



Propiedades psicométricas de escalas y cuestionarios para medir la seguridad digital universitaria

Psychometric properties of scales and questionnaires for measuring digital safety in university students

Bohen G. Solís T.

Universidad de Panamá. Centro Regional Universitario de Coclé. Panamá.
bohen.solis@up.ac.pa, <https://orcid.org/0000-0002-2159-3584>

James Bermúdez-Vargas

Universidad de Panamá. Centro Regional Universitario de Coclé. Panamá.
james.bermudez@up.ac.pa, <https://orcid.org/0000-0001-8943-6430>

Dayalis Vargas

Universidad de Panamá, Centro Regional Universitario de Coclé, Panamá
dayalis.vargas@up.ac.pa, <https://orcid.org/0009-0009-8640-2660>

***Autor de correspondencia:** bohen.solis@up.ac.pa

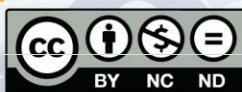
Fecha de recepción: 02/06/2026

Fecha de aceptación: 20/08/2026

DOI: <https://doi.org/10.48204/synergia.v5n2.11565>

Resumen

La rápida transformación de los contextos social, académica y profesional ha promovido un aumento importante en los peligros relacionados con la seguridad digital. En este sentido, es fundamental tener instrumentos diseñados de manera rigurosa que posibiliten la medición de esas competencias con fiabilidad y validez. Por lo tanto, este estudio tiene como objetivo llevar a cabo un análisis sistemático de publicaciones científicas que estén vinculadas con la creación, el desarrollo y la validación psicométrica de cuestionarios, escalas u otros instrumentos destinados al análisis de la seguridad digital, con la finalidad de contribuir con fundamentos sólidos para el diseño o la modificación de herramientas que estén contextualizadas en la educación superior. La revisión de la literatura se realizó utilizando la metodología PRISMA a través de Google Académico y EBSCO. Se restringió a publicaciones de entre 2020 y 2025. Al principio, se identificaron 179 fuentes; de ellas, se examinaron nueve: ocho artículos originales y una tesis de licenciatura. Entre los hallazgos más relevantes, el 66.7 % de los estudios emplearon alfa de Cronbach como principal medida de consistencia interna; el 33.3 %, análisis factorial confirmatorio como técnica de validación; y el 22.2 %, omega de McDonald como un método extra para medir la fiabilidad. En términos geográficos, Asia abarcó el 33.3 % de las investigaciones, luego Europa y América, con un 22.2 % cada una. Además, se observó una





limitada representación latinoamericana, ya que el 88.9 % de las publicaciones estaba en inglés y solo el 11.1 % en español.

Palabras clave: digitalización, psicometría, evaluación de la educación, validez, fiabilidad, seguridad digital.

Abstract

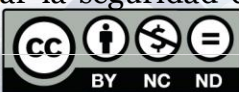
The rapid transformation of social, academic, and professional contexts has led to a significant increase in dangers related to digital security. In this regard, it is essential to have rigorously designed instruments that enable the reliable and valid measurement of these competencies. Therefore, this study aims to conduct a systematic analysis of scientific publications related to the creation, development, and psychometric validation of questionnaires, scales, and other instruments for digital security analysis, in order to contribute a solid foundation for the design or modification of tools contextualized within higher education. The literature review was conducted using the PRISMA methodology through Google Scholar and EBSCO. It was restricted to publications from 2020 to 2025. Initially, 179 sources were identified; of these, nine were examined: eight original articles and one undergraduate thesis. Among the most relevant findings, 66.7% of the studies used Cronbach's alpha as the main measure of internal consistency; 33.3% used confirmatory factor analysis as a validation technique; and 22.2% used McDonald's omega as an additional method for measuring reliability. Geographically, Asia accounted for 33.3% of the research, followed by Europe and the Americas, each with 22.2%. Furthermore, Latin American representation was limited, as 88.9% of the publications were in English and only 11.1% in Spanish.

Keywords: digitization, psychometrics, educational evaluation, validity, reliability, digital security.

Introducción

En la actualidad la transformación digital ha reconceptualizado las fronteras del aprendizaje y la gestión académica de nuestros estudiantes universitarios, donde aprenden, se comunican y construyen una identidad profesional a través de ambientes digitales. Sin embargo, esa misma conectividad que amplía oportunidades también nos hace vulnerables a muchos peligros. El robo de identidad, fraudes electrónicos, ciberacoso, malware y violaciones de privacidad ya no son riesgos abstractos; como señalan Kraiwanit et al. (2025) y Ma et al. (2025), sino que se han convertido en amenazas concretas que afectan diariamente a las personas con mayor tiempo de conexión. Bajo esta premisa, la seguridad digital deja de ser una opción teórica, para transformarse en una necesidad en el entorno universitario.

La creciente relevancia de los riesgos informáticos ha impulsado a la comunidad académica a integrar la seguridad digital como una dimensión fundamental, dentro de los marcos de la





competencia digital. Los estándares DigComp 2.0 y 2.1 de la Comisión Europea, los cuales sentaron las bases para medir y certificar habilidades digitales, han sido los referentes más utilizados para estructurar este debate, tanto en investigación como en la praxis educativa (Abubakari et al., 2023; Ma et al., 2025). Su influencia es innegable. Sin embargo, la existencia de un marco conceptual sólido no asegura que los instrumentos de evaluación derivados posean fiabilidad y solidez métrica.

Precisamente, es aquí donde radica el problema; en una significativa variabilidad en los instrumentos utilizados para evaluar la seguridad digital, los mismos difieren en el número de ítems, las escalas de respuesta, los constructos que priorizan y los enfoques de validación psicométrica que emplean. Por lo que, un diseño deficiente o una validación insuficiente no constituyen un problema técnico menor, pero pueden traer consigo diagnósticos erróneos, con intervenciones educativas desconectadas de la realidad estudiantil universitaria y en última instancia, una falsa percepción de seguridad de un riesgo que permanece latente.

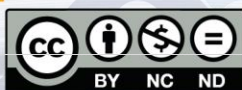
El objetivo principal de este artículo es analizar de manera sistemática las publicaciones científicas vinculadas a la creación, desarrollo y validación psicométrica de los instrumentos utilizados en la evaluación de la seguridad digital para estudiantes universitarios, divulgadas entre 2020 y 2025. Además, se busca identificar las prácticas metodológicas predominantes, los constructos más evaluados y las brechas que aún persisten en la literatura actual.

A través de este artículo de revisión sistemática se busca responder a las siguientes preguntas fundamentales. En primer lugar, ¿cuál es el estado actual de la validación psicométrica de los instrumentos de seguridad digital elaborado para los estudiantes universitarios?, también, ¿qué dimensiones de seguridad se evalúan con mayor frecuencia en las publicaciones científicas?, y ¿qué limitaciones metodológicas y vacíos teóricos presentan los instrumentos de seguridad digital disponible en la actualidad según la metodología PRISMA?

Materiales y métodos

Tabla 1.

Materiales y recursos utilizados





Material	Descripción
Computadora	Procesador Intel Core i7 (12 ^a generación o superior) o AMD Ryzen 7 (serie 5000 o superior). Mínimo, 16 GB DDR4 o DDR5 de memoria RAM, disco duro o disco de estado sólido de mínimo 512 GB. Pantalla Full HD (1920x1080) o superior, 15.6". Conexión a internet por cable o inalámbrico.
Bases de datos académicas	EBSCO: proveedor de bases de datos de investigación, revistas electrónicas, libros y tecnología para bibliotecas. Google Scholar: motor de búsqueda sin costo enfocado en la literatura académica y científica, creado para encontrar libros, tesis, artículos, patentes, resúmenes e informes técnicos de varios campos.
Software de procesador de texto, Microsoft Word	Word de Office 365 (Microsoft 365) o Word 2016, en adelante.
Software gestor de base de datos, Mendeley	Mendeley 2.142.0.
Método de selección PRISMA	Declaración de PRISMA 2020
Descriptores, palabras claves y operadores booleanos	AND, OR, Seguridad digital, estudiantes universitarios, educación superior, Higher education, diseño de instrumentos, Instrument design, Instrument validation, scale development, questionnaire validation.

Para el desarrollo de esta revisión se utilizaron las herramientas detalladas en la Tabla 1.

Se ajustaron los parámetros de PRISMA, de acuerdo a Page et al. (2021), como método para elegir la literatura empleada en la determinación del estado actual del arte vinculado con el tema central de la revisión, que es instrumentos de evaluación de la seguridad digital en estudiantes universitarios.

Las bases de datos académicas que se usaron para llevar a cabo la revisión de la literatura, que tuvo lugar en febrero de 2026, fueron EBSCO y Google Scholar.

En el proceso de búsqueda, para analizar correctamente las publicaciones encontradas, se implementó el uso de descriptores o palabras clave que, al combinarse con los operadores booleanos AND, OR y NOT, posibilitaron la creación de una estrategia de búsqueda en las diferentes fuentes consultadas. Asimismo, se utilizaron las opciones de exportación que ofrecen las bases de datos empleadas.

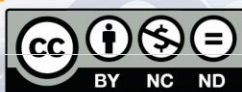


Tabla 2.*Estrategia de búsqueda*

Cadena de búsqueda utilizada en Google Scholar	Cadena de búsqueda utilizada en EBSCO
("seguridad digital" OR "digital safety") AND ("estudiantes universitarios" OR "educación superior" OR "university students" OR "higher education") AND ("instrument validation" OR "scale development" OR "questionnaire validation" OR "psychometric validation" OR "validación de instrumento")	TX ("seguridad digital" OR "digital safety") AND TX ("estudiantes universitarios" OR "educación superior" OR "university students" OR "higher education") AND TX ("diseño de instrumento" OR "validación de instrumento" OR "instrument validation" OR "scale development" OR "questionnaire validation" OR "psychometric validation")

Nota. Se presentan las cadenas de búsqueda utilizadas en Google Scholar y EBSCO para la identificación de publicaciones relacionadas con seguridad digital y validación de instrumentos. Los operadores booleanos AND y OR se emplearon para combinar y delimitar los términos de búsqueda.

Tabla 3.*Lista de Bases de datos consultadas*

Nombre	Dirección	Cantidad de artículos encontrados
Google Scholar	https://scholar.google.com/	164
EBSCO	https://www.ebsco.com/es	15

Nota. Se presentan las bases de datos consultadas durante el proceso de búsqueda bibliográfica y la cantidad de artículos identificados en cada una. En total, se localizaron 179 publicaciones, de las cuales 164 correspondieron a Google Scholar y 15 a EBSCO.

En la tabla 3 se aprecian las diferentes bases de datos académicas consultadas, su dirección URL, y la cantidad de artículos obtenidos de cada una.

El proceso de búsqueda arrojó un total de 179 artículos, 164 de Google Scholar y 15 de EBSCO. Además, se establecieron los criterios de inclusión y exclusión a los cuales se someterá la literatura encontrada, con el fin de identificar las publicaciones académicas que contengan información relevante relacionada al tema principal.

Tabla 4.
Criterios de inclusión y exclusión

Criterios de inclusión	
Criterio	Criterio de inclusión
Tema	La literatura debe abordar temas relacionados a instrumentos de evaluación de seguridad digital en estudiantes universitarios que incluyan procesos de validación de instrumento, desarrollo de escala, validación psicométrica y validación de cuestionario
Longitud	Los documentos deben tener 6 o más páginas.
Fecha de publicación	La literatura debe haber sido publicada entre 2020 – 2025.
Idioma	Los documentos deben estar escritos en español e inglés.
Disponibilidad	Los documentos deben ser de acceso abierto.
Criterios de exclusión	
Artículos duplicados.	
Documentos cuyo contenido completo no sea accesible.	
Estudios que utilicen un cuestionario sin proceso formal de validación, no reporten propiedades psicométricas y solo describan percepciones sin instrumento estructurado.	
Escritos sobre instrumentos de seguridad digital en educación básica o secundaria, docentes únicamente (sin incluir estudiantes) y contexto empresarial o corporativo.	

Nota: En la tabla 4 se detallan los criterios aplicados en el proceso de revisión.

Figura 1.

Diagrama de flujo del proceso de selección de la literatura para la revisión aplicando las recomendaciones de PRISMA 2020.

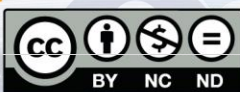


Nota. El diagrama muestra el proceso de identificación, cribado, evaluación de elegibilidad e inclusión de los estudios considerados en la revisión. De los 179 registros inicialmente identificados, se incluyeron finalmente 9 estudios.

Se inició comparando los registros obtenidos con el objetivo de eliminar aquellos que estuviesen duplicados. De los 179 registros encontrados, se descartó 3, quedando un total de 176 registros para la revisión. Seguidamente se revisó el título, objetivos, resumen, hallazgos y conclusiones de los documentos restantes, de estos, 146 fueron excluidos debido a que no contenían información relacionada al tema.

Posteriormente se procedió a realizar la revisión de los 30 artículos aplicando los criterios de inclusión y exclusión establecidos previamente. Quedando un total de 9 documentos, los cuales se utilizaron para el desarrollo del artículo propuesto.

Resultados y discusión



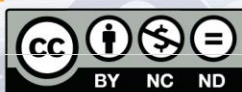


Para este artículo de revisión sistemática 9 publicaciones fueron seleccionados y revisados. La figura 1, muestra el diagrama de flujo del proceso de selección de la literatura aplicando los parámetros adaptados de PRISMA.

Tabla 5

Hallazgos principales de las publicaciones seleccionadas

Autor / Año	Título	País idioma	/ Principales Resultados
(Abubakari et al., 2023)	Validating the Digital Competence (Dig-Comp 2.1) Framework in Higher Education Using Confirmatory Factor Analysis: Non-Western Perspective	Uganda Inglés	/ Cuestionario de 30 ítems. Se realizó análisis Factorial Confirmatorio (CFA) y Análisis Compuesto Confirmatorio (CCA), mostrando una validez de 0.50 y alfa de Cronbach general fue de 0.959, con valores específicos por constructo entre 0.854 y 0.873
(Cabero-Almenara et al., 2024)	Technological and Sustainable Security: A Longitudinal Study on Teacher Training	España Inglés	/ Cuestionario de 14 ítems. La validación fue realizada mediante un Análisis Factorial Confirmatorio (CFA) con índices de ajuste adecuados (GFI: .875; NFI: .753) y con relación a la confiabilidad se utilizó Alfa de Cronbach (0.979), Omega de McDonald (0.981) y Confiabilidad Compuesta (0.979).
(Gewirtz-Meydan et al., 2025)	One Group or Many? Identifying Distinct Profiles of Adolescents Involved in Image-Based Sexual Abuse	Estados Unidos Inglés	/ Se usó la escala IBSA y elementos del "Cuestionario de Victimización Juvenil". La validación de la Escala IBSA cuenta con validación psicométrica detallada en publicaciones de los mismos autores. En cuanto a la confiabilidad, se aplicó el análisis de perfiles latentes (LPA) para identificar grupos, asegurando que los perfiles estuvieran bien separados





				con una puntuación de entropía de 0.84.
(Gümüş et al., 2023)	Investigation of pre-service teachers' sensitivity to cyberbullying, perceptions of digital ethics and awareness of digital data security	Turquía Inglés	/	Cuestionario compuesto de 73 ítems. Las confiabilidades medidas por Alfa de Cronbach fueron 0.71 para sensibilidad al ciberacoso, 0.64 para ética TIC y 0.91 para seguridad de datos
(Kraiwanit et al., 2025)	Predictors of Digital Fraud: Evidence from Thailand	Tailandia Inglés	/	Se realizó un proceso de validación de contenido y una prueba piloto con 30 participantes. En cuanto a la confiabilidad, se evaluó mediante el coeficiente Alfa de Cronbach, el cual arrojó un valor de 0.896
(Ma et al., 2025)	The Impact of Digital Safety Competence on Cognitive Competence, AI Self-Efficacy, and Character	Hong Kong Inglés	/	Cuestionario- Escala con 25 ítems. Se empleó CFA para confirmar la estructura factorial. La confiabilidad (alfa de Cronbach) fue de 0.81 para seguridad digital y 0.73 para competencia cognitiva
(Mieg et al., 2024)	Short digital-competence test based on DigComp2.1: Does digital competence support research competence in undergraduate students?	Alemania Inglés	/	Escala de 10 ítems, pero solo 2 dedicados a seguridad digital. Se reportó un Alfa de Cronbach de 0.87 y un Omega de McDonald de 0.88
(Santamaria, 2025)	Implementación de un programa de concientización en ciberseguridad para estudiantes de la Universidad Nacional Pedro Ruiz Gallo: un enfoque basado en ISO/IEC 27001: 2022 y NIST CSF 2.0	Perú Español	/	Cuestionario de 23 ítems. Evalúa dimensiones como protección de dispositivos, gestión de contraseñas y comportamiento en redes sociales. En cuanto a la validación se hizo mediante juicio de expertos y se utilizó el coeficiente Alfa de Cronbach, obteniendo un valor de 0.831 en el pre-test (confiabilidad alta) y 0.918 en el post-test (confiabilidad muy alta)



(Shah, 2025)	Cross-Cultural Examination of Cyberbullying and Cybervictimization among University Students in India and Africa: Gender, Platform, and Behavioral Disparities	India / Inglés	Cuestionario de 86 ítems. El autor escribe que los cuestionarios están estandarizados.
--------------	--	----------------	--

Nota: Resumen de los artículos se presenta en la tabla 5. Los artículos seleccionados fueron publicados en el período comprendido entre el 2020 y 2025.

A continuación, se presenta los resultados relevantes de cada una de las publicaciones seleccionadas, después de aplicar la metodología PRISMA.

En el artículo de Abubakari et al. (2023), se muestra una investigación piloto que tiene como objetivo verificar el Marco de Competencia Digital (DigComp 2.1) en el sistema educativo superior ugandés. La investigación se origina por la necesidad de tener instrumentos confiables para evaluar en naciones en desarrollo, porque la mayor parte de los marcos que ya existen están enfocados en contextos occidentales. Los autores corroboraron la consistencia y validez del instrumento para evaluar las habilidades tecnológicas a través de un análisis cuantitativo realizado en estudiantes universitarios.

El artículo destaca las dimensiones que posee el instrumento, las cuales son:

Figura 2.

Esquema de dimensiones del instrumento por el autor Abubakari et al. (2023)



Nota. El esquema representa las cinco dimensiones consideradas en el instrumento: alfabetización informacional y de datos (IDL), comunicación y colaboración (CC), creación de contenido digital (DCD), seguridad digital (SD) y resolución de problemas digitales (DPS).

La dimensión de Seguridad digital (SD), se refiere a la capacidad para utilizar las herramientas digitales de forma segura. En esta dimensión el artículo menciona que consta de 6 ítems, denominados con los códigos DS1, DS2, DS3, DS4, DS5 y DS6, sin embargo, no se presenta el instrumento. Los autores realizaron, para la validación del cuestionario, dos enfoques estadísticos principales que son el análisis Factorial Confirmatorio (AFC) y Análisis Compuesto Confirmatorio (ACC), en cuanto a confiabilidad, se menciona la realización de Alfa de Cronbach (CA) y la fiabilidad Compuesta (CR).

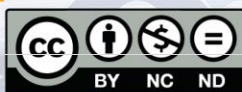
En el artículo de Cabero-Almenara et al. (2024), se destaca el uso de un cuestionario que consta de 14 ítems en total, evaluados con una escala Likert de 8 puntos. Estos ítems se agrupan en cuatro áreas o propósitos principales, conocimiento del impacto ambiental (Ítems 1-5), aplicación práctica en la enseñanza (Ítems 6-7), capacidad de identificación y reducción (Ítems 8-10) y habilidades de formación (Ítems 11-14). En relación con la confiabilidad, este instrumento fue sometido a Alfa de Cronbach, Omega de McDonald y fiabilidad Compuesta (CR). Por otro lado, se realizó la validación mediante un Análisis Factorial Confirmatorio (AFC) para verificar la estructura del modelo con los nuevos datos. Cabe señalar que el instrumento no está orientado específicamente a la seguridad digital; sin embargo, aborda estos aspectos desde una perspectiva de sostenibilidad y responsabilidad ambiental.



Para los autores Gewirtz-Meydan et al. (2025), en el artículo One Group or Many? Identifying Distinct Profiles of Adolescents Involved in Image-Based Sexual Abuse, se emplea una variedad de instrumentos y constructos para reconocer perfiles de jóvenes a partir de 18 años, que participan en el abuso sexual basado en imágenes (IBSA), en este análisis solo se mencionará los instrumentos que tengan relación con el tema del artículo que se realiza, la dimensión de abuso Sexual basado en imágenes (IBSA), que consta de 6 ítems que representan dimensiones distintas como toma o creación no consensuada, intercambio de imágenes no consensuado, reclutamiento forzado de imágenes (coerción), amenaza de compartir (sextorsión), intercambio de imágenes de producción propia con alguien mucho mayor y explotación sexual comercial. Otro factor es el de Conductas de Riesgo en Línea, en el que se analizaron 5 conductas específicas por separado que son ciberacoso, pretender ser otra persona, encontrarse en persona con extraños conocidos en línea, visitar sitios pornográficos y enviar imágenes o videos sexuales de uno mismo. El artículo no menciona un proceso de confiabilidad, sino a la entropía e índices de ajuste del modelo.

Otro de los artículos seleccionados pertenece a Gümüş et al. (2023), quienes mencionan el uso de tres escalas para medir variables en un grupo de docentes en formación dentro de la universidad. La primera escala mencionada en la publicación es la escala de Sensibilidad al Ciberbullying, solo tiene un factor, compuesto por 13 ítems, otra escala empleada es la de Ética en el Uso de las Tecnologías de la Información y la Comunicación, que contiene 4 dimensiones principales que son Exactitud (referente a la veracidad de la información), Efectos sociales de las TIC, Propiedad Intelectual y Confianza (Seguridad y fiabilidad en el uso), en total esta escala tiene 28 ítems, y por último se empleó la Escala de Conciencia sobre la Seguridad de los Datos Digitales, con un solo factor, de 32 ítems.

En la publicación de Kraiwanit et al. (2025), Predictors of Digital Fraud: Evidence from Thailand, se utilizó un cuestionario estructurado con cinco secciones principales que son información demográfica, comportamiento digital, beneficios percibidos de las transacciones digitales, características percibidas de seguridad digital y experiencia con el fraude digital: Historial de victimización y pérdida financiera. La consistencia interna del instrumento se midió mediante el coeficiente alfa de Cronbach, mientras que la validación se realizó a través de validación de contenido (fundamentación teórica, adaptación contextual, selección de



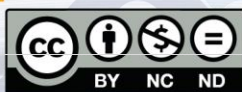


variables y la prueba piloto), prueba Ómnibus de Coeficientes del Modelo y R-cuadrado de Nagelkerke.

En la investigación de Ma et al. (2025), se adoptó una escala desarrollada por Skov (2016), basada en el marco DigComp 2.0 de la Comisión Europea, y constó de 14 ítem. La consistencia interna de las escalas se midió principalmente mediante el Alfa de Cronbach y la validación fue realizada a través de Análisis Factorial Confirmatorio (AFC) y Modelado de Ecuaciones Estructurales (SEM). Este artículo destaca y demuestra la importancia de la seguridad digital, como una habilidad esencial para navegar de manera responsable y efectiva en una sociedad impulsada por la IA.

En la obra que se cita de Santamaria (2025), con título Implementación de un programa de concientización en ciberseguridad para estudiantes de la Universidad Nacional Pedro Ruiz Gallo: un enfoque basado en ISO/IEC 27001: 2022 y NIST CSF 2.0, un trabajo de graduación de pre-grado, se elaboró un cuestionario que se denominó nivel de concienciación en ciberseguridad. Este instrumento constó de 23 ítems, que se agruparon en las siguientes dimensiones, Seguridad y Protección de Dispositivos, gestión de Contraseñas y seguridad de la información, comportamiento en línea y uso de Redes Sociales. La consistencia interna del cuestionario se determinó mediante el coeficiente Alfa de Cronbach, mientras que la validación fue realizada empleando juicio de expertos consultados, entre los que se encuentran ingenieros y doctores. Cabe señalar que para el diseño del instrumento se utilizó deferentes teorías, como lo son la teoría de la motivación de protección (PMT) y el modelo de aceptación tecnológica (TAM).

En la última fuente analizada de Shah (2025), se encontró que este estudio empleó una combinación de tres cuestionarios estandarizados que miden dos dimensiones que son ciberacoso (frecuencia con la que el sujeto realiza conductas agresivas en línea) y cibervictimización (frecuencia con la que el sujeto es el objeto de agresiones). El artículo no menciona alguna prueba estadística que se realiza a la confiabilidad, sin embargo, menciona el uso de esos instrumentos estandarizados, y algo muy importante fue el hecho de que para obtener los resultados se tuvo una demora a la hora de contestar algunos ítems del instrumento, quizás producto de la calidad y precisión de la respuesta.



En relación a la procedencia geográfica de los nueve estudios elegidos, se observó una distribución internacional desigual, siendo el continente asiático el que más predominaba. En particular, el 33.3% del total de la muestra corresponde a tres investigaciones ubicadas en Asia: Hong Kong, India y Tailandia. En Europa, se llevaron a cabo dos investigaciones (22.2%) provenientes de Alemania y España. También contribuyó el continente americano con dos investigaciones provenientes de Estados Unidos y Perú (22.2%). Un estudio realizado en Uganda (11,1%) representó a África. Se encontró también un estudio que se desarrolló en Turquía (11.1%), una nación que, geográficamente, está influenciada por Europa y Asia a la vez. Estos hallazgos muestran que en el corpus estudiado se observa una representación escasa de América Latina y África, mientras que las investigaciones en contextos europeos y asiáticos son más frecuentes.

Tabla 6

Distribución geográfica de las publicaciones analizadas según región

Región	Cantidad de estudios
África	1
América	2
Asia	3
Europa	2
Euroasiático	1
Total	9

Nota. La tabla presenta la distribución geográfica de las publicaciones analizadas según la región de procedencia de los estudios.

Como podemos observar en la Tabla 6, la clasificación regional se realizó con base en la ubicación geográfica del país de desarrollo de las publicaciones, entre el 2020 y 2025, y se constató una notable prevalencia del inglés como lengua científica en lo que respecta a la distribución de publicaciones por idioma.

También se corroboró el dominio del inglés como lengua para la divulgación científica en estudios vinculados a la seguridad digital y la ética digital. Sin embargo, la escasa cantidad de investigaciones en español indica que hay una brecha en la producción académica regional, especialmente en América Latina, lo que podría restringir el acceso y la visibilidad del conocimiento en este contexto.

Tabla 7.*Distribución de publicaciones por idioma*

Idioma de Pub.	Cantidad
Inglés	8
Español	1

Nota. La tabla presenta la distribución de las publicaciones según el idioma, evidenciándose un predominio de estudios publicados en inglés.

La tabla 7 nos muestra que de los nueve estudios analizados, ocho (88.9%) se publicaron en inglés y solo uno (11.1%) en español; este último fue realizado en Perú.

La prueba de alfa de Cronbach fue el estadístico más utilizado en las publicaciones analizadas para evaluar la consistencia interna de los instrumentos. Los estudios demuestran valores elevados, que por lo general son mayores a 0.70 o 0.80, en las siguientes publicaciones (Cabero-Almenara et al., 2024), (Santamaria, 2025), (Abubakari et al., 2023), (Kraiwanit et al., 2025), (Ma et al., 2025) y (Gümüş et al., 2023).

Con relación a la validación, en los artículos de Cabero-Almenara et al. (2024), Ma et al. (2025), Abubakari et al. (2023), se evidencia que la técnica empleada es el Análisis Factorial Confirmatorio y en otras publicaciones como la de Santamaria (2025) y Kraiwanit et al. (2025) fue el análisis de expertos.

Las diferencias entre las publicaciones revisadas surgen producto de la complejidad de los modelos utilizados, por ejemplo, el uso de la entropía, para validar la separación y precisión de perfiles latentes en lugar de una escala de consistencia y otro estudio, evidencia el uso de la prueba de McDonald como alternativa adicional al Alfa de Cronbach.

Los resultados muestran que es necesario crear y validar instrumentos de seguridad digital adaptadas al entorno universitario. La escasa producción en español y en América Latina, además de la variedad de procedimientos de validación, indica que es relevante definir criterios metodológicos más homogéneos y culturalmente apropiados. Los hallazgos pueden guiar



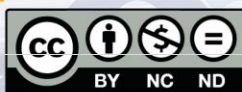
investigaciones futuras para la creación y adaptación de instrumentos confiables en la educación superior.

Conclusiones

La evaluación de los estudios seleccionados a través de PRISMA 2020 muestra una gran variedad en los instrumentos y procedimientos empleados para analizar la seguridad digital. A pesar de que algunos trabajos se basan en marcos como DigComp, hay variaciones en el número de ítems, dimensiones y grados de transparencia. El análisis factorial confirmatorio, SEM y coeficientes de fiabilidad como el alfa de Cronbach y Omega son los métodos más utilizados, sin embargo, no todos los estudios llevan a cabo procesos integrales de validación. Se percibe, además, una variedad conceptual, dado que la seguridad digital se trata desde las habilidades técnicas, de prevención de riesgos, éticas y conductuales. En términos geográficos, los estudios en inglés y en idioma asiático son los más comunes, mientras que la representación de América Latina, África y las publicaciones en español es escasa. Por ende, se sugiere llevar a cabo investigaciones contextualizadas e instrumentos accesibles, así como protocolos de validación estandarizados que promuevan la capacidad de replicar. Además, para robustecer la seguridad digital en la educación superior, son fundamentales las políticas institucionales, la alfabetización digital y la formación de los docentes.

Referencias

- Abubakari, M., Nasir, G., Musa, J., & Kalinaki, K. (2023). Validating the Digital Competence (Dig-Comp 2.1) Framework in Higher Education Using Confirmatory Factor Analysis: Non-Western Perspective. *Canadian Journal of Educational and Social Studies*, 3(6), 15–26. <https://doi.org/10.53103/cjess.v3i6.184>
- Cabero-Almenara, J., Barragán-Sánchez, R., Llorente-Cejudo, C., & Palacios-Rodríguez, A. (2024). Technological and Sustainable Security: A Longitudinal Study on Teacher Training. *Computers in the Schools*, 41(3), 263–280. <https://doi.org/10.1080/07380569.2024.2381717>
- Gewirtz-Meydan, A., Mitchell, K. J., O'Brien, J. E., & Colburn, D. A. (2025). One Group or Many? Identifying Distinct Profiles of Adolescents Involved in Image-Based Sexual Abuse. *Journal of Interpersonal Violence*. <https://doi.org/10.1177/08862605251393734>
- Gümüş, M. M., Çakır, R., & Korkmaz, Ö. (2023). Investigation of pre-service teachers' sensitivity to cyberbullying, perceptions of digital ethics and awareness of digital data security. *Education and Information Technologies*, 28(11), 14399–14421. <https://doi.org/10.1007/s10639-023-11785-7>





- Kraiwanit, T., Limna, P., Sonsuphap, R., & Chutipat, V. (2025). Predictors of Digital Fraud: Evidence from Thailand. *Journal of Risk and Financial Management*, 18(12). <https://doi.org/10.3390/jrfm18120671>
- Ma, C. M. S., Shek, D. T. L., Fan, I. Y. H., Zhu, X., & Hu, X. (2025). The Impact of Digital Safety Competence on Cognitive Competence, AI Self-Efficacy, and Character. *Applied Sciences (Switzerland)*, 15(10). <https://doi.org/10.3390/app15105440>
- Mieg, H. A., Klieme, K. E., Barker, E., Bryan, J., Gibson, C., Haberstroh, S., Odebiyi, F., Rismondo, F. P., Römmer-Nossek, B., Thiem, J., & Unterpertinger, E. (2024). Short digital-competence test based on DigComp2.1: Does digital competence support research competence in undergraduate students? *Education and Information Technologies*, 29(1), 139–160. <https://doi.org/10.1007/s10639-023-12251-0>
- Santamaria, S. (2025). *Implementación de un programa de concientización en ciberseguridad para estudiantes de la Universidad Nacional Pedro Ruiz Gallo: un enfoque basado en ISO/IEC 27001: 2022 y NIST CSF 2.0*. [Tesis de licenciatura, Universidad Nacional Pedro Ruiz Gallo]. Repositorio Institucional de la Universidad Nacional Pedro Ruiz Gallo.
- Shah, K. (2025). Cross-Cultural Examination of Cyberbullying and Cybervictimization among University Students in India and Africa: Gender, Platform, and Behavioral Disparities. *International Journal for Research in Applied Science and Engineering Technology*, 13(11), 2715–2725. <https://doi.org/10.22214/ijraset.2025.75887>