REVISTA INTERNACIONAL
TECNOLÓGICA – EDUCATIVA DOCENTES 2.0
ISSN: 2665-0266 / ISNI: 0000 0005 0409 1664 / RINGGOLD ID 608948.
VOL. 18 (1), MAYO 2025 | https://doi.org/10.37843/rted.v18i1.632

RTED Resiliencia Paradigmática

Evaluación de la Competencia Digital de Seguridad en Estudiantes de una Universidad del Centro del Perú

Assessment of Digital Security Competence in University Students from Central Peru

Jhon Richard Orosco-Fabian[1], Rocío Pomasunco-Huaytalla[2], Wilfredo Gómez-Galindo[3] y Aracely Milagros Rosales-Puchoc[4]

EDICIÓN: RTED Resiliencia Paradigmática

Recibido: 8/diciembre/2024
Aceptado: 12/mayo/2025
Publicado: 29/mayo/2025

Páginas: desde 472-486

País
[1]Perú
[2]Perú
[3]Perú
[4]Perú

Institución
[1234]Universidad Nacional del Centro del Perú

Correo Eletrónico
[1]jorosco@uncp.edu.pe
[2]rpomasunco@uncp.edu.pe
[3]wgomez@uncp.edu.pe
[4]arosales@uncp.edu.pe

ORCID
[1]https://orcid.org/0000-0001-9035-706X
[2]https://orcid.org/0000-0002-8656-1479
[3]https://orcid.org/0000-0002-9946-0538
[4]https://orcid.org/0000-0002-3963-1593

Citar así: APA / IEEE

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

J. Orosco-Fabian, R. Pomasunco-Huaytalla, W. Gómez-Galindo y A. Rosales-Puchoc, "Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba", RTED, vol. 18, n.°1, pp. 472-486, may. 2025.

Resumen

El contexto actual, impactado por las Tecnologías de Información y Comunicación requiere profesionales con competencias digitales sólidamente desarrolladas en su campo. Por tanto, es necesario evaluar estas competencias, pero con instrumentos pertinentes. El objetivo de la investigación fue diseñar y validar una prueba para evaluar la competencia digital de seguridad en estudiantes universitarios, en los ámbitos de conocimiento, capacidad y actitud. La investigación se fundamentó bajo el método hipotético-deductivo, paradigma positivista, enfoque cuantitativo, con diseño no experimental, de tipo descriptivo, y de corte transversal. En el estudio participaron 269 estudiantes de pregrado de las carreras profesionales de administración hotelera y turismo, administración de negocios e ingeniería agroindustrial de una universidad pública del centro del Perú. Si bien los resultados indican que los ítems de la prueba discriminan de manera adecuada (46%), se observa una falta de equilibrio, ya que predominan las preguntas de nivel fácil (67%); en cuanto a la fiabilidad, la prueba es adecuada para el propósito que fue elaborada (0.70, 0.81) y el análisis factorial evidencia dos factores a ser evaluados (factor 1: ámbito actitudinal, factor 2: ámbito de conocimiento y capacidad). En conclusión, la prueba sobre competencia digital de seguridad presenta adecuadas propiedades psicométricas, por lo tanto, puede ser utilizado con estudiantes universitarios.

Palabras clave: Tecnologías de la información, competencia, seguridad de la información, seguridad informática, estudiantes universitarios.

Abstract

The current context, impacted by Information and Communication Technologies, requires professionals with solidly developed digital competencies. Therefore, it is necessary to assess these competencies with relevant instruments. This research aimed to design and validate a test to assess digital security competency in university students in terms of knowledge, ability, and attitude. The research was based on the hypothetico-deductive method, a positivist paradigm, a quantitative approach, and a non-experimental, descriptive, and cross-sectional design. The study involved 269 undergraduate students from the professional programs of hotel and tourism management, business administration, and agroindustrial engineering at a public university in central Peru. While the results indicate that the test items provide adequate discrimination (46%), a lack of balance is observed, as easy-level questions predominate (67%). Regarding reliability, the test is adequate for its intended purpose (0.70, 0.81), and the factor analysis reveals two factors to be evaluated (factor 1: attitudinal domain; factor 2: knowledge and ability domain). In conclusion, the digital security competency test has adequate psychometric properties and can be used with university students.

Keywords: Information technology, competence, information security, computer security, college students.

D.L:LA2017000128 / ISSN: 2665-0266 / Ringgold ID:608948
ISNI: 0000 0005 0409 1664
Mayo 2025 - Volumen 18, Número 1 , Ejemplar No. 40.

Introducción

El contexto actual, impactado por las Tecnologías de Información y Comunicación requiere profesionales con competencias digitales sólidamente desarrolladas en su campo. Por tanto, es necesario evaluar estas competencias, pero con instrumentos pertinentes. Estas herramientas han introducido una variedad de recursos que optimizan actividades y procedimientos, lo que conduce a una economización de tiempo y recursos (Frania, 2017; Jiménez-Tecillo, 2022). La pandemia de la Covid-19 ha exacerbado su relevancia, multiplicando su uso y convirtiéndolas en elementos esenciales tanto en actividades laborales como personales, integrándose plenamente en la vida cotidiana (García, 2020). A pesar de su omnipresencia, la interacción con la tecnología muestra variaciones significativas según el contexto específico (López-Gil y Sevillano, 2020).

La educación superior ha experimentado importantes transformaciones, destacando el uso de plataformas y recursos digitales tras el traslado a entornos virtuales (Rocha et al., 2021). Aunque las actividades académicas presenciales se han reanudado, la creciente conectividad global ha permitido que la mayoría de los estudiantes cuenten con dispositivos tecnológicos y acceso a Internet (Fernández, 2023). Esto ofrece oportunidades para acceder a nuevas formas de aprendizaje, siempre que los estudiantes desarrollen competencias digitales, una responsabilidad de las instituciones educativas que influirá en el desempeño laboral de sus egresados (López-Gil & Sevillano, 2020; Candia, 2023). En este contexto, la estandarización de competencias digitales, como las propuestas por la *International Society for Technology in Education* (ISTE, 2007) y el Marco Europeo de Competencia Digital (DigComp) (Carretero et al., 2017), es clave. Este último define la competencia digital como el uso seguro, crítico y creativo de tecnologías para el trabajo, aprendizaje y participación social (INTEF, 2017), abarcando cinco áreas y 21 competencias específicas.

Las competencias digitales son importantes, porque preparan al estudiantado a enfrentar los retos de la era digital, mejorando su aprendizaje y sus habilidades académicas y profesionales (Candia, 2023). Su evaluación varía según el instrumento: la autovaloración, aunque común, puede ser subjetiva, mientras que las pruebas de medida directa resultan más confiables (Casillas-Martín et al., 2020; Cabezas-González et al., 2021). Varios estudios priorizan la autovaloración en lugar de analizar los componentes específicos de las competencias digitales (Bernate et al., 2021; García-Prieto et al., 2022; Pérez-Escoda et al., 2021; Pegalajar & Rodríguez, 2023; Rentería-Macías, 2022), como los cognitivos, actitudinales y procedimentales (Gallardo, 2017). Aunque las TIC generan oportunidades de aprendizaje, también presentan diversos riesgos (Torres-Hernández et al., 2019; Rocha et al., 2021; Orosco & Pomasunco, 2020; Cruz et al., 2022; León et al., 2022; Kaspersky, 2023; Gutiérrez et al., 2022).

Ante este panorama, la competencia digital de seguridad (INTEF, 2017) se presenta como un elemento necesario para mitigar estos riesgos y preparar a los estudiantes para un entorno digital seguro. La falta de estudios que analicen esta competencia de manera integral y con instrumentos psicométricamente validados genera una incertidumbre sobre el nivel de desarrollo de estas competencias de los universitarios. Por ello, esta investigación busca desarrollar y validar una prueba que permita medir de manera objetiva la competencia digital de seguridad, proporcionando una base sólida para futuras intervenciones educativas y contribuyendo al fortalecimiento de la formación en seguridad digital.

Con base en los mencionado, es necesario contar con una prueba que permita medir la competencia digital de seguridad en estudiantes universitarios, abarcando los aspectos de conocimiento, capacidad y actitud. Por tanto, el objetivo de la investigación fue diseñar y validar una prueba para evaluar la competencia digital de seguridad en estudiantes universitarios, en los ámbitos de conocimiento, capacidad y actitud, a partir de la pregunta ¿Cómo diseñar y validar una prueba para evaluar la competencia digital de seguridad en estudiantes universitarios, en los ámbitos de conocimiento, capacidad y actitud?

Metodología

Para dar respuesta al objetivo planteado y a partir de las líneas de investigación, como, además, la generación del conocimiento. Se realizó una investigación que se enmarcó en el paradigma Positivista, que tiene como base la "medición, revisión, descripción, experimentación, verificación, explicación del fenómeno objeto de estudio" (Maldonado, 2018, p. 20). Bajo el método Hipotético-Deductivo, que consiste en formular hipótesis como posibles explicaciones de un fenómeno y luego someterlas a pruebas para verificar su validez (Rodríguez & Pérez, 2017). Con enfoque cuantitativo, que consiste en analizar los datos que se recolectaron con el fin de probar las hipótesis planteadas, pero con apoyo de la medición numérica (Hernández-Sampieri & Mendoza, 2018). Con diseño no experimental (Hernández-Sampieri & Mendoza, 2018), de tipo descriptivo, y de corte transversal.

La población, consiste en el total de las unidades de estudio, que contienen características requeridas para ser consideradas (Ñaupas et al., 2018). En el estudio participaron 269 estudiantes de pregrado de las carreras profesionales de administración hotelera y turismo, administración de negocios e ingeniería agroindustrial de una universidad pública del centro del Perú. De estos participantes, 85 (31.60%) son varones y 184 (68.40%) son mujeres, con una edad promedio de 20.08 años (DE=2.18). En cuanto al ciclo de estudios que cursaban los estudiantes, la distribución fue la siguiente: 24.91% en el primer ciclo, 15.99% en el tercer ciclo, 16.36% en el quinto ciclo, 18.96% en el séptimo ciclo y 23.79% en el noveno ciclo.

La prueba de competencias digitales en seguridad se diseñó siguiendo el modelo DigComp 2.0 (INTEF, 2017), que comprende cuatro competencias: protección de dispositivos y contenido digital, protección de datos personales y privacidad, protección de la salud y el bienestar, y protección del entorno. En un primer momento, se revisaron y analizaron estas competencias para luego plantear los indicadores que servirían como base en la formulación de las preguntas. Posteriormente, se planteó las preguntas para cada dimensión, teniendo en cuenta los ámbitos de la competencia (conocimiento, capacidad y actitud) y en función de la población objeto de estudio. Las preguntas para los ámbitos de conocimiento y capacidad fueron de opción múltiple, donde una respuesta es la correcta entre cinco opciones, mientras que, para el ámbito de actitud, las preguntas se valoraron con una escala Likert (1= Totalmente en desacuerdo, 2 = En desacuerdo, 3 = Indiferente, 4 = De acuerdo, y 5 = Totalmente de acuerdo).

El instrumento, denominado prueba de competencia digital de seguridad, se sometió a una validez de contenido por juicio de expertos, donde 5 profesionales, especialistas en TIC y en metodología de la investigación, revisaron y proporcionaron sugerencias, principalmente en cuanto a la redacción de algunas preguntas. Estas sugerencias fueron tomadas en consideración, y la prueba final quedó conformada por 36 preguntas, distribuidas equitativamente entre los ámbitos de conocimiento, capacidad y actitud. La estructura de la prueba se detalla en la Tabla 1.

Tabla 1

Número de Preguntas por Dimensión y Ámbito de las Competencias Digitales de Seguridad.

Competencia	Número de preguntas		
	Conocimiento	Capacidad	Actitud
Protección de dispositivo y contenido digital	03	03	03
Protección de datos personales y privacidad	03	03	03
Protección de la salud y el bienestar	03	03	03
Protección del entorno	03	03	03

Nota. Cantidad de preguntas por dimensiones de las competencias digitales de seguridad, elaboración propia (2023).

Para la recolección de datos, se obtuvo el permiso correspondiente de la autoridad de la universidad pública más representativa del centro del Perú, así como se solicitó autorización a los docentes de las aulas correspondientes. La prueba se administró de manera presencial al estudiantado de forma anónima y voluntaria, previa aceptación del consentimiento informado. La recopilación de datos se llevó a cabo entre los meses de junio y julio del 2023.

Se realizó un análisis descriptivo de las competencias digitales de seguridad según los ámbitos de la competencia. Luego, se llevó a cabo la verificación del índice de dificultad y de discriminación de los ítems de conocimiento y capacidad. Además, se realizó un análisis de

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

fiabilidad utilizando el coeficiente Alfa de Cronbach. Finalmente, se realizó un análisis de la validez estructural mediante el Análisis Factorial de Componentes Principales con el método de rotación Varimax con normalización Kaiser. Para el procesamiento de datos, se utilizó el software estadístico libre y de código abierto JASP. Este software proporciona las herramientas necesarias para llevar a cabo análisis estadísticos complejos de manera eficiente y confiable.

Al realizar una revisión de estudios a nivel global y local, se observa una escasez de investigaciones sobre la competencia en seguridad digital. Una búsqueda en las bases de datos de Scopus y Web of Science utilizando la ecuación de búsqueda: TITLE-ABS-KEY (*"digital security competence" OR "digital security skills" OR "cybersecurity competence" OR "knowledge in digital security")* arrojó solo ocho resultados relacionados con el tema en cuestión. Estos estudios son los de Dodel y Mesch (2018), Glazunova et al. (2021), Matovu et al. (2022), Salminen et al. (2023), Holguin-Alvarez y Cruz-Montero (2023), Luthfia et al. (2023), Henrichsen y Shelton (2023), Latorre-Medina y Tnibar-Harrus (2023). Esta limitada cantidad de estudios sugiere que aún hay una falta de investigación en este ámbito, como lo corroboraron Salminen et al. (2023) al señalar que en países de la Unión Europea hay una falta de comprensión sobre esta temática. Además, los estudios relacionados con instrumentos que permitan medir esta competencia son escasos, debido a que este tema ha cobrado importancia recientemente (Torres-Hernández et al., 2019).

Basándose en lo anteriormente expuesto, resulta imperativo disponer de una prueba que permita medir la competencia digital de seguridad en estudiantes universitarios, abarcando los aspectos de conocimiento, capacidad y actitud. Por lo tanto, el objetivo principal de esta investigación fue diseñar y validar una prueba para evaluar la competencia digital de seguridad en estudiantes universitarios. Para lograr este objetivo, se tomaron en consideración los aspectos conceptuales propuestos por INTEF (2017) en relación con el área de competencia digital de seguridad. Dentro de esta área, se consideraron las cuatro competencias que la componen, las cuales se describen a continuación:

1. ***Protección de dispositivos y contenido digital.*** La competencia se centra en garantizar la seguridad de los dispositivos tecnológicos y del contenido digital personal. Incluye medidas como el uso de antivirus y contraseñas, así como la comprensión de los peligros y amenazas en línea, y estar al tanto de las medidas de protección y seguridad.
2. ***Protección de datos personales y privacidad.*** La competencia se orienta a comprender los términos comúnmente utilizados en el uso de programas, aplicaciones y servicios digitales, así como de tomar medidas preventivas para salvaguardar la información personal. Esto implica no exponer información personal innecesariamente, respetar la privacidad de terceros y tomar precauciones ante posibles amenazas, estafas y acoso en línea.
3. ***Protección de la salud y el bienestar.*** La competencia se enfoca en prevenir los peligros para la salud asociados con el uso de la tecnología, que pueden poner en riesgo la integridad física y el bienestar emocional. Incluye aspectos ergonómicos, visuales y otros relacionados con la adicción al uso de las tecnologías y la exposición a riesgos. Se busca encontrar un equilibrio entre las actividades en línea y fuera de línea para promover un estilo de vida saluda4.
4. ***Protección del entorno.*** La competencia implica tener en cuenta el impacto de las tecnologías sobre el medio ambiente. Se trata de optimizar el uso de los dispositivos tecnológicos para reducir el consumo de energía y tomar decisiones adecuadas en la compra y desecho de tecnología, con el fin de minimizar el impacto ambiental.

Resultados

Los resultados revelan que, en cuanto a las competencias en seguridad digital, los estudiantes universitarios presentan actitudes muy positivas, seguidas de capacidades adecuadas, mientras que los conocimientos están en proceso de desarrollo, este último evidencia la necesidad de reforzar su formación. Asimismo, la competencia digital más desarrollada corresponde a la protección de la salud y el bienestar en los tres ámbitos analizados.

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

Tabla 2

Estadísticos Descriptivos de las Competencias de Seguridad Digital.

Área de seguridad	Conocimiento		Capacidad		Actitud	
	M	*DE*	*M*	*DE*	*M*	*DE*
Competencia 1	1.11	0.90	2.36	0.73	12.05	2.27
Competencia 2	2.10	0.77	2.18	0.92	12.89	1.97
Competencia 3	2.36	0.83	2.42	0.70	13.01	1.99
Competencia 4	1.73	0.80	2.03	0.93	12.61	1.95
Total	7.31	2.01	8.98	2.21	50.55	6.34

Nota. Competencia 1= Protección de dispositivo y contenido digital. Competencia 2= Protección de datos personales y privacidad. Competencia 3= Protección de la salud y el bienestar. Competencia 4= Protección del entorno, elaboración propia (2023).

En la Tabla 2 se presentan los resultados del conocimiento de seguridad digital, donde se observa que las puntuaciones medias oscilan entre 1.11 y 2.36, sobre un puntaje máximo de 3. Lo que indica que los estudiantes universitarios poseen un mayor conocimiento en relación con la protección de la salud y el bienestar (M=2.36), seguido de la protección de datos personales y privacidad (M=2.10). Sin embargo, tienen un menor conocimiento en cuanto a la protección del entorno (M=1.73) y la protección de dispositivos y contenido digital (M=1.11). La puntuación media total de la prueba de conocimientos es de 7.31, y de acuerdo con la escala vigesimal utilizada en el contexto universitario peruano, la puntuación respecto al conocimiento de seguridad digital es de 12.18.

Asimismo, en la Tabla 2 se presentan los resultados de las capacidades en seguridad digital, donde se observa que, en una escala de puntaje máximo de 3, las puntuaciones medias oscilan entre 2.03 y 2.42. Estos resultados indican que los estudiantes universitarios

muestran una mayor capacidad en relación con la protección de la salud y el bienestar (M=2.42), seguida de la protección de dispositivos y contenido digital (M=2.36). Sin embargo, muestran una capacidad menor en cuanto a la protección de datos personales y privacidad (M=2.18) y la protección del entorno (M=2.04). La puntuación media total de la prueba de capacidades es de 8.98, y utilizando la escala vigesimal utilizada en el contexto universitario peruano, la puntuación respecto a la capacidad en seguridad digital es de 14.97.

También, en la Tabla 2, se presentan los resultados de las actitudes en seguridad digital, donde, en una escala de puntaje máximo de 15, las puntuaciones medias oscilan entre 12.05 y 13.01. Estos resultados evidencian que los estudiantes universitarios muestran mejores actitudes en relación con la protección de la salud y el bienestar (M=13.01), seguido de la protección del entorno (M=12.61) y la protección de datos personales y privacidad (M=12.89). La puntuación más baja se encuentra en la protección de dispositivos y contenido digital (M=12.05). La puntuación media de la escala de actitudes es de 50.55, y utilizando la escala vigesimal empleada en el contexto universitario peruano, la puntuación respecto a las actitudes frente a la seguridad digital es de 16.85.

Índice de Dificultad y de Discriminación de los Ítems de Conocimiento y Capacidad

El índice de dificultad y de discriminación son dos parámetros fundamentales para evaluar la efectividad de un instrumento de medición. El índice de dificultad permite determinar el nivel de facilidad/dificultad que presenta cada ítem del instrumento, identificando si los estudiantes tienen dificultades para responder a ciertos ítems, en este caso, en relación a la seguridad digital. Por otro lado, el índice de discriminación mide la capacidad de un ítem para diferenciar entre estudiantes con diferentes niveles de conocimiento y capacidad en el tema, lo que ayuda a asegurar que el instrumento sea sensible a las variaciones en el dominio de la seguridad digital.

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

Tabla 3

Índice de Dificultad y de Discriminación de los Ítems de Conocimiento y Capacidad.

Área de seguridad	Ítems	° de ítem	Índice de dificultad	Índice de discriminación
Competencia 1	Conocimiento	3	37%	67%
	Capacidad	3	79%	
Competencia 2	Conocimiento	3	70%	50%
	Capacidad	3	73%	
Competencia 3	Conocimiento	3	79%	33%
	Capacidad	3	81%	
Competencia 4	Conocimiento	3	58%	50%
	Capacidad	3	68%	
Total	Conocimiento	12	61%	50%
	Capacidad	12	75%	42%
Total		24	67%	46%

Nota. Resultados del índice de dificultad y de discriminación de los ítems de conocimiento y capacidad, elaboración propia (2023).

En la Tabla 3 se presentan los resultados del índice de dificultad del instrumento, donde se evidencia que la prueba de 24 ítems arroja un resultado del 67%, confirmando empíricamente que es fácil. Además, el índice de discriminación de esta prueba es adecuado (Id=46%). Asimismo, al analizar los ítems que evalúan conocimiento, se observa que los aciertos conforman el 61%, mientras que para los ítems que evalúan capacidades el porcentaje es del 75%, lo que indica que la prueba es fácil en ambos componentes del área de competencias digitales de seguridad. Además, las preguntas tanto de conocimiento (Id=50%) como de capacidad (Id=42%) discriminan adecuadamente.

Al examinar los ítems de las cuatro competencias de seguridad digital, se observa lo siguiente: En la Competencia 1: protección de dispositivos y contenido digital, los ítems de conocimiento son difíciles, mientras que los que evalúan capacidades son fáciles. Sin embargo, la discriminación es adecuada (Id=67%). Respecto a la Competencia 2: Protección de datos personales y privacidad, se aprecia que tanto los ítems de conocimiento como los de capacidad son fáciles, con un índice de discriminación adecuado (Id=50%). En cuanto a la Competencia 3: Protección de la salud y el bienestar, se encontró que los ítems de conocimiento son fáciles y los de capacidad son muy fáciles. El índice de discriminación muestra que los ítems son buenos, pero es posible mejorarlos (Id=33%). Por último, en relación con la Competencia 4: Protección del entorno, los resultados muestran que los ítems de conocimiento son adecuados y los de capacidad son fáciles, pero discriminan adecuadamente (Id=50%).

Tabla 4

Índice de Dificultad de cada uno de los Ítems que Conforman la Prueba.

Área de seguridad	Ítems	N° de ítems	Índice de dificultad	Criterio	Calificación
Competencia 1	4, 5	2	84, 84	81 – 100	Muy fácil
	6	1	68	61 – 80	Fácil
	1, 3,	2	41,47	41 – 60	Moderado
	2	1	23	21 – 40	Difícil
Competencia 2	7	1	86	81 – 100	Muy fácil
	9, 10, 12	3	65, 80, 80	61 – 80	Fácil
	8, 11	2	60, 57	41 – 60	Moderado
				21 – 40	Difícil
Competencia 3	14, 17, 18	3	86, 91, 91	81 – 100	Muy fácil
		2	70, 80	61 – 80	Fácil
	13, 15	1	60	41 – 60	Moderado
	16			21 – 40	Difícil
Competencia 4	21	1	87	81 – 100	Muy fácil
	23, 23, 24	3	66, 66, 71	61 – 80	Fácil
		1	50	41 – 60	Moderado
	20	1	36	21 – 40	Difícil
	19				

Nota. Resultados del índice de dificultad de los ítems que conforman la prueba, elaboración propia (2023).

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

En la Tabla 4 se presentan los resultados del índice de dificultad de cada una de las preguntas de la prueba de competencia digital de seguridad. Según los resultados obtenidos, se observa que el 29% de las preguntas son clasificadas como muy fáciles, el 38% como fáciles, el 25% como moderadas y el 8% como difíciles. Por lo tanto, se evidencia que la prueba no es equilibrada, ya que predominan las preguntas fáciles.

Fiabilidad y Validez

La fiabilidad para la prueba de conocimiento y capacidad, compuesta por 24 ítems, se evaluó mediante el Coeficiente Alfa, que mide la consistencia interna del instrumento, obteniendo un valor de 0.70. Asimismo, para el ámbito de la escala de actitudes, conformada por 12 ítems, se utilizó el mismo coeficiente, obteniendo un valor de 0.81. Estos resultados, evidencian que los ítems de la prueba y de la escala están suficientemente relacionados entre sí para medir el constructor de seguridad digital.

En cuanto a la validez del instrumento, se optó por realizar la validez de contenido y la validez estructural. Para la validez de contenido, en primera instancia, se diseñaron los ítems del instrumento basados en el modelo DigComp 2.0 (INTEF, 2017), específicamente en el área competencial denominada seguridad, que abarca cuatro competencias: protección de dispositivos y contenido digital, protección de datos personales y privacidad, protección de la salud y el bienestar, y protección del entorno. Estos ítems se formularon teniendo en cuenta los ámbitos de conocimiento, capacidad y actitud. En segunda instancia, el instrumento fue sometido a revisión por parte de expertos, quienes proporcionaron sugerencias y se realizaron los cambios necesarios.

Para evaluar la validez estructural, se llevó a cabo el Análisis Factorial (AF) de Componentes Principales. Se inició calculando el índice de adecuación muestral de Kaiser-Meyer-Olkin (KMO) y la prueba de esfericidad de Bartlett, obteniendo resultados aceptables y estadísticamente significativos, como se muestra en la Tabla 5. Estos resultados indican que los datos tienen una correlación positiva, lo que permite realizar un análisis factorial con confianza.

Tabla 5

Resultados del Índice de Adecuación Muestral.

	Prueba de Bartlett		
KMO	**X**	**Gl**	***p***
.839	1113.83	120	.000

Nota. Resultado de la prueba de Kaiser-Meyer-Olkin (KMO) y de la prueba de Bartlett, elaboración propia (2023).

A partir del cálculo anterior, se realizó el Análisis Factorial a través de Componentes Principales utilizando el método de rotación Varimax con normalización Kaiser. Se consideraron como variables el ámbito del conocimiento y capacidad correspondientes al área competencial de seguridad, que abarca cuatro competencias, así como los ítems del ámbito actitudinal (12 ítems) (ver Tabla 6). "La técnica empleada fue la multivariante con el propósito de simplificar, en el menor número de elementos posible, un grupo de variables interrelacionadas en un grupo de factores independientes, para comprobar la correlación entre variables y poder realizar una reducción de los datos simplificando la estructura" (Cabezas-González et al., 2021, p. 15).

Tabla 6

Porcentaje de la Varianza Total Explicada.

Componentes	**Sumas de cargas al cuadrado de la extracción**		
	Total	**% de varianza**	**% acumulado**
1	4.56	28.52	28.52
2	1.98	12.37	40.89
3	1.20	7.52	48.41
4	1.06	6.34	**54.76**
5	.89	5.59	60.34
6	.88	5.52	65.87
7	.82	5.15	71.02
8	.76	4.76	75.77
9	.68	4.22	79.99
10	.59	3.69	83.68
11	.54	3.37	87.05
12	.46	2.85	89.91

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

13	**.44**	**2.73**	**92.64**
14	.42	2.65	95.29
15	.42	2.60	97.87
16	.34	2.11	**100.00**

Nota. Resultados del porcentaje de la varianza total explicada, elaboración propia (2023).

En el proceso de análisis de Componentes Principales, se calcularon los valores λ para cada componente, reteniendo factores cuando el valor $\lambda \geq 1$. El primer factor explicó el 54.76% de la varianza, mientras que el segundo añadió el 45.24%, lo que significa que ambos factores explican el 100% de la varianza de la matriz factorial, es decir, los dos factores seleccionados capturan toda la información relevante contenida en los datos.

Al realizar un análisis factorial exploratorio y fijar el número de factores en dos (factor 1: ámbito actitudinal, factor 2: ámbito de conocimiento y capacidad), se logró la bidimensionalidad de la prueba con un 100% de varianza explicada, confirmando así la validez del instrumento. En la Tabla 7 se presenta la matriz de componentes, donde se evidencia la saturación de ítems relacionados a las actitudes en el primer factor y de conocimientos y capacidades en el segundo.

Tabla 7

Matriz de Componentes Principales.

Variables	**Factor**	
	1	2
C1: Protección de dispositivo y contenido digital	-.016	**.577**
C2: Protección de datos personales y privacidad	.193	**.797**
C3: Protección de la salud y el bienestar	.121	**.765**
C4: Protección del entorno	.009	**.681**
Actitud 1	**.504**	.131
Actitud 2	**.611**	-.109
Actitud 3	**.354**	.037
Actitud 4	**.582**	.142
Actitud 5	**.544**	.131
Actitud 6	**.658**	.120
Actitud 7	**.586**	.165
Actitud 8	**.717**	.051
Actitud 9	**.746**	.150
Actitud 10	**.761**	-.113
Actitud 11	**.387**	-.035
Actitud 12	**.596**	.141

Nota. Método de extracción: Análisis de componentes principales. Método de rotación: Varimax con normalización Kaiser.

También se observa en la Tabla 7 que todos los ítems del factor 1 (actitud) adquieren un peso suficiente (>0.4) o muy próximos a este valor (por ejemplo, Actitud 3 y Actitud 11). De manera similar, en cuanto al factor 2 (conocimiento y capacidad), los ítems muestran un peso adecuado (>0.4), lo que confirma lo establecido por el equipo de investigadores, así como por los expertos que revisaron el contenido del instrumento.

Prueba para Evaluar la Competencia Digital de Seguridad

Instrucciones

A continuación, se presentan preguntas relacionadas con la competencia digital de seguridad, las cuales se dividen en dos partes. En la primera parte, lea cada pregunta y marque la respuesta según su percepción, teniendo en cuenta que no hay respuestas correctas ni incorrectas. La escala es la siguiente: Totalmente en desacuerdo (TD), En desacuerdo (D), Indiferente (I), De acuerdo (A) y Totalmente de acuerdo (TA) (ver Tabla 8). En la segunda parte, lea cada pregunta y marque con una X la respuesta correcta.

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

Tabla 8

Primera Parte.

		TD	D	I	A	TA
Protección de dispositivo y contenido digital						
01	Los sistemas operativos, programas o aplicaciones suelen presentar fallas de seguridad, por lo cual resulta necesario realizar actualizaciones periódicas					
02	Es imprescindible contar con un software antivirus original instalado.					
03	Se recomienda no utilizar la misma contraseña para acceder a la cuenta de correo electrónico, redes sociales, páginas web, y otros servicios en línea					
	Protección de datos personales y privacidad					
4	Los dispositivos móviles deben tener algún tipo de contraseña para iniciar sesión.					
5	Es recomendable hacer copia de seguridad de nuestros datos de manera periódica.					
6	Compartir información personal y de otros en internet es peligroso.					
	Protección de la salud y el bienestar					
7	El uso no controlado de dispositivos tecnológicos puede tener un impacto negativo en nuestra salud					
8	Es fundamental tener conocimiento de los hábitos posturales adecuados al utilizar dispositivos tecnológicos					
9	Se debe usar la tecnología de manera adecuada, sin que afecte nuestra vida personal.					
	Protección del entorno					
0	En lo posible debemos ahorrar recursos energéticos cuando utilizamos los dispositivos tecnológicos.					
1	Es importante maximizar el uso de los recursos consumibles (hardware, tinta, papel) para reducir el impacto de los dispositivos tecnológicos en el medio ambiente					
2	Reconozco que el uso irresponsable de dispositivos tecnológicos puede tener impactos negativos en el medio ambiente					

Segunda parte

Protección de dispositivo y contenido digital

1. ¿Cuál de los siguientes no es un software antivirus?

a. Bitdefender
b. Malware
c.Kaspersky
d. Avira
e.Eset

2. ¿Cuál de las siguientes opciones describe un software malicioso que "secuestra" archivos, los encripta y luego exige un pago para eliminar la restricción?

a.Ransomware
b. Spyware
c.Troyanos
d. Avast
e.Norton

3. ¿Cuál de las siguientes opciones no es una buena práctica al utilizar contraseñas?

a. Combinar varios caracteres (mayúsculas, minúsculas, números, símbolos, etc.).
b. No utilizar la misma contraseña para todos los accesos.
c. No compartir la contraseña por algún medio de mensajería.
d. Cambiar las contraseñas que son proporcionadas por defecto.
e. No cambiar contraseñas con regularidad.

4. ¿Qué acción debo tomar si en mi dispositivo tecnológico (laptop, smartphone, tablet, etc.) aparece un aviso para actualizar el sistema operativo?

a. No debo realizar ninguna acción.
b. Debo aceptar la actualización (instantáneamente o después).
c.Debo apagar o reiniciar el equipo para que me deje trabajar.
d. Debo desactivar la opción de actualización para que no me moleste.
e.Debo reclamarle a la empresa que me vendió el dispositivo tecnológico.

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

5. ¿Cuál de las siguientes contraseñas es más segura?

a. 23244589
b. MARCELO2023
c. Ricardoperez
d. JuanJulian963=?
e. ROBERTOjugatino

6. Juan es un ciberdelincuente que ha logrado obtener el usuario y la contraseña de una cuenta de red social de Roberto. Cuando Juan intenta iniciar sesión utilizando esas credenciales, Roberto recibe un mensaje de código de seguridad en su teléfono celular. Esto sucede porque Roberto está utilizando:

a. Autenticación de doble factor
b. Contraseña robusta
c. Un buen antivirus
d. Ransomware
e. Keeper Security

Protección de datos personales y privacidad

7. ¿Cuáles son las medidas básicas para proteger la información en nuestros dispositivos tecnológicos (*laptop, smartphone, tablet,* entre otros)?

a. Configurar el inicio de sesión con una contraseña y el bloqueo automático de pantalla.
b. Solo una contraseña robusta para el inicio de sesión es suficiente.
c. No establecer ninguna contraseña para facilitar el inicio de sesión.
d. Utilizar una contraseña sencilla y fácil de recordar.
e. Colocar el patrón de acceso.

8. ¿Cuál es el propósito principal de realizar una copia de seguridad de datos (*backup* de datos)?

a. Aumentar la velocidad de acceso a los archivos de la *laptop, smartphone,* etc.
b. Eliminar archivos innecesarios de manera permanente para liberar espacio de almacenamiento.
c. Optimizar el rendimiento del hardware de la *laptop, smartphone*, etc.
d. Tener acceso a la información de manera inmediata.
e. Proteger y recuperar los datos personales ante posibles pérdidas, fallas del sistema, formateo, etc.

9. La identidad digital consiste en:

a. La representación física de una persona en el espacio virtual.
b. La información y los datos asociados a una persona o entidad en internet.
c. El proceso de crear perfiles falsos en redes sociales.
d. La capacidad de acceder a internet desde diferentes dispositivos.
e. Las normas de conducta socialmente aceptables en Internet.

10. Pamela y su familia se fueron de vacaciones por cinco días al Cuzco, desde que iniciaron el viaje, ella publicó la ruta del viaje, los datos de los integrantes de su familia, fotografías de cada actividad que realizan, etc. ¿Cuál es el principal riesgo de la conducta de Pamela al publicar detalles personales y de su familia durante su viaje en redes sociales?

a. Bien por Pamela, porque es bueno compartir sus vivencias con su entorno familiar y amigos de internet.
b. La información publicada no afecta de ninguna manera a su familia ya que uno es libre de publicar lo que desea.
c. Pamela debe darse cuenta de que la información compartida en línea puede ser peligrosa y difícil de controlar una vez publicada.
d. Pamela recibirá muchos *likes* y comentarios a la publicación.
e. Es normal realizar ese tipo de publicaciones para tener identidad digital y ser reconocidos en el mundo virtual.

11. Manuel solicita recomendaciones sobre cómo realizar una copia de seguridad de la información almacenada en su *laptop*. ¿Cuál de las siguientes sugerencias no deberías darle?

a. Guardar la información en un disco duro externo u otra laptop.
b. Realizar periódicamente una copia de seguridad.
c. Guardar también en algún servicio de la nube (*Google Drive*, *One Drive*, *Box*, *Mega*, etc.).
d. Realizar una sola copia de seguridad ya que será suficiente porque ya hay respaldo
e. Almacenar la copia de seguridad realizada en lugares seguros o servicios confiables.

12. Hoy fue el último día de clases en la universidad y Pedro, muy emocionado, se tomó una foto con sus compañeros y la publicó en su red social etiquetándolos a cada uno sin consultar. En relación con la privacidad de la información:

a. Pedro no es respetuoso de la privacidad de los demás.
b. Pedro es un buen amigo, porque publicó la foto ahorrando tiempo a los demás.
c. Pedro está ayudando para que los integrantes de la promoción sean conocidos.
d. Pedro etiquetó a todos para recibir muchos *likes*.
e. Pedro practica la libertad de expresión.

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0,* 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

Protección de la salud y el bienestar

13. ¿Cuál de las siguientes opciones no representa un riesgo que pueda afectar mi salud física y psicológica al momento de usar dispositivos tecnológicos?

a. Pasar casi todo el día frente a una pantalla.
b. Estar pendiente de los mensajes que envían y comparten mis amigos.
c. Priorizar la comunicación cara a cara en cuanto sea posible.
d. Estar agachado frecuentemente para usar el dispositivo móvil.
e. No equilibrar la vida en el "mundo virtual" con el "mundo real".

14. ¿Cuál es la postura adecuada al momento de usar un dispositivo móvil (*smartphone* o *tablet*)?

a. Encorvarse y agachar la cabeza.
b. Mantener el dispositivo móvil a la altura de los ojos.
c. Cruzar las piernas y encoger los hombros.
d. Inclinar la cabeza hacia un lado.
e. Usar el dispositivo móvil echado en la cama.

15. ¿Cuál de las siguientes opciones no es un riesgo asociado a la adicción por el uso de dispositivos móviles (smartphone o tablet)?

a. Aislamiento social.
b. Disminución del rendimiento académico.
c. Problemas de salud mental como la ansiedad.
d. Trastornos de sueño.
e. Mejora el bienestar emocional.

16. ¿Cuál de las siguientes imágenes muestra la postura correcta para usar un dispositivo móvil?

a  b.  c.  d.  e. 

17. Rosario se reúne con sus compañeras en su casa para realizar sus tareas académicas, pero generalmente se pasan viendo videos en YouTube, revisando publicaciones en redes sociales, escuchando música, etc. Y después recién realizan sus deberes. ¿Cuál de las siguientes opciones describe mejor la situación de Rosario y sus compañeras al realizar tareas académicas juntas en su casa?

a. No son capaces de controlar los distractores.
b. Están fortaleciendo sus lazos de amistad.
c. Está bien, ya que primero deben relajarse.
d. No afecta al bienestar psicológico.
e. Es normal en dicha edad.

18. Ante la situación en la que Mario ha creado un perfil falso en Facebook para difamar a Julio, ¿cuál sería la mejor acción que Julio debería tomar?

a. No hacer caso.
b. Crearse otro perfil en Facebook y atacar a Mario.
c. Es su problema para que se mete en líos.
d. Guardar todas las pruebas y denunciar en la plataforma de Facebook y ante las autoridades correspondientes.
e. Desconectarse de Facebook por un tiempo para olvidarse del problema.

Protección del entorno

19. ¿Cuál es el significado de RAEE?:
a. Real Academia de la Escuela de Electrónica.
b. Residuos de Aparatos Eléctricos y Electrónicos.
c. Reposición y Adquisición Eléctrica y Electrónica.
d. Reusar los Aparatos Eléctricos y Electrónicos.
e. Reciclar Eléctrica y Electrónicamente los Dispositivos Tecnológicos.

20. ¿Es cierto que existen marcas y modelos de smartphones que han sido fabricados con prácticas sostenibles?

a. No
b. Sí
c. Había en la década pasada
d. Habrá en un futuro no muy lejano
e. Eso es imposible

21. ¿El uso de dispositivos tecnológicos como la *laptop*, *smartphone*, *tablet*, etc., generan impacto medioambiental?

a. No tiene nada que ver con el medio ambiente.
b. Si, tiene impacto en el medio ambiente.
c. La *laptop* sí, porque consume más energía que el *smartphone* y la *tablet*.
d. No impactan porque usan energía limpia.
e. No impactan porque tienen certificado de calidad.

22. Beto es un estudiante que con mucho esfuerzo se compró una *laptop*, pero después de un tiempo se malogró. ¿Cuál sería una buena actitud para aprovechar dicho equipo malogrado?

a. Botar a la basura y comprarse otra.
b. Donar a una institución donde estudian reparación de *laptops*.
c. Llevar a un técnico y ver la posibilidad de venderle la laptop para que algunas partes puedan ser utilizadas en otras.
d. a, b y c
e. b y c

23. Qué acción no contribuye a proteger el medio ambiente al usar los *smartphones*:

a. Desactivar funciones innecesarias cuando no se use.
b. Aprovechar al dejar cargando la batería toda la noche.

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

c. Al comprar algún *smartphone*, elegir marcas y modelos que implementen prácticas sostenibles.
d. Actualizar el software y las aplicaciones para mejorar el rendimiento.
e. Si el celular presenta problemas, valorar la opción de repararlo en lugar de adquirir uno nuevo.

24. Para reducir el impacto ambiental de los dispositivos tecnológicos durante su uso diario, seleccione la acción que se debe realizar para reducir el impacto medioambiental.

a. Usar solo durante un año cualquier dispositivo tecnológico y luego cambiarlo.
b. Estos dispositivos tecnológicos no impactan al medio ambiente.
c. Debo apagarlos cuando no se utilicen.
d. Usar solo dispositivos tecnológicos nuevos.
e. Debo cargarlos bien para que dure todo el día.

Discusiones

En función de la pregunta planteada, se diseñó y validó una prueba para evaluar la competencia digital de seguridad en estudiantes universitarios, en los ámbitos de conocimiento, capacidad y actitud, evidenciando propiedades psicométricas adecuadas, con una consistencia interna sólida y un índice de discriminación y dificultad que asegura la medición del constructo estudiado. Además, el análisis factorial confirma la estructura bifactorial del instrumento, agrupando el conocimiento y la capacidad en un factor, y las actitudes en otro.

En el contexto actual, donde la sociedad está cada vez más dependiente de las TIC (De Bruijn & Janssen, 2017), es imperativo poseer competencias digitales en seguridad. Esto es especialmente relevante en el ámbito de la educación superior, ya que es en este nivel donde se están formando los futuros profesionales que se integrarán en un entorno laboral cada vez más virtualizado, lo que los expone a diversos problemas relacionados con la seguridad digital. Según Rocha et al. (2021), las instituciones de educación superior deben promover de manera obligatoria la formación en seguridad digital, independientemente de la carrera profesional.

En este contexto, se presenta una prueba que evalúa la competencia digital en seguridad en estudiantes universitarios, con el objetivo de abordar esta brecha en la investigación. Se busca superar el sesgo presente en los instrumentos de autovaloración, los cuales tienden a centrarse en el aspecto subjetivo de las respuestas de los participantes (Cabezas-González et al., 2021). Por lo tanto, cobra gran importancia la evaluación de esta competencia, considerando que son escasos los estudios que proponen instrumentos para medir esta, teniendo en cuenta los tres ámbitos clave: conocimiento, capacidad y actitud. Además, es fundamental que estos instrumentos proporcionen evidencias de validez. Hasta el 2023 solo se han encontrado algunos estudios que abordan las competencias digitales y evalúan los tres ámbitos mencionados (García-Valcárcel et al., 2019; Cabezas-González et al., 2021; Casillas-Martín et al., 2020; García-Valcárcel et al., 2020).

Los hallazgos del estudio se asemejan a los de la investigación realizada por García-Valcárcel et al. (2019), quienes diseñaron una prueba para medir los conocimientos, capacidades y actitudes de los estudiantes respecto a las competencias digitales de seguridad. Aunque su muestra incluyó tanto a estudiantes de educación primaria como secundaria, los resultados obtenidos revelaron que los ítems de la prueba presentaban índices adecuados de discriminación y dificultad. Además, su estudio mostró una fiabilidad apropiada y validó el instrumento mediante juicio de expertos y el análisis de la estructura factorial de la prueba, garantizando así su validez.

También son similares con otro estudio donde diseñaron y validaron un instrumento para evaluar la competencia digital en la resolución de problemas, abarcando los tres componentes de la competencia: conocimiento, capacidad y actitud. Ellos concluyeron que el instrumento propuesto es válido y fiable, y que posee un buen nivel de discriminación. Sin embargo, señalaron que los ítems presentan un desequilibrio en cuanto al nivel de dificultad, con una predominancia de ítems de mayor dificultad (Cabezas-González et al., 2021).

Asimismo, en el estudio de Casillas-Martín et al. (2020), quienes validaron una prueba para evaluar la competencia digital en estudiantes en los ámbitos de conocimiento, capacidad y actitud, se identificaron buenas propiedades psicométricas, lo que permite calificar el

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

instrumento como fiable y válido para medir las competencias digitales evaluadas, incluyendo la seguridad digital. Estos hallazgos son consistentes con los resultados obtenidos en el presente estudio.

Además, los resultados son similares a los obtenidos en el trabajo de García-Valcárcel et al. (2020), quienes diseñaron un instrumento para evaluar competencias digitales (incluye la competencia de seguridad digital), considerando conocimientos, habilidades y actitudes. Al finalizar el estudio, los autores concluyeron que el modelo del instrumento propuesto puede servir como una estructura y base para el diseño de pruebas de evaluación específicas en esta temática.

Los estudios mencionados, aunque validaron sus pruebas con muestras de estudiantes de educación primaria y secundaria, presentan consistencia con el presente estudio, ya que los instrumentos propuestos evalúan los tres componentes de la competencia: conocimiento, capacidad y actitud. Esta metodología permite obtener datos más objetivos y con menor sesgo en comparación con los instrumentos basados en la autovaloración, que suelen utilizarse con mayor frecuencia. Por lo tanto, el instrumento propuesto en este estudio, que se aplica en el ámbito universitario, refuerza esta consistencia y validación.

Por último, es importante señalar que este instrumento presenta algunas limitaciones a tener en cuenta, como el tamaño de la muestra. Por lo tanto, se recomienda en futuros estudios incluir una mayor cantidad de estudiantes, provenientes de diversas carreras profesionales y modalidades de estudio, entre otros aspectos que permitan una mayor heterogeneidad en la muestra. Además, se sugiere realizar un Análisis Factorial Confirmatorio (AFC) para continuar aportando evidencias de validez del instrumento.

Conclusiones

La prueba utilizada en el estudio demuestra propiedades psicométricas adecuadas, con una consistencia interna sólida y un índice de discriminación y dificultad que asegura su capacidad para medir competencias digitales en seguridad. Además, el análisis factorial confirma la estructura bifactorial del instrumento, agrupando el conocimiento y la capacidad en un factor, y las actitudes en otro. Esto lo convierte en una herramienta confiable para futuras investigaciones.

Este estudio tiene importancia porque proporciona una herramienta fiable para evaluar las competencias digitales en seguridad de los estudiantes universitarios, un área de creciente relevancia en la educación superior. Los resultados del instrumento indican que, aunque los estudiantes presentan actitudes favorables hacia la seguridad digital, existe una brecha en cuanto a sus conocimientos y capacidades, lo que revela la necesidad de fortalecer la formación teórica y práctica en este campo dentro de los programas educativos universitarios. Este hallazgo evidencia la necesidad de incluir en los planes de estudio temas orientados al desarrollo de las competencias digitales de seguridad.

Los resultados obtenidos en el estudio tienen un impacto para el futuro de la educación universitaria, ya que la prueba demuestra ser una herramienta útil para medir las competencias digitales en seguridad de manera objetiva y confiable. Al evidenciar que los conocimientos aún están en proceso de desarrollo, el estudio subraya la importancia de incorporar temas que fortalezcan no solo las actitudes positivas hacia la seguridad digital, sino también las capacidades y conocimientos de los estudiantes en este ámbito. De este modo, se contribuirá a formar profesionales con competencias digitales adecuada para enfrentar los riesgos derivados de la digitalización.

Finalmente, se recomienda que futuras investigaciones exploren las competencias digitales en seguridad mediante instrumentos como el utilizado en este estudio, que permite obtener mediciones más objetivas y representativas al evitar los sesgos asociados con los métodos de autovaloración. Además, se sugiere que estudios futuros aborden el diseño de estrategias educativas que fomenten el desarrollo integral de las competencias digitales, enfocándose tanto en el conocimiento teórico como en la aplicación práctica y las actitudes hacia la seguridad digital, para formar a los futuros profesionales que respondan al contexto impactado por las tecnologías.

Orosco-Fabian, J., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. (2025). Competencia digital de seguridad en estudiantes universitarios: diseño y validación de una prueba. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

Declaración de Conflictos de Intereses

Los autores declaran que no existe ningún conflicto de interés que pudiera haber influido en la realización de este estudio. Ninguno de los autores ha recibido financiación ni mantiene relaciones personales o profesionales que puedan haber condicionado los resultados obtenidos o su interpretación. La totalidad del trabajo fue llevado a cabo de manera independiente, garantizando la imparcialidad y rigor científico en cada una de las etapas del proceso investigativo.

Referencias

Bernate, J., Fonseca, I., Guataquira, A., & Perilla, A. (2021). Competencias Digitales en estudiantes de Licenciatura en Educación Física. *Retos, 41*, 310-318. https://doi.org/10.47197/retos.v0i41.85852

Cabezas-González, M., Casillas-Martín, S., García-Valcárcel-Muñoz-Repiso, A., & Basilotta-Gómez-Pablos, V. (2021). Validación de prueba para evaluar la competencia digital en el área de resolución de problemas en estudiantes de educación obligatoria. *Revista Electrónica Educare, 25*(3), 1-21. https://doi.org/10.15359/ree.25-3.2

Candia, J. C. (2023). Competencias digitales en la educación superior. *Horizontes Revista de Investigación en Ciencias de la Educación, 7*(29), 1548-1563. https://doi.org/10.33996/revistahorizontes.v7i29.612

Carretero, S., Vuorikari, R., & Punie, Y. (2017). *The digital competence framework for citizens with eight proficiency levels and examples of use* [El marco de competencias digitales para los ciudadanos con ocho niveles de competencia y ejemplos de uso]. Office of the European Union. https://doi.org/10.2760/38842

Casillas-Martín, S., Cabezas-González, M., & García-Valcárcel, A. (2020). Análisis psicométrico de una prueba para evaluar la competencia digital de estudiantes de Educación Obligatoria. *RELIEVE, 26*(2), Artículo 2. http://doi.org/10.7203/relieve.26.2.17611

Cruz, G. I., Delgado, L. E., Ponce, B. R., & Marcillo, M. J. (2022). Riesgos de seguridad de los datos en la web. *Journal TechInnovation, 1*(2), 43–49. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.43-49

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies [Crear conciencia sobre la ciberseguridad: la necesidad de estrategias de encuadre basadas en evidencia]. *Government Information Quarterly, 34*, 1-7. http://dx.doi.org/10.1016/j.giq.2017.02.007

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors [Desigualdad en habilidades digitales y adopción de comportamientos de seguridad en línea]. *Information Communication and Society, 21*(5), 712 – 728. https://doi.org/10.1080/1369118X.2018.1428652

Fernández, R. (2023). *El uso de Internet a nivel mundial–Datos estadísticos.* Statista. https://acortar.link/p7kKkG

Frania, M. (2017). Self-assessment of Attitudes Towards Media and the Knowledge of Safety in Cyberspace of Future Pedagogues and Teachers in Croatia and Poland [Autoevaluación de las actitudes hacia los medios de comunicación y el conocimiento de la seguridad en el ciberespacio de los futuros pedagogos y profesores de Croacia y Polonia]. *The New Educational Review, 50*, 227-240. https://doi.org/10.15804/tner.2017.50.4.18

Gallardo, A. (2017). *Las competencias emocionales en el currículum de las carreras de Pedagogía de la Universidad de Playa Ancha* [Tesis doctoral, Universidad de Girona]. https://acortar.link/Yvzjha

García-Valcárcel, A., Salvador, L., Casillas, S., & Basilotta, V. (2019). Evaluación de las competencias digitales sobre seguridad de los estudiantes de educación básica. *Revista de Educación a Distancia, 19*(61), Artículo 5. https://doi.org/10.6018/red/61/05

García-Valcárcel, A., Casillas-Martín, S., & Basilotta, V. (2020). Validation of an Indicator Model (INCODIES) for Assessing Student Digital Competence in Basic Education [Validación de un modelo de indicadores (INCODIES) para evaluar la competencia digital de los estudiantes de Educación Básica]. *Journal of New Approaches in Educational Research, 9*(1), 110-125. https://doi.org/10.7821/naer.2020.1.459

García, J. C. (2020). Las TIC en la pandemia Covid-19. *Nuevo hospital, XVI*, 11-12. https://acortar.link/yD1TP

García-Prieto, F. J., López-Aguilar, D., & Delgado-García, M. (2022). Competencia digital del alumnado universitario y rendimiento académico en tiempos de COVID-19 [Digital competence of university students and academic performance in times of COVID-19]. *Pixel-Bit. Revista de Medios y Educación, 64*, 165–199. https://doi.org/10.12795/pixelbit.91862

Glazunova, O. G., Sayapina, T. P., Kasatkina, OM, Korolchuk, V. I. & Voloshina, TV (2021). Формування навичок цифрової безпеки майбутніх фахівців з економіки [Formación de competencias en seguridad digital de futuros especialistas en economía]. *Інформаційні технології і засоби навчання, 82*(2), 93–108. https://doi.org/10.33407/itlt.v82i2.4308

Gutiérrez, J. L., Castro, J. W., Calderón, A. P., & Arteaga, J. A. (2022). Impacto ambiental generado por la basura electrónica. *Revista Científica Arbitrada Multidisciplinaria Pentaciencias, 4*(4), 417-426. https://n9.cl/4r4fv

Henrichsen, J. R. & Shelton, M. (2023). Boundaries, Barriers, and Champions: Understanding Digital Security Education in US Journalism Programs [Límites, barreras y campeones: comprensión de la educación en seguridad digital en los programas de periodismo de EE. UU.]. *Journalism Studies, 24*(3), 309 – 328. https://doi.org/10.1080/1461670X.2022.2148267

Hernández-Sampieri, R., & Mendoza, C. P. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill Educación.

Holguin-Alvarez, J., & Cruz-Montero, J. (2023). Gamified dances, digital and socio-emotional skills in collaborative virtual environments of university students surviving the Covid-19 virus [Danzas gamificadas, habilidades digitales y socioemocionales en entornos virtuales colaborativos de estudiantes universitarios sobrevivientes al virus Covid-19]. *Frontiers in Education, 8,* Artículo 1179684. https://doi.org/10.3389/feduc.2023.1179684

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). (2017). Marco común de competencia digital docente. Ministerio de Educación, Cultura y Deporte. https://acortar.link/dWyUvP

International Society for Technology in Education. (2007). *NETS (National Education Technology Standards) [NETS* (Estándares Nacionales de Tecnología Educativa)]. https://n9.cl/xi180

Jiménez-Tecillo, F. J. (2022). TICs y educación: Aplicación en pandemia. Revista de Investigaciones. *Universidad del Quindío, 34*(2), 245–250. https://doi.org/10.33975/riuq.vol34n2.977

Kaspersky. (2023). *¿Cómo afecta la tecnología a tu salud física?* https://acortar.link/jZjoMf

Latorre-Medina M. J., & Tnibar-Harrus, C. (2023). Цифрова безпека в освітніх програмах: дослідження на основі сприйняття майбутніх учителів. [Seguridad digital en los programas educativos: un estudio basado en las percepciones de los futuros docentes]. *Інформаційні технології і засоби навчання, 95*(3), 102–111. https://doi.org/10.33407/itlt.v95i3.5204

León, T., Piñón, J. C., & Álvarez, J. (2022). Alertas en salud sobre el uso de los dispositivos electrónicos y su impacto en el bienestar visual. Revista Cubana de Medicina, 61(3), Artículo e3140. https://n9.cl/lpk0lt

López-Gil, K., & Sevillano, M. (2020). Desarrollo de competencias digitales de estudiantes universitarios en contextos informales de aprendizaje. *Educatio Siglo XXI, 38*(1), 53-78. http://dx.doi.org/10.6018/educatio.413141

Luthfia, A., Handayani, F., Gasa, F. M., Ramadanty, S., & Ridzuan, A. R. (11-13 de julio de 2023). *Navigating the Cyber Frontier: Youth Capabilities to Confront Dis/Misinformation with Digital Literacy and Digital Security* [Navegando por la frontera cibernética: capacidades de los jóvenes para afrontar la desinformación y la desinformación con alfabetización digital y seguridad digital]. 17th International Conference on Telecommunications, ConTEL 2023, Graz, Austria. https://doi.org/10.1109/ConTEL58387.2023.10198919

Maldonado, J. E. (2018). *Metodología de la investigación social. Paradigmas: cuantitativo, sociocrítico, cualitativo, complementario*. Ediciones de la U.

Matovu, R., Nwokeji, J. C., Holmes, T., & Rahman, T. (08 – 11 de octubre de 2022). *Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges* [Enseñar y aprender concientización sobre ciberseguridad con gamificación en universidades y colegios más pequeños]. Proceedings - Frontiers in Education Conference, FIE, Uppsala, Sweden. https://doi.org/10.1109/FIE56618.2022.9962519

Ñaupas, H., Mejía, E., Novoa, E. & Villagomez, A. (2014). *Metodología de la investigación cuantitativa-cualitativa y redacción de tesis.* Ediciones de la U.

Orosco, J. R., & Pomasunco, R. (2020). Adolescentes frente a los riesgos en el uso de las TIC. *Revista Electrónica de Investigación Educativa, 22,* Artículo e17, 1-13. https://doi.org/10.24320/redie.2020.22.e17.2298

Pérez-Escoda, A., Lena-Acebo, F. J., & García-Ruiz, R. (2021). Brecha digital de género y competencia digital entre estudiantes universitarios. *Aula Abierta, 50*(1), 505–5014. https://doi.org/10.17811/rifie.50.1.2021.505-5014

Pegalajar, M., & Rodríguez, A. F. (2023). Las competencias digitales en estudiantes de las carreras de Educación en Ecuador. *Campus. Virtuales, 12*(2), 113-126. https://doi.org/10.54988/cv.2023.2.1215

Rocha, F. J., George, C. E., & Glasserman, L. D. (2021). *La necesidad de la seguridad digital en entornos de aprendizaje no presenciales*. [Conferencia]. XVI Congreso Nacional de Investigación Educativa CNIE-2021, Puebla, México. https://n9.cl/gage8

Rodríguez, A., & Pérez, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela de Administración de Negocios,* (82), 1-26. https://doi.org/10.21158/01208160.n82.2017.1647

Rentería-Macías, H. J. (2022). Competencias Digitales de Estudiantes Universitarios en último nivel de Carrera en Ecuador. *Polo del conocimiento, 7*(1), 284-297. https://n9.cl/rcoaa

Salminen, M., Candelin, N., Cullen, K. Latvanen, S., Lindroth, M., & Matilainen, T. (19-22 de junio de 2023). *Cybersecurity education in European higher education institutions* [Educación en ciberseguridad en instituciones europeas de educación superior]. 9th International Conference on Higher Education Advances, Valencia, España. http://dx.doi.org/10.4995/HEAd23.2023.16336

Torres-Hernández, N., Pessoa, T., & Gallego-Arrufat, M. J. (2019). Intervención y evaluación con tecnologías de la competencia en seguridad digital. *Digital Education Review (DER),* (35), 111-129. https://doi.org/10.1344/der.2019.35.111-129