivo y centrado en la seguridad digital, sin embargo, la mayoría solo se ha centrado en el uso básico de dispositivos [2], [3] dejando de lado el desarrollo de competencias en ciberseguridad.

Se identificaron tres vacíos concretos en el estado del arte, en primer lugar la ausencia de instrumentos de evaluación específicos para competencias de ciberseguridad en adultos mayores, los existentes están centrados en medir literacidad digital general, no abarcan el contexto de ciberseguridad; el siguiente vacío fue la falta de marcos educativos que consideren las características cognitivas, sociales y culturales de los adultos mayores desde una perspectiva de ciberseguridad, más allá del acceso a TIC. El presente estudio busca contribuir en estos dos vacíos de forma estructurada.

La mayoría de los trabajos encontrados se enfocan principalmente en la adopción de Tecnologías de la Información y la Comunicación (TIC) [2], [3]. En contraste, el presente estudio ofrece una visión más profunda de las áreas que requieren fortalecimiento en materia de alfabetización digital, así como de los planes y métodos que han mostrado resultados positivos en la formación digital de personas mayores.

El estudio presentado en [2] señala que el acceso limitado a las TIC suele estar relacionado con bajos ingresos y niveles educativos, situación que se ve agravada por el uso de dispositivos obsoletos, por lo que se destaca la necesidad urgente de invertir mayores recursos y atención en el desarrollo de habilidades digitales para adultos mayores. Asimismo, se observa que el

dominio de herramientas como Zoom y WhatsApp puede incrementar significativamente la alfabetización digital, ayudando a mitigar el aislamiento y a mejorar el bienestar general. También se enfatiza la necesidad de adaptar contenidos y métodos pedagógicos a las características emocionales, sociales y cognitivas de los adultos mayores.

Por su parte, la investigación referida en [3] analiza la evolución de la brecha digital en adultos mayores, sus factores causales y los esfuerzos de diversas organizaciones para enfrentar este fenómeno de manera proactiva. Además, evalúa la eficacia de diferentes modalidades educativas (presenciales y remotas) que fomentan la interacción social disminuyendo el aislamiento, y analiza la influencia de la frecuencia de las clases en los resultados de aprendizaje. Finalmente, destaca los beneficios del aprendizaje intergeneracional en el fortalecimiento de competencias digitales y la reducción de la brecha digital, así como el centrarse en el empoderamiento al momento de enseñar, lo cual provoca sentirse más seguros al utilizar dispositivos digitales, se destaca la importancia de las sesiones flexibles y adaptadas a las capacidades de los adultos mayores, brindando un ambiente donde puedan equivocarse sin ser juzgados.

La revisión sistemática de literatura realizada previamente permitió identificar aquellas estrategias relevantes para atender esta problemática, la tutoría entre pares, la capacitación de líderes comunitarios, el diseño de material educativo adaptado al sector, así como el aprendizaje intergeneracional. Asimismo, se evidenció una carencia de estrategias diseñadas específicamente para los adultos mayores, así como de instrumentos de evaluación para medir sus competencias digitales en ciberseguridad.

En un contexto latinoamericano, se identifica la necesidad de diseñar programas de capacitación orientados al desarrollo de competencias digitales que permitan que los adultos mayores tengan acceso a las tecnologías de la información, así como a servicios públicos y justicia [4]. Adicionalmente, se resalta la importancia de que no solo se diseñen herramientas tecnológicas, sino también el diseño de estrategias que fomenten su uso de forma clara [5].

El presente estudio propone una extensión del trabajo anteriormente realizado con el objetivo de diseñar y validar un marco estratégico de alfabetización digital para adultos mayores en ciberseguridad adaptado a las características, necesidades y preferencias de los adultos mayores. La propuesta se fundamenta en el modelo europeo DigComp [6]-[8] y en la metodología Context-Based Micro-Training (CBMT) [9], abordando dos competencias clave: la identificación de información verídica y la gestión de contraseñas. Además, se presenta un instrumento de evaluación diseñado específicamente para este marco estratégico (Cuestionario de Competencias en Ciberseguridad para Adultos Mayores (CCAM)). Esto fue sometido a un proceso de validación mediante juicio de expertos en ciberseguridad, educación e investigación para evaluar su pertinencia y solidez.

El diseño de esta propuesta se alinea con los objetivos particulares declarados en la sección de metodología: permitir que los adultos mayores reconozcan estafas y ofertas falsas, así como identificar prácticas para crear, gestionar y resguardar contraseñas de forma segura.

La estructura del artículo se divide en las siguientes secciones: en la sección 2, el diseño del protocolo de intervención, el diseño del marco estratégico y del instrumento CCAM; la sección 3 presenta los resultados de la evaluación del marco, así como la discusión de estos; finalmente, en la sección 4 se presentan las conclusiones del estudio.

2. METODOLOGÍA

Este trabajo se orienta a definir un marco de alfabetización en ciberseguridad para adultos mayores. El método de investigación consta de 3 fases (ver Figura 1). La primera fase, comprendió el diseño del Marco Estratégico de Alfabetización en Ciberseguridad para Adultos Mayores y del Cuestionario de Competencias en Ciberseguridad para Adultos Mayores (CCAM), fundamentados en los hallazgos de la RSL previa. La segunda fase consistió en la validación del

marco estratégico y del cuestionario de competencias mediante juicio de expertos [10], [11]. Finalmente, la tercera fase comprendió la identificación de áreas de mejora del marco.

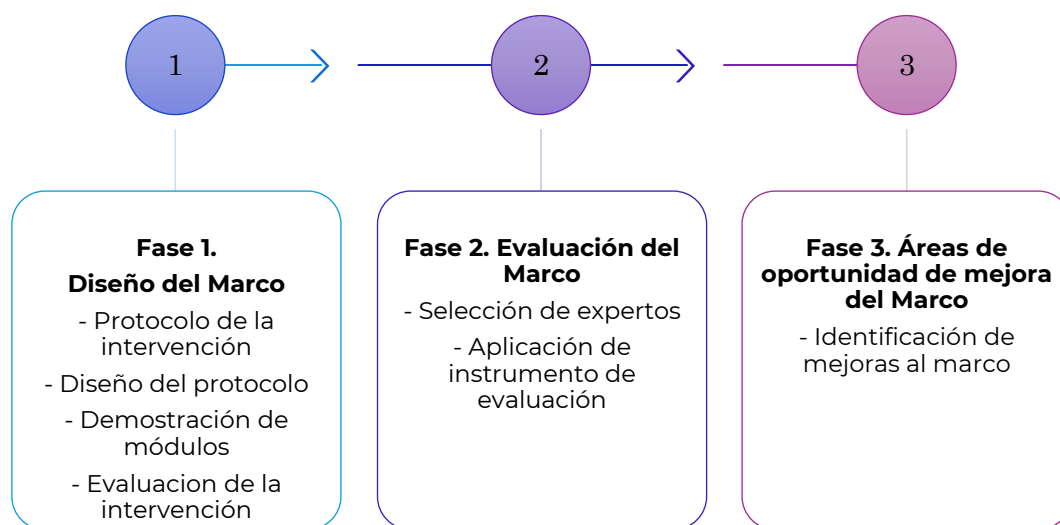


Figura 1. Proceso metodológico del estudio. Fuente: elaboración propia.

2.1 Fase 1. Diseño del marco estratégico

La propuesta está compuesta por cuatro apartados: el protocolo de la intervención, que incluye los objetivos, la selección de competencias, la metodología de aprendizaje y la modalidad educativa; el diseño de los materiales, la demostración de los módulos diseñados y la evaluación de la intervención.

2.1.1 Protocolo de intervención

El protocolo de la intervención define cómo se diseña el marco estratégico a partir del análisis de los hallazgos de la revisión de la literatura. En él se describen los objetivos, las competencias seleccionadas, la metodología de aprendizaje, así como la modalidad educativa.

Objetivo general: Diseñar un marco estratégico de alfabetización en ciberseguridad para adultos mayores con métodos adaptados a las características y necesidades específicas de la población.

Objetivos específicos:

- Permitir que los adultos mayores reconozcan estafas y ofertas falsas en mensajes publicitarios sospechosos mediante escenarios simulados.
- Permitir que los adultos mayores identifiquen cómo crear, gestionar y resguardar contraseñas seguras mediante escenarios prácticos.

Selección de competencias: La revisión sistemática de literatura [1] permitió identificar seis competencias digitales en ciberseguridad que los adultos mayores necesitan adquirir para tener una presencia segura en el ciberespacio (ver Tabla 1): evaluación de información verídica, identificación de correos sospechosos, gestión del acoso cibernético, gestión de contraseñas, gestión de la huella digital y protección de la privacidad. Estas competencias fueron documentadas en estudios que destacan la necesidad de iniciativas educativas que permitan a los adultos mayores adquirir competencias digitales en ciberseguridad para una inclusión digital segura [12]-[16].

Tabla 1. Competencias en ciberseguridad que los adultos mayores necesitan adquirir.

Fuente: elaboración propia basada en [1].

Competencia	Descripción
Evaluación de información verídica	Capacidad para encontrar y confiar en fuentes confiables y corroborar que información sea correcta o de lugares confiables.
Identificación de correos sospechosos	Habilidad para reconocer correos electrónicos fraudulentos mediante la revisión de la gramática y redacción del mensaje, incluso si proviene de una marca reconocida por el usuario.
Gestión del acoso cibernético	Capacidad para identificar y manejar el acoso en línea de manera adecuada.
Gestión de contraseñas	Habilidad de crear y proteger contraseñas de manera adecuada
Gestión de la huella digital	Habilidad de reconocer que registros y datos se manejan en línea.
Protección de la privacidad	Estrategias para limitar la información personal compartida en redes sociales, usar apodos y restringir el acceso a la información.

De las seis competencias identificadas, la gestión de contraseñas y la identificación de información verídica son las más frecuentemente reportadas en la literatura como prioritarias para este sector, con el mayor impacto documentado en su seguridad digital cotidiana. De acuerdo con la literatura revisada, estas dos competencias representan las áreas donde una intervención educativa tendría mayor impacto para la población objetivo de este estudio [1].

Sin embargo, para estructurar y organizar estas competencias dentro de un marco educativo, fue necesario identificar un referente de competencias digitales que permitiera fundamentar el diseño del marco propuesto. Durante la revisión de literatura [1], no fue posible identificar un marco de referencia específico para competencias de ciberseguridad en adultos mayores, por lo tanto, se realizó una revisión exploratoria de los marcos digitales disponibles, identificando el marco europeo DigComp [6]-[8], como un marco relevante y mayormente utilizado en estudios de alfabetización digital para contextos similares al del sector objetivo. El marco DigComp [6]- [8] estructura las competencias digitales en cinco áreas principales: búsqueda, evaluación y gestión de la información; comunicación y colaboración; creación de contenidos; seguridad, bienestar y uso responsable; e identificación y resolución de problemas, estas últimas identificadas en la versión más reciente del marco [8]. Su pertinencia en el estudio está respaldada por estudios regionales que evidencian que la brecha digital de adultos mayores va más allá de la brecha de acceso a dispositivos, incluye la brecha de calidad de uso presentando una carencia de competencias para interactuar de manera segura en el ciberespacio, y se presenta como una oportunidad para que los adultos mayores desarrollen sus competencias digitales básicas que implican conocimientos en seguridad y solución de problemas, competencias que para este sector amplía sus oportunidades y reduce su exclusión [4].

Las dos competencias seleccionadas se alinearon con dos áreas específicas del marco DigComp 3.0: la identificación de información verídica corresponde al “Área 1. búsqueda, evaluación y gestión de la información”, que comprende de la capacidad para buscar, evaluar y gestionar información digital de forma crítica; la gestión de contraseñas se alinea con el “Área 4. seguridad, bienestar y uso responsable”, que abarca la protección de dispositivos, datos personales y privacidad en el entorno digital [8]. Esta alineación permite que los módulos del taller propuestos en la sección 2.1.2 no solo atiendan las necesidades identificadas en la RSL [1], sino que también se vinculen con un referente de competencias válido y reconocido internacionalmente.

Metodología de aprendizaje: Para seleccionar la metodología de aprendizaje del marco, se consideraron los métodos de alfabetización para adultos mayores identificados en la RSL [1], entre los que destacan el aprendizaje basado en escenarios cotidianos, los talleres presenciales con tutoría entre pares y el uso de material educativo adaptado a sus necesidades y características. Los estudios analizados coinciden en dos principios base para lograr el

aprendizaje en los adultos mayores: la brevedad de los contenidos y la relevancia contextual de los ejemplos. Independientemente del soporte utilizado, las intervenciones más efectivas presentan la información en fragmentos cortos vinculados directamente a situaciones con las que se vean familiarizados en su vida diaria [1]. Para esta selección se revisaron metodologías de alfabetización digital para adultos mayores reportadas en la literatura, como el modelo Elderlearn y enfoques de micro-aprendizaje genérico. Sin embargo, estas metodologías están diseñadas para atender principalmente a la adopción de competencias digitales básicas y la literacidad tecnológica, dejando a un lado la formación en ciberseguridad. Asimismo, no integran de forma explícita el uso de contextos cotidianos ni la retroalimentación inmediata como elementos centrales de aprendizaje. Es por ello, que a partir de una revisión exploratoria se identificó la metodología Context-Based Micro-Training (CBMT) [9], un marco diseñado específicamente para la formación en ciberseguridad que utiliza secuencias cortas de aprendizaje directamente relacionadas con situaciones del contexto del participante, se propone presentar la información de forma sencilla evitando sobrecargar al participante, la incorporación de ejemplos reales y retroalimentación inmediata.

Diversos estudios respaldan la efectividad de este enfoque. En un estudio de [17] que consideró a participantes de distintos países, se demostró que el CBMT presenta resultados positivos en la enseñanza de distintos grupos demográficos donde la edad no impacta negativamente en su percepción, por el contrario, fue descrito como una forma accesible de recibir capacitación corta y fácil de entender en temas de ciberseguridad. De igual manera, en el experimento comparativo de [18] donde se buscó evidenciar la eficiencia de la enseñanza basada en juegos y con la metodología CBMT demostró que esta era más efectiva debido a que generaba un grado de consciencia en los participantes para la relación de phishing. Por otro lado, en un estudio donde la muestra fue específicamente el sector de adultos mayores, los participantes reportaron que recibir la información de forma breve y consejos prácticos sobre situaciones contextuales es justamente lo que necesitan e incluso reportaron sentir menos preocupación por usar internet [19], lo que sugiere que CBMT puede contribuir a reducir la ansiedad tecnológica identificada en la RSL [1] como una de las principales barreras reportadas para este sector. La alineación de estos elementos y los principios identificados en la RSL [1] justifica la selección del CBMT como metodología de aprendizaje del marco propuesto.

CBMT incluye objetivos que describen lo que las capacitaciones deben tratar y describen cómo hacerlo. Este enfoque sugiere que la capacitación debe impartirse en secuencias cortas cuando la información es de relevancia directa, incorporando contenido breve y práctico, ejemplos reales adaptados al contexto de los adultos mayores y retroalimentación inmediata tras ejercicios teóricos o prácticos. De acuerdo con el enfoque CBMT, la propuesta del marco se adaptó al diseño de módulos cortos basados en las competencias identificadas en el marco europeo DigComp. En la sección 2.2.2 se presentan los dos módulos desarrollados con sus respectivos escenarios basados en el contexto de los adultos mayores, retroalimentación y ejercicios prácticos.

Selección de modalidad educativa: En cuanto a la selección de modalidad educativa, los hallazgos de la RSL [1] indican que los adultos mayores se ven mayormente beneficiados por estrategias que combinan el apoyo social con la práctica guiada. Los estudios revisados muestran una preferencia consistente por los cursos presenciales frente a las modalidades virtuales, asociando la modalidad presencial con mayor confianza, menor ansiedad tecnológica y una mejor participación para la resolución de dudas. Estrategias como los talleres con tutoría entre pares y los programas de CiberGuardianes, donde adultos mayores con mayor alfabetización digital apoyan a sus pares demostraron ser particularmente efectivas en este sector, puesto que la interacción entre pares, especialmente con personas de su misma edad genera un ambiente de confianza donde pueden resolver dudas y compartir experiencias sin temor a ser juzgados. Así mismo, la mayoría de las personas mayores culminaron su vida laboral y se encuentran jubilados, lo que podría permitirles disponer de tiempo libre para participar en actividades presenciales. La estrategia educativa busca capacitar a los adultos mayores en conocimiento y habilidades de ciberseguridad, con el fin de fortalecer su confianza digital y

promover su autonomía en el uso de TIC e internet. Dado lo anterior, un taller presencial se presenta como la modalidad más adecuada al asegurar un aprendizaje a través de la práctica guiada y el acompañamiento social.

2.1.2 Diseño de la propuesta

Los contenidos se estructuraron con base en dos competencias principales de ciberseguridad identificadas como las prioritarias en la RSL [1], los cuales se integraron como módulos.

Identificación de información verídica: este módulo busca capacitar a las personas mayores para reconocer información falsa o engañosa. Permitiendo una interacción más segura y consciente en redes sociales, sitios web y mensajería.

Gestión de contraseñas: Este módulo busca enseñar a los adultos mayores a crear, gestionar y proteger contraseñas seguras de manera fácil, usando técnicas que les permitan recordar y mantener seguras sus cuentas.

Pautas para el diseño del material educativo: los hallazgos de la RSL [1] señalan que los adultos mayores presentan preferencias con respecto a los materiales educativos, los cuales deben contar con ciertas características como: tipografía clara y adecuada, lenguaje simple, guías paso a paso e ilustraciones visuales. Con base en estas preferencias, el marco establece las siguientes pautas para el diseño del material educativo.

- Guías/manuales digitales o físicas, paso a paso con lenguaje simple e ilustraciones visuales.
- Videos cortos con lenguaje simple y claro.
- Presentaciones minimalistas con tamaño de fuentes adecuadas y textos claros.
- Ejercicios prácticos adaptados a contextos reales.
- Uso de juegos tradicionales: lotería, memorama, sopa de letras, crucigramas.
- Actividades donde involucren métodos tradicionales como el escribir o subrayar.

Detalles operativos del marco estratégico: los detalles operativos del marco estratégico incluyen características de los participantes, características del facilitador, duración de las sesiones y tamaño del grupo (ver Tabla 2).

Tabla 2. Detalles operativos del marco estratégico. Fuente: elaboración propia.

Detalle	Descripción
Características de los participantes	- Personas de 60 años en adelante.
	- Saber leer y escribir.
	- Contar con conocimientos básicos en el uso de algún dispositivo móvil, tableta o computadora.
Características del facilitador	- Experiencia en alfabetización digital.
	- Tener conocimiento de las características, necesidades y ritmos de aprendizaje de los adultos mayores.
	- Afinidad generacional [20].
Duración de las sesiones	- Implementar sesiones cortas para evitar fatiga cognitiva. La metodología CBMT propone secuencias de aproximadamente cinco minutos por escenario contextual [9].
Tamaño del grupo	- Trabajar con grupos reducidos de entre 8 y 15 participantes para facilitar el acompañamiento personalizado y la atención de dudas durante las actividades [21].

2.1.3 Demostración de módulos

Para garantizar que las actividades sean adecuadas y atractivas para los adultos mayores, se diseñan siguiendo la metodología de Context-Based Micro-Training (CBMT) que se enfoca en utilizar escenarios reales o contextos cotidianos para los participantes. La retroalimentación inmediata se proporciona de manera sencilla y comprensible para reforzar el aprendizaje.

A continuación, se muestra un escenario de ejemplo por cada uno de los módulos definidos en esta estrategia.

Módulo 1: Identificación de información verídica

Objetivo: que los adultos mayores logren reconocer información falsa o engañosa en internet mediante escenarios que simulen situaciones reales.

Escenario 1. ¿Qué hacer si recibes un mensaje como el siguiente de un supuesto familiar?

Descripción. Un adulto mayor recibe un mensaje en WhatsApp, se presenta una imagen (ver Figura 2), que contiene un mensaje simulando ser un familiar solicitando dinero. Se les pide a los participantes que lo analicen y discutan que harían para comprobar si es real o falso.

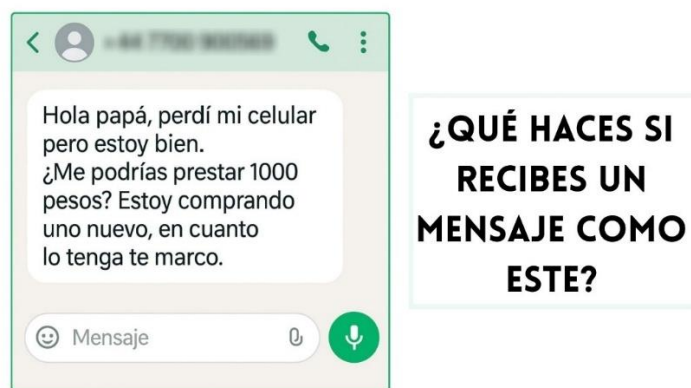


Figura 2. Escenario mensajes de WhatsApp sospechosos. Fuente: elaboración propia.

Retroalimentación inmediata: explicar las señales de alerta que pueden indicar que el mensaje es un intento de estafa (ver Figura 3):

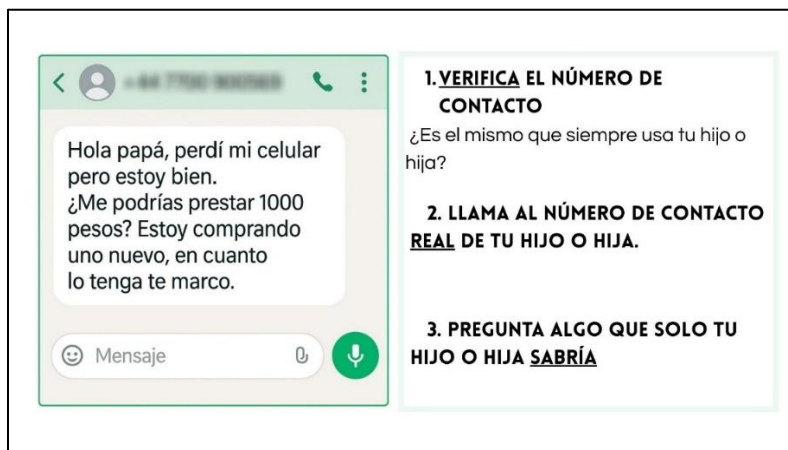


Figura 3. Señales de alerta en mensajes de WhatsApp. Fuente: elaboración propia.

- La lada o número desconocido
- El lenguaje de urgencia o exagerado
- Foto de perfil

Ejercicio práctico: proporcionar varios ejemplos de mensajes falsos que podrían recibir y pedir que analicen cada mensaje basándose en lo que han aprendido sobre señales de alerta.

Sugerencia de actividad para los participantes:

- Preguntar a los participantes si alguna vez han recibido mensajes similares o si conocen un caso parecido.
- Que los participantes compartan consejos desde su punto de vista recibiendo retroalimentación de si son o no correctos sus consejos.

Módulo 2: Gestión de contraseñas

Objetivo: Que los adultos mayores reconozcan como crear, gestionar y resguardar contraseñas seguras mediante escenarios prácticos.

Escenario 1. Creación de contraseñas seguras.

Descripción. Después de la explicar los elementos que necesita una contraseña para considerarse segura, se les muestra a los participantes de forma visual y simplificada los cuatro elementos que requiere una contraseña (ver Figura 4). Además, es necesario brindar consejos que los adultos mayores puedan recordar (ver Figura 5), una forma fácil de sustituir letras por números.



Figura 4. Consejos para elaborar contraseñas seguras. Fuente: elaboración propia.

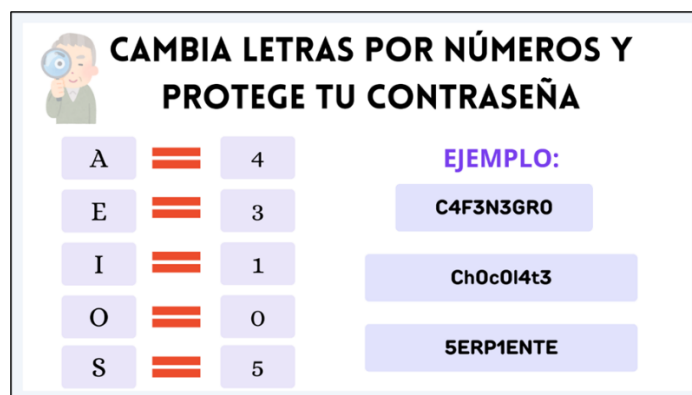


Figura 5. Consejos para elaborar contraseñas seguras. Fuente: elaboración propia.

2.1.4 Evaluación de la intervención

La evaluación de la intervención se estructura en dos momentos: un pre-test aplicado antes del taller para identificar el nivel de competencias en ciberseguridad de los participantes y un post-test aplicado al finalizar el taller para medir el impacto de este y comparar los niveles de competencia adquiridos.

Evaluación pre-intervención (pre-test): de acuerdo con la RSL [1] se identificó una carencia significativa de instrumentos específicos para evaluar competencias de ciberseguridad en adultos mayores. Los instrumentos disponibles, como el Senior Digital Literacy Evaluation (SDLE), diseñado para evaluar la alfabetización digital en personas mayores [22], el Computer Proficiency Questionnaire (CPQ), orientado a medir competencias digitales generales, y su adaptación para dispositivos móviles, el Mobile Device Proficiency Questionnaire (MDPQ) [23], evalúan habilidades digitales generales sin centrarse específicamente en competencias de ciberseguridad. Esta carencia justifica el diseño del Cuestionario de Competencias en Ciberseguridad para Adultos Mayores (CCAM) como instrumento diagnóstico específico para las dos competencias priorizadas en este marco.

En este contexto, para evaluar la efectividad de la estrategia propuesta se plantea una fase diagnóstica para tener el contexto de conocimientos y habilidades de los participantes antes de tomar el taller, por ello se propone la aplicación del Cuestionario de Competencias en Ciberseguridad para Adultos Mayores (CCAM) que fue diseñado para este proyecto.

El cuestionario se enfoca en la evaluación dos competencias principales: la evaluación de información verídica y la gestión de contraseñas. Siendo estas competencias las más mencionadas en la RSL [1] como necesarias para los adultos mayores. Estas habilidades están alineadas en dos áreas con el Marco de Competencias Digitales para la Ciudadanía (DigComp).

Área 1. Búsqueda, evaluación y gestión de la información.

Área 4. Seguridad, bienestar y uso responsable.

- 4.2 Protección de los datos personales y la privacidad.
- 4.3 Apoyar el bienestar.

Para asegurar la validez del cuestionario, el diseño se basó en la estructura del “Computer and Mobile Device Proficiency Questionnaires (CPQ y MDPQ)” adaptado al español por [23]. Este instrumento es ampliamente utilizado para evaluar las competencias digitales en adultos mayores. Así mismo, para crear las preguntas del cuestionario diseñado, se tomó como referencia el estudio de [24], “Cybersecurity competence of older adult users of mobile devices”. Sin embargo, a diferencia del estudio original, el cuestionario no se centra solo en dispositivos móviles, sino en competencias básicas de ciberseguridad basadas en las áreas antes mencionadas.

El CCAM cuenta con 18 preguntas, cada una con una escala de Likert de cinco niveles. Se propone su aplicación en formato impreso, ya que en el CPQ [23] documentaron que el 62.3 % de los adultos mayores que participaron en su estudio rechazó completar el cuestionario en línea, optando por la versión en papel supervisada, lo que refleja las barreras tecnológicas propias de este sector.

Con el fin de garantizar la accesibilidad en la aplicación del cuestionario, se consideran los principios de accesibilidad cognitiva establecidos por el “W3C COGA Task Force” [25], que recomienda permitir que las personas completen las tareas a su propio ritmo y sin presión de tiempo. Estas consideraciones son particularmente relevantes para adultos mayores y personas con diversas necesidades cognitivas, quienes pueden requerir tiempo suficiente para analizar la información y formular sus respuestas correctamente.

Con base en el número de preguntas y en las características del sector, se propone un tiempo de aplicación entre 20 a 40 minutos con supervisión, dado que este puede variar según las condiciones individuales de cada participante, ya que algunos podrían requerir apoyo adicional para comprender la dinámica del cuestionario o interpretar ciertas preguntas.

A continuación, se muestra un fragmento del instrumento diseñado considerando ambas referencias (ver Tabla 3). El cuestionario completo se puede consultar en el [Material suplementario](#) (Tabla A1).

Tabla 3. Cuestionario de Competencias en Ciberseguridad para Adultos Mayores (CCAM).

Fuente: elaboración propia.

No.	Afirmación	Nunca lo he intentado	Lo intenté, pero no pude hacerlo	A veces lo logro, con dificultad	Casi siempre lo hago bien
1	Sé cómo bloquear mi teléfono o tableta con una contraseña o PIN.				
2	Sé que no debo usar contraseñas fáciles de adivinar como "123456" o mi fecha de nacimiento.				
3	Sé cómo crear una contraseña segura (por ejemplo: usando letras, números y símbolos)				

Evaluación post-intervención (post-test): Con el objetivo de medir el impacto real de la estrategia implementada, se contempla una fase de post-evaluación que consiste en aplicar nuevamente el Cuestionario de Competencias en Ciberseguridad para Adultos Mayores (CCAM) utilizado previamente en la fase diagnóstica.

Esta fase permitirá comparar los resultados obtenidos antes y después del taller, lo que ayudará a identificar los avances en la adquisición de las competencias, identificar áreas que requieren ajustes, lo cual también servirá como retroalimentación para mejorar futuros talleres y, si es necesario, el diseño de los materiales educativos.

2.2 Fase 2. Evaluación del marco estratégico

Para validar la propuesta del marco estratégico de ciberseguridad para adultos mayores, se optó por el juicio de expertos, una técnica que, según [11], puede definirse como una opinión o valoración fundamentada por profesionales con experiencia en un área específica, quienes pueden contribuir con información, evidencia y criterio para la toma de decisiones. En este caso el proceso de validación de la propuesta se realizó con 5 expertos que cumplen con el perfil relacionado con alguna de las dimensiones identificadas y que cuentan con experiencia en áreas relacionadas como la educación en ciberseguridad, administración educativa e investigación. Cada uno de ellos cumple con un perfil que aporta retroalimentación importante para la propuesta, como la planeación educativa, el diseño de estrategia o el análisis de resultados.

Los criterios de selección de los expertos consideraron: (1) contar con un mínimo de tres años de experiencia profesional o académica en alguna de las áreas relevantes para el estudio tales como ciberseguridad, educación o investigación educativa, (2) haber participado en proyectos de formación o investigación relacionados con tecnología educativa o seguridad informática y (3) contar con al menos un producto académico o profesional en el área, ya sea publicación, proyecto o actividad de formación (ver Tabla 4). El método de reclutamiento se realizó mediante una invitación por correo electrónico a los expertos para solicitar su participación en el proceso de evaluación. Por medio de esta notificación se dio contexto de la propuesta y se acordó con ellos la fecha, hora y lugar de la revisión. Para evaluar la propuesta, se utilizó el modelo de evaluación conceptual utilizado en trabajos como [9].

Este instrumento consta de ocho preguntas (numeradas de P1 al P8), además de una pregunta abierta, para obtener retroalimentación de los participantes (ver Tabla 5). El instrumento utiliza una escala Likert numerada del 1 al 5 donde 1 es un valor de “totalmente en desacuerdo” y 5 es “totalmente de acuerdo”.

Tabla 4. Información demográfica de los evaluadores de la propuesta. Fuente: elaboración propia.

ID	Género	Cargo actual	Categoría	Experiencia	Actividades relevantes
EP- 1	F	Alta Dirección en Tecnologías de Información	Administración	+ 20 años	Liderazgo en iniciativas de cultura de ciberseguridad Participación en redes nacionales de TIC en educación superior Coordinación del Grupo de Ciberseguridad de MetaRed México (ANUIES-TIC)
EP- 2	M	Dirección de Servicios de Red e Infraestructura Tecnológica	Administración	+ 20 años	Docencia en asignaturas de redes y seguridad Participación en foros internacionales de gobernanza de internet
EP- 3	M	Departamento de Seguridad y Monitoreo	Investigación	+ 5 años	Impartición de pláticas de concienciación en ciberseguridad nivel universitario
EP- 4	M	Profesor de Tiempo Completo en asignaturas relacionadas a ciberseguridad	Investigación y educación	+ 15 años	Investigación en accesibilidad e inclusión digital Docencia en ciberseguridad
EP- 5	M	Profesor por Asignatura, en ciberseguridad	Investigación y educación	+ 8 años	Docencia en ciberdelitos y herramientas forenses digitales Publicaciones en conferencias nacionales.

Tabla 5 Preguntas del instrumento de evaluación conceptual aplicado a los evaluadores. Fuente: elaboración propia.

ID	Pregunta
P1	¿Los principios teóricos son sólidos?
P2	¿Los principios teóricos son relevantes?
P3	¿La literatura revisada es adecuada?
P4	¿La propuesta conceptual es lógicamente coherente?
P5	¿La propuesta es adecuada para el propósito para el cual fue diseñada?
P6	¿La propuesta conceptual resultante es congruente?
P7	¿La propuesta aporta algo nuevo?
P8	¿El estilo de presentación es adecuado para un informe científico?

2.3 Fase 3. Áreas de oportunidad de mejora del marco

A partir del análisis de las respuestas de los expertos obtenidas durante la evaluación del marco estratégico y del Cuestionario de Competencias en Ciberseguridad para Adultos Mayores (CCAM) mediante juicio de expertos, se realizó la interpretación de las valoraciones cuantitativas

obtenidas para cada uno de los criterios evaluados mediante el instrumento de evaluación, así como el análisis de las observaciones cualitativas proporcionadas por los expertos.

El instrumento de evaluación utilizado (Tabla 5), evaluó ocho puntos: solidez de los principios teóricos (P1), relevancia del marco teórico (P2), pertinencia de la revisión de literatura (P3), coherencia lógica (P4), adecuación al propósito (P5), congruencia conceptual (P6), aporte de novedad (P7) y estilo de presentación (P8). Los datos recopilados indican una aceptación positiva de la propuesta por parte de los expertos consultados (ver Figura 6).

RESULTADOS DE EVALUACIÓN DE 5 EXPERTOS

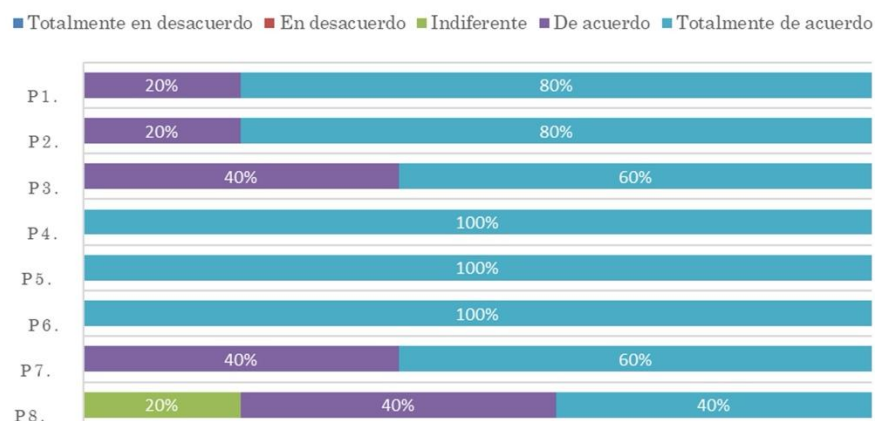


Figura 6. Resultados de evaluación de 5 expertos. Fuente: elaboración propia.

Este análisis permitió conocer el grado de aceptación de la propuesta y detectar oportunidades de mejora relacionadas con la fundamentación teórica, la estructura del marco, el instrumento CCAM y la claridad en la presentación de la propuesta. Las recomendaciones proporcionadas por los expertos se utilizaron para establecer sugerencias y ajustes orientados a fortalecer el marco estratégico antes de su implementación con la población objetivo.

Como resultado de esta fase se identificaron oportunidades de mejora relacionadas con la adaptación sociocultural del instrumento CCAM, la definición de la población objetivo y el fortalecimiento del marco previo a su implementación.

En relación con la solidez y relevancia de los principios teóricos de la propuesta (P1 y P2), el 80 % de los participantes manifestó estar “totalmente de acuerdo” mientras que el 20 % restante indicó estar “de acuerdo”.

Los expertos consideraron que la revisión de la literatura realizada es adecuada (P3) con el 60 % expresando “totalmente de acuerdo” mientras el 40 % respondió “de acuerdo”. Todos los expertos (100 %) estuvieron de acuerdo en la coherencia lógica de la propuesta (P4) lo que significa que está alineada con su contenido. Los expertos estuvieron de acuerdo con la propuesta, ya que el 100 % de los participantes afirmó estar “totalmente de acuerdo” con la adecuación de la estrategia al propósito planteado (P5). En cuanto a la congruencia conceptual (P6) también se obtuvo el 100 % de respuestas en la opción “totalmente de acuerdo”. Respecto al aporte de novedad (P7), el 60 % de los expertos manifestó estar “totalmente de acuerdo” y el 40 % “de acuerdo”, esto indica que se reconoce como una contribución novedosa. En relación con el estilo de presentación de la propuesta (P8) el 40 % de los expertos indicó estar “totalmente de acuerdo”, un 40 % estar “de acuerdo” mientras que un 20 % se mostró “indiferente”, si bien la mayoría considera el estilo adecuado para un informe científico existen percepciones distintas que podrían indicar áreas de mejora. Finalmente, como se mencionó, el instrumento incluyó una pregunta abierta para recibir comentarios adicionales sobre la propuesta diseñada. Los comentarios recibidos se listan a continuación:

- “Sin cambios respecto a la retroalimentación durante la exposición”.
- “Validar que todas las preguntas del instrumento si consideren el nivel socio-cultural y de alfabetización de nuestro país”.
- “Me parece una muy buena estrategia, el tema es muy relevante y llevarlo a cabo sería un gran éxito”.
- “Haciendo un estudio experimental con adultos mayores en México, sobre todo porque los papers analizados deben ser de otros países y dada la diversidad que existe en el conocimiento, habilidades y aspectos culturales de un adulto mayor puede dar un sesgo. Felicidades por el trabajo”.
- “Analizar los contextos de la información consultada para adecuar la propuesta de mejor forma. Definir una población objetivo con mayor detalle”.

3. RESULTADOS Y DISCUSIÓN

A partir de la evaluación por expertos se identifican hallazgos relevantes. Las preguntas relacionadas con la coherencia lógica, la adecuación al propósito y la congruencia conceptual (P4, P5 y P6) obtuvieron valoraciones de “totalmente de acuerdo” por todos los expertos participantes, lo que sugiere que el marco presenta consistencia interna y se mantiene alineado con los objetivos planteados para la propuesta. El único aspecto que no alcanzó consenso absoluto entre los expertos fue el relativo al estilo de presentación (P8), en el que uno de los participantes emitió una valoración neutral. No obstante, las observaciones cualitativas asociadas a este criterio proporcionan información relevante para futuras mejoras del marco y refuerzan la necesidad de realizar procesos de validación empírica con la población objetivo antes de su implementación a en grupos más grandes.

El enfoque del marco propuesto y los resultados de la evaluación mantienen consistencia con trabajos previos realizados en contextos similares sobre la alfabetización digital de adultos mayores. En el trabajo de [26], a partir de un programa municipal que buscó la capacitación presencial, se logró documentar una preferencia por la interacción cara a cara frente a las alternativas virtuales, así como el uso de un lenguaje libre de tecnicismos y centrado en metáforas cotidianas para reducir la ansiedad ante temas de ciberseguridad. En dicho trabajo, se incorpora la seguridad a un ritmo lento mediante instrucciones paso a paso y repetitivas. De manera similar, [27] señalan que los enfoques comunes de ciberseguridad desarrollados para usuarios jóvenes suelen generar barreras para los adultos mayores y recomiendan, en su lugar, el uso de lenguaje sencillo, ejemplos concretos y apoyo comunitario continuo, principios que coinciden con la modalidad presencial, la metodología de aprendizaje CBMT y las pautas de diseño de material educativo recomendadas en el presente marco.

Adicionalmente, [28], mediante su análisis de segmentación de usuarios basada en técnicas de clustering, observaron que los adultos mayores no son un grupo homogéneo incluso en poblaciones demográficamente similares, identificando subgrupos con necesidades de capacitación distintas según el área de ciberseguridad evaluada. Esta consideración es relevante para el presente marco, ya que sugiere que, en una futura fase, la aplicación del CCAM podría contemplar un proceso previo de segmentación de los participantes, sin asumir que todos los adultos mayores requieran la misma intervención.

A diferencia de otros estudios orientados únicamente al diseño de estrategias educativas, el presente trabajo incorpora tanto la validación del protocolo de intervención como la del instrumento de evaluación CCAM, lo que permite verificar la coherencia entre la propuesta educativa y la herramienta diseñada para evaluar las competencias abordadas. Asimismo, las observaciones de los expertos sugieren la necesidad de adaptar ciertas preguntas del CCAM, considerando con mayor detalle las características socioculturales de la población objetivo. Este aspecto resulta relevante en contextos con diferencias regionales y educativas, donde el

lenguaje, los ejemplos y las situaciones planteadas podrían requerir ajustes para garantizar su adecuada comprensión por parte de distintos grupos de adultos mayores.

El juicio de expertos permitió evaluar la pertinencia teórica y la solidez conceptual tanto del marco como del instrumento CCAM, verificando su coherencia con los objetivos planteados y contribución al sector. Sin embargo, este proceso no permite determinar la efectividad real del taller para adultos mayores en un contexto de implementación práctica. Es por ello, que es necesario validar si la aplicación del marco favorece efectivamente la adquisición de competencias de ciberseguridad, requiere el desarrollo de estudios empíricos con la población objetivo, aspecto que constituye una de las principales líneas de trabajo futuro de la presente investigación.

La definición de estrategias que fomenten el desarrollo de competencias de ciberseguridad en adultos mayores representa un área de oportunidad clara en investigación. Tal como lo señala [5], donde destaca que en realidad no existe de forma clara una inclusión digital en un contexto latinoamericano, lo que propicia el aumento de la brecha digital en ciertos grupos demográficos. Sin embargo, las implicaciones prácticas de la presente propuesta están enfocadas justamente en contribuir a la disminución de la brecha en la población de adultos mayores. También señala que se identifican procesos para el conocimiento de herramientas tecnológicas, sin profundizar en el desarrollo de competencias que permitan su uso eficiente. Este hallazgo concuerda con lo identificado en la revisión de literatura realizada previamente por los autores de este trabajo.

Este tipo de brechas se han analizado desde distintas perspectivas. En el trabajo de [4] se analiza la necesidad de que los estados proporcionen programas de capacitación constante dirigida a adultos mayores lo que posibilita el acceso a servicios públicos y a la justicia. Adicionalmente destacan los beneficios asociados con funciones motoras y cerebrales, ya que estos beneficios no solo se adquieren directamente con la capacitación, sino que al participar en grupos sociales se fomenta la interacción con otras personas, impactando positivamente en el bienestar de esta población.

La propuesta de este marco para el desarrollo de las competencias mencionadas en el presente estudio se alinea con lo identificado en el estado del arte. Este marco incorpora metodologías para el desarrollo de competencias en ciberseguridad sustentado en la metodología CBMT y en el marco de competencias digitales DigComp. Así mismo, considera la interacción del adulto mayor en grupos presenciales y uso de material adaptado a su contexto, con la finalidad de facilitar la comprensión de los temas apoyado de un entorno social.

4. CONCLUSIONES

El presente estudio muestra el diseño de un marco de alfabetización en ciberseguridad para adultos mayores fundamentado en la evidencia hallada en la literatura existente, metodológicamente alineado con la metodología Context-Based Micro-Training y con el marco de competencias DigComp.

Este estudio busca cubrir un área de oportunidad en la investigación sobre el diseño de propuestas educativas que fomenten el desarrollo de competencias en ciberseguridad para el sector de adultos mayores. Desde una perspectiva metodológica, el instrumento CCAM representa una aportación concreta al campo al ser un cuestionario diseñado explícitamente para evaluar competencias de ciberseguridad en adultos mayores, que adapta la estructura del CPQ/MDPQ al contexto de ciberseguridad y al sector. Desde una perspectiva práctica, el marco propuesto puede orientar a instituciones educativas o programas gubernamentales que busquen implementar estrategias de alfabetización digital que consideren aspectos de ciberseguridad. La validación mediante juicio de cinco expertos en ciberseguridad, educación e investigación confirmó la validez y la pertinencia teórica del marco y del instrumento CCAM, con niveles de acuerdo del 100 % en coherencia lógica, adecuación al propósito y congruencia conceptual. Sin embargo, es importante delimitar el alcance de esta validación, puesto que el

juicio de expertos evalúa la pertinencia conceptual de la propuesta, no su efectividad real en contextos de implementación.

En consecuencia, la capacidad del marco para favorecer el desarrollo de competencias de ciberseguridad en adultos mayores requiere confirmación mediante estudios empíricos con la población objetivo, lo cual constituye la principal limitación del presente trabajo. Adicionalmente, dado que los hallazgos identificados en la revisión de la literatura realizada previa al diseño de este trabajo consideran el contexto global, el marco propuesto requiere un proceso de adaptación y validación que considere las características socioculturales específicas de los adultos mayores en un contexto latinoamericano, incluyendo los niveles de alfabetización, el acceso a dispositivos y los contextos cotidianos de exposición digital. Como líneas de trabajo futuras, se proponen: la implementación y evaluación empírica del taller con adultos mayores en contextos reales para medir el impacto del marco en la adquisición de las competencias abordadas, la ampliación de los módulos y el instrumento del CCAM para incorporar otras competencias de ciberseguridad identificadas en la RSL, como la identificación de correos sospechosos, la gestión de la huella digital y la protección de la privacidad. Atender estas líneas permitiría no solo validar el potencial del marco propuesto, sino también contribuir al diseño de estrategias de inclusión digital segura adaptadas a las necesidades de los adultos mayores en la región.

5. AGRADECIMIENTO Y FINANCIACIÓN

Los autores agradecen a la Facultad de Estadística e Informática de la de México por el apoyo recibido para la realización de esta investigación.

6. REFERENCIAS

- [1] D. Vázquez-Torres, J. C. Pérez-Arriaga, M. E. Domínguez-Bárcenas, and H. X. Limón-Riaño, "Cybersecurity Strategies for the Digital Inclusion of Older Adults: A Systematic Literature Review," in *Jor. Iberoam. Interac. Hum. Comput.*, 2025, *Interac. Hum-Tecnol. Era Intel. Art.*, 1. México, 2022, pp. 94-105. <http://ricaxcan.uaz.edu.mx/jspui/handle/20.500.11845/4179>
- [2] M. Nedeljko, D. Bogataj, B. Toplak Perović, and B. Miha Kaučič, "Digital literacy during the coronavirus pandemic in older adults: Literature Review and Research Agenda," *IFAC Pap. OnLine*, vol. 55, no. 39, pp. 153-158, Dec. 2022. <https://doi.org/10.1016/j.ifacol.2022.12.027>
- [3] A. Goad, and O. Holmes, "Bridging the digital divide: an evaluation of existing elderly digital literacy education," Dec. 2022. <https://doi.org/10.13140/RG.2.2.32730.62409>
- [4] A. M. Benavides Román, and Y. M. M. Chipana Fernández, "Competencias digitales en adultos mayores y acceso a la justicia: Una revisión sistemática," *Rev. Derecho*, vol. 6, no. 1, pp. 182-194, Apr. 2021. <https://doi.org/10.47712/rd.2021.v6i1.121>
- [5] C. Pérez-Valles, and E. Reeves Huapaya, "Educación inclusiva digital: Una revisión bibliográfica actualizada. Las brechas digitales en la educación inclusiva," *Act. Inv. Educación*, vol. 23, no. 3, pp. 1-23, Sep. 2023. <https://doi.org/10.15517/aie.v23i3.54680>
- [6] I. Bernardino, R. J. Vieira Baptista, J. M. E. B. de Almeida, and J. H. P. Sao Mamede, "Serious Games for seniors: Learning safe behaviors on the web: Position paper," in *2021 16th Iberian Conf. Info. Systems Technol. (CISTI)*, Chaves, Portugal, IEEE, Jun. 2021, pp. 1-4. <https://doi.org/10.23919/CISTI52073.2021.9476310>
- [7] R. Vuorikari, S. Kluzer, and Y. Punie, *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*, Luxembourg: Publications Office of the European Union, 2022. <https://doi.org/10.2760/115376>
- [8] J. Cosgrove, and A. Cechia, *DigComp 3.0: Marco Europeo de Competencias Digitales, 5ª ed.*, Luxemburgo: Asociación Somos Digital, Oficina de Publicaciones de la Unión Europea, 2025. https://somos-digital.org/wp-content/uploads/2026/05/DigComp_3.0_Marco_Europeo_de_Competencias_Digitales_Castellano_V1.pdf

- [9] D. Lindvall, "Cybersecurity Awareness Training: Using ContextBased MicroTraining to teach senior citizens about phishing," Degree thesis, University of Skövde, Skövde, Sweden, 2022. [Online]. Available: <https://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-21979>
- [10] F. Sánchez Vásquez, J. C. Pérez-Arriaga, G. Contreras Vega, S. Luján-Mora, and S. Otón Tortosa, "Towards the Implementation Process of Accessible Virtual Campuses in Higher Education Institutions in Latin America," *Appl. Sci.*, vol. 12, no. 11, p. 5470, May. 2022. <https://doi.org/10.3390/app12115470>
- [11] J. Escobar-Pérez, and Á. Cuervo-Martínez, "Validez de contenido y juicio de expertos: una aproximación a su utilización," *Av. Medición*, vol. 6, no. 1, pp. 27-36, Jan. 2008. https://www.researchgate.net/publication/302438451_Validez_de_contenido_y_juicio_de_expertos_Una_aproximacion_a_su_utilizacion
- [12] J. Nicholson, L. Coventry, and P. Briggs, "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults," in *Proceed. 2019 CHI Conf. Human Fact. Comput. Syst.* Glasgow Scotland Uk: ACM, 2019, p. 349, pp. 1-11. <https://doi.org/10.1145/3290605.3300579>
- [13] C. Noiklueb, S. Boonlue, and D. Srikaew, "Development of Cyber Wellness Assessment Model for Thai elderly population," in *2022 Int. Conf. Digit. Govern. Technol. Innov. (DGTi-CON)*, Bangkok, Thailand, IEEE, 2022, pp. 43-46. <https://doi.org/10.1109/DGTi-CON53875.2022.9849181>
- [14] P. Sannd, and D. M. Cook, "Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks," in *2018 Fourteenth Int. Conf. Info. Process. (ICINPRO)*, Bangalore, India, IEEE, 2018, pp. 1-5. <https://doi.org/10.1109/ICINPRO43533.2018.9096878>
- [15] K. Cerna, and C. Müller, "Fostering digital literacy through a mobile demo-kit development: Co-designing didactic prototypes with older adults," in *Adjunct Publ. 23rd Int. Conf. Mobile Human-Comp. Interact.* Toulouse & Virtual France, ACM, Sep. 2021, p. 3, pp. 1-6. <https://doi.org/10.1145/3447527.3474849>
- [16] A. Quan-Haase, and I. Eluze, "Revisiting the Privacy Paradox: Concerns and Protection Strategies in the Social Media Experiences of Older Adults," in *Proceed. 9th Int. Conf. Social Media Society.* Copenhagen, Denmark, ACM, 2018, pp. 150-159. <https://doi.org/10.1145/3217804.3217907>
- [17] J. Kävrestad, S. Furnell, and M. Nohlberg, "User perception of context-based micro-training – a method for cybersecurity training," *Inf. Security J.*, vol. 33, no. 2, pp. 121-137, 2024. <https://doi.org/10.1080/19393555.2023.2222713>
- [18] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, and S. Furnell, "Evaluation of Contextual and Game-Based Training for Phishing Detection," *Future Internet*, vol. 14, no. 4, p. 114, Mar. 2022. <https://doi.org/10.3390/fi14040104>
- [19] J. Kävrestad, D. Lindvall, and M. Nohlberg, "Combating Digital Exclusion with Cybersecurity Training – An Interview Study with Swedish Seniors," in *Human Aspects of Information Security and Assurance*, S. Furnell and N. Clarke, Eds., Cham: Springer Nature Switzerland, 2023, pp. 3-12. https://doi.org/10.1007/978-3-031-38530-8_1
- [20] A. Schlomann, C. Even, and T. Hammann, "How Older Adults Learn ICT—Guided and Self-Regulated Learning in Individuals with and without Disabilities," *Front. Comput. Sci.*, vol. 3, p. 803740, Jan. 2022. <https://doi.org/10.3389/fcomp.2021.803740>
- [21] K. Cerna, C. Müller, D. Randall, and M. Hunker, "Situated scaffolding for sustainable participatory design: Learning online with older adults," in *Proc. ACM Hum.-Comput. Interact.*, vol. 6, 2022, p. 12, pp. 1-25. <https://doi.org/10.1145/3492831>
- [22] C. I. Martínez-Alcalá et al., "Digital Inclusion in Older Adults: A Comparison Between Face-to-Face and Blended Digital Literacy Workshops," *Front. ICT*, vol. 5, p. 21, Aug. 2018. <https://doi.org/10.3389/fict.2018.00021>
- [23] C. Moret-Tatay, M. J. Beneyto-Arrojo, E. Gutierrez, W. R. Boot, and N. Charness, "A Spanish Adaptation of the Computer and Mobile Device Proficiency Questionnaires (CPQ and MDPO) for Older Adults," *Front. Psychol.*, vol. 10, p. 1165, May. 2019. <https://doi.org/10.3389/fpsyg.2019.01165>
- [24] S. Vrhovec, I. Bernik, D. Fujs, and D. Vavpotič, "Cybersecurity competence of older adult users of mobile devices," in *Europ. Interdisc. Cybersecur. Conf.* Xanthi, Greece, ACM, Jun. 2024, pp. 221-223. <https://doi.org/10.1145/3655693.3656551>
- [25] L. Seeman-Horwitz, R. Bradley Montgomery, S. Lee, and R. Ran "Making content usable for people with cognitive and learning disabilities," World Wide Web Consortium (W3C), Cambridge, Massachusetts, Apr. 29, 2021. [Online]. Available: <https://www.w3.org/TR/coga-usable/>
- [26] P. Ghadamighalandari et al., "Mediating digital security: Participatory learning with older adults in smartphone café sessions," in *Proceed. 19th Particip. Des. Conf. 2026, Vol. 1: Full Papers (PDC '26)*. New York, NY, USA, Association for Computing Machinery, 2026, pp. 74-88.

- <https://doi.org/10.1145/3796624.3796644>
- [27] S. Nti Berko, and L. A. Odozor, "Designing Age-Inclusive Cybersecurity: Enhancing Protection for Older Adults in Digital Environments," *Int. J. Innovat. Sci. Res. Technol.*, vol. 10, no. 9, pp. 1616-1628, Sep. 2025. <https://doi.org/10.38124/ijisrt/25sep709>
- [28] 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, pp. 19911-19932, Sep. 2025. <https://doi.org/10.1007/s10639-025-13564-y>

CONFLICTO DE INTERÉS

Los autores declaran no tener conflictos de interés.

CONTRIBUCIÓN DE AUTORÍA

Dayhan Vázquez-Torres: Investigación, escritura del borrador original, recopilación y gestión de datos, visualización, escritura (revisión y edición).

Juan Carlos Pérez-Arriaga: conceptualización, metodología, escritura del borrador original, escritura (revisión y edición), supervisión.

Martha Elizabet Domínguez-Bárcenas: Metodología, escritura (revisión y edición), supervisión.

Xavier Limón: Metodología, escritura (revisión y edición), supervisión.