Revista de Pensamiento Estratégico y Seguridad CISDE

CISDE Journal, 9(1), 2024

Recibido: 15-12-2022 / Revisado: 05-04-2023
Aceptado: 14-04-2023 / Publicado: 30-05-2024

Evaluación de la seguridad digital para la complejidad en estudiantes universitarios: diseño y validación del instrumento Complex-ADS

Assesment of digital security for complexity in university students: design and validation of the Complex-DSL instrument

Carlos E. George-Reyes[1], Francisco J. Rocha-Estrada[1], Leonardo D. Glasserman-Morales[1], Raidell Avello-Martínez[2]

[1] Tecnológico de Monterrey, México
[2] Universidad de Cienfuegos, Cuba

cgeorge@tec.mx , fcojvr25@gmail.com , glasserman@tec.mx , ravello@ucf.edu.cu

RESUMEN. El uso de la tecnología digital es indispensable para participar en la sociedad del conocimiento, sin embargo, no existe certeza de que los estudiantes universitarios tengan la alfabetización suficiente para hacerlo de forma segura. En este artículo se elaboró, validó y analizó la confiabilidad de un instrumento para evaluar la Alfabetización en Seguridad Digital (ASD) desde el enfoque del pensamiento complejo. Participaron 15 expertos en la validación realizada por el método Delphi Digital Simplificado, en el estudio de confiabilidad colaboraron 254 estudiantes. Los resultados indican que se obtuvo un coeficiente V de Aiken superior a 0.8 para cada ítem, lo que indica una validez aceptable, respecto al análisis de confiabilidad, los ítems obtuvieron puntuaciones mayores a 0.8 en el coeficiente Omega de McDonald. Lo anterior confirma que se elaboró un instrumento válido y fiable que permite medir de forma consistente la ASD.

ABSTRACT. The use of digital technology is essential to participate in the knowledge society, however, there is no certainty that university students have sufficient literacy to do so safely. In this article, the reliability of an instrument to assess Digital Security Literacy (DSL) from the complex thinking approach was developed, validated, and analyzed. 15 experts participated in the validation carried out by the Simplified Delphi Digital method, 254 students collaborated in the reliability study. The results indicate that an Aiken V coefficient greater than 0.8 was obtained for each item, which indicates acceptable validity. Regarding the reliability analysis, the items obtained scores greater than 0.8 in Cronbach's alpha and McDonald's Omega coefficients. This confirms that a valid and reliable instrument was developed that allows for consistent measurement of DSL.

PALABRAS CLAVE: Alfabetización digital, Educación superior, Innovación educativa, Pensamiento complejo, Seguridad digital.

KEYWORDS: Digital literacy, Higher education, Educational innovation, Complex thinking, Digital security.

George-Reyes, C. E.; Rocha-Estrada, F. J.; Glasserman-Morales, L. D.; Avello-Martínez, R. (2024). Evaluación de la seguridad digital para la complejidad en estudiantes universitarios: diseño y validación del instrumento Complex-ADS. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(1), 37-50.
https://doi.org/10.54988/cisde.2024.1.1311

1. Introducción

Las tecnologías de la información y comunicación (TIC) son herramientas fundamentales para el desarrollo de los individuos y de las sociedades al facilitar la transformación de la información en conocimiento, en los últimos años su presencia en las actividades formativas se intensificó gracias al uso masivo del Internet (INEGI, 2022). Asimismo, este incremento se multiplicó debido a la aparición de la pandemia del COVID-19 que obligó a las personas no solamente a permanecer en sus hogares, sino también a participar en modalidades nos presenciales de llevar a cabo actividades laborales, de entretenimiento y de educación basadas en el uso de herramientas tecnológicas (Valle & Basilio, 2020).

Esta transformación de los entornos de participación propició un aumento asociado con los riesgos de seguridad digital en los ambientes virtuales (Ismailova et al., 2019), así como debates en torno a cuáles son los niveles de alfabetización que necesitan tener las personas para desenvolverse sin peligro en la sociedad digital (Figueroa et al., 2019; Salado et al., 2019). En este sentido, la alfabetización en seguridad digital es un conjunto de habilidades o competencias necesarias para participar con éxito en ambientes digitales y virtuales en los que se requiere realizar actividades como registrar y compartir datos e identidad personal (List, 2019).

Este concepto también hace referencia a la adquisición de habilidades y actitudes relacionadas con la búsqueda, comprensión, creación y comunicación de productos e información utilizando tecnologías digitales (Macià & Garreta, 2018), así como la habilidad para proteger los activos digitales a través del tratamiento de amenazas desde la perspectiva de los sistemas de información, así como de los usuarios (Ghafir et al, 2018; ISACA, 2015) e implica realizar mejores prácticas digitales y utilizar apropiadamente herramientas tecnológicas para la autoprotección (DQInstitute, 2018).

Así como las herramientas tecnológicas brindan una amplia gama de oportunidades para acceder a la formación profesional mediante el uso de plataformas educativas, privilegiar el aprendizaje adaptativo, establecer canales de comunicación inmediata y permitir evidenciar el aprendizaje mediante diversos formatos de entrega, también admiten la aparición de amenazas digitales como la suplantación de la identidad, el robo de datos personales y distintos tipos de delitos cibernéticos (Mikelic et al., 2016), por lo que los usuarios deben estar alfabetizados para afrontarlas con éxito (Ismailova & Muhametjanova, 2016; Vitak et al., 2018) y cultivar la ciberseguridad para hacer un uso cauteloso del internet basado en la mitigación del riesgo (Pangrazio & Cardozo, 2020).

Por otra parte, debe señalarse que los riesgos relacionados con el uso de internet cada vez son más complejos por lo que no es suficiente abordarlos desde sus componentes elementales como la construcción del conocimiento, los derechos y la identidad digital y la privacidad personal (Ata & Yildirim, 2019; Nasrullah & Baharman, 2018; Postigo, 2013; Moreno et al., 2018; Pangrazio & Selwyn, 2019) y desde las amenazas que se derivan de ellos como el ciberacoso, el sexting, el grooming, las noticias falsas y la vulneración de los datos personales (Gamito et al., 2017; Na-Nan et al., 2019; Tomczyk, 2019).

Es necesario observar a la seguridad digital desde un enfoque de pensamiento complejo (PC) el cual aglutina un conjunto de habilitadores que sirven para tomar decisiones académicas más acertadas en una amplia gama de disciplinas (Vázquez et al., 2022), este tipo de pensamiento comprende 4 subdimensiones que pueden observarse en la Figura 1, estás son: el pensamiento científico (PCT), crítico (PCR), sistémico (PS) e innovador (PI) (Ramírez et al., 2022), que habilitan a los estudiantes para participar en educación y la sociedad del conocimiento que están inmersas en ecosistemas de interacción digital (Miranda et al., 2021).

George-Reyes, C. E.; Rocha-Estrada, F. J.; Glasserman-Morales, L. D.; Avello-Martínez, R. (2024). Evaluación de la seguridad digital para la complejidad en estudiantes universitarios: diseño y validación del instrumento Complex-ADS. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(1), 37-50. https://doi.org/10.54988/cisde.2024.1.1311

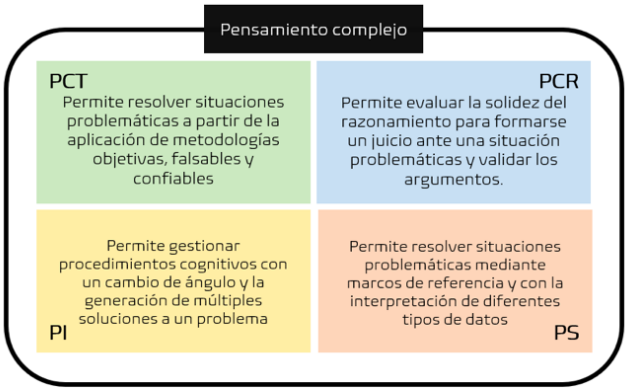

Figura 1. Componentes del pensamiento complejo. Fuente: Elaboración propia.

Por lo anterior, es ineludible formular propuestas que contribuyan a habilitar el pensamiento complejo como un mediador para fortalecer la alfabetización en seguridad digital y con ello cultivar en los estudiantes habilidades para hacer frente los riesgos inherentes a la comunicación e intercambio de contenidos en internet (Gamito et al., 2019), así como para adquirir la capacidad de reconocer los peligros relacionados con la seguridad personal en entornos virtuales (Kopecky & Szotkowski, 2017; Tomczyk, 2019; Vitak et al., 2018). En la Figura 2 se puede observar una primera aproximación a la imbricación de la alfabetización en seguridad digital con los componentes del pensamiento complejo.

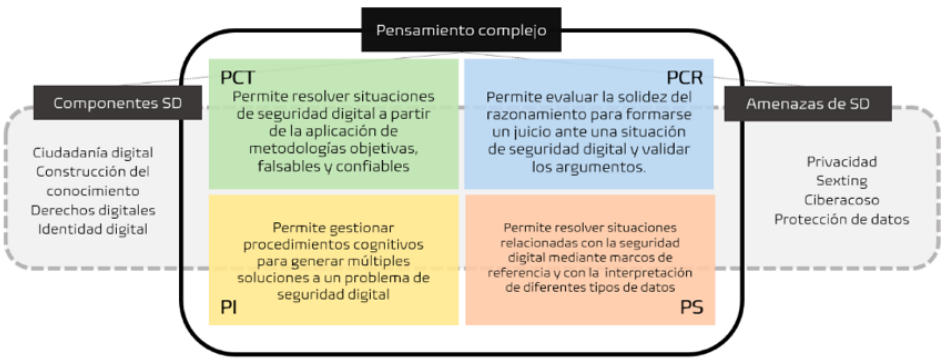

Figura 2. Imbricación de la alfabetización en seguridad digital con el pensamiento complejo. Fuente: Elaboración propia.

El propósito de este artículo es contribuir con la medición de la comprensión del tema en los estudiantes que participan en entornos y modalidades de aprendizaje mediados por el uso de tecnologías digitales y aplicaciones tanto educativas como de colaboración social en el entorno de creciente complejidad. Para lograrlo se diseñó un instrumento que imbrica los componentes del pensamiento complejo y la alfabetización en seguridad digital con la orientación de la siguiente pregunta de investigación: ¿cómo se puede elaborar un instrumento para evaluar la alfabetización en seguridad digital de estudiantes universitarios en los entornos mediados por tecnología a partir de los componentes elementales del pensamiento complejo?.

2. Metodología

La metodología utilizada fue de corte descriptiva e interpretativa, orientada para validar el contenido y analizar la consistencia interna del cuestionario Alfabetización en seguridad digital para todos en el entorno de la complejidad (eComplex-ADS). El objetivo que se ha planteado es validar y analizar la confiabilidad de un instrumento elaborado para evaluar la alfabetización en seguridad digital de estudiantes universitarios desde el enfoque del pensamiento complejo.

La investigación se desarrolló siguiendo una metodología secuencial en tres etapas, en la primera se elaboró

el cuestionario, en la segunda se validó el instrumento aplicando el Método Método Delphi Digital Simplificado (MDDS) (George-Reyes & Valerio-Ureña, 2022) y finalmente se analizó la confiabilidad mediante un análisis de factorial exploratorio para corroborar la correcta distribución de los ítems en las categorías correspondientes, también se utilizó el coeficiente Omega de McDonald para conocer la consistencia interna del instrumento (Ventura-León & Caycho-Rodríguez, 2017).

Para diseñar el instrumento se tomaron como referencia diversos cuestionarios, el primero llamado eComplexity, que tiene como objetivo medir la percepción del razonamiento complejo por medio de las subcompetencias de pensamiento sistémico crítico, científico e innovador (Vázquez et al., 2022). También se consideraron cuestionarios que han sido adaptados e implementados para conocer la alfabetización en seguridad digital (Alammary et al., 2022; Rocha et al., 2022; Hirschprung et al., 2022; Maqsood & Chiasson, 2021; Reilly, 2021). Se tomó como eje articulador a las dimensiones del pensamiento complejo mediante las cuales se propusieron ítems. En la Tabla 1 se muestra el resultado inicial de intersectar ambos constructos.

	Ciudadanía digital	Construcción del conocimiento	Derechos e identidad digital	Privacidad	Sexting	Ciberacoso	Protección de datos
Pensamiento sistémico	Ítems relacionados con utilizar marcos de referencia para realizar actividades digitales.						
Pensamiento crítico	Ítems relacionados con formarse juicios de valor respecto a la seguridad digital.						
Pensamiento científico	Ítems relacionados con la aplicación de métodos adecuados para interactuar con seguridad en internet.						
Pensamiento innovador	Ítems relacionados con seleccionar soluciones para generar prácticas de seguridad digital.						

Tabla 1. Intersección entre PC-ASD. Fuente: Elaboración propia.

Se eligió que la escala de respuesta fuera de tipo Likert de 4 opciones, sin opción de respuesta intermedia con el fin de que los encuestados posicionaran su respuesta a favor o en contra (Matas, 2018). El instrumento inicial se segmentó en cinco secciones: a) información del cuestionario y consentimiento informado, b) datos sociodemográficos de los participantes, b) pensamiento sistémico, c) pensamiento crítico, d) pensamiento científico y e) pensamiento innovador.

2.1. Análisis de datos

Se realizaron dos tipos de análisis: 1) validación de contenido por un juicio de expertos mediante el Método Delphi Digital Simplificado (George-Reyes & Valerio, 2022) y el uso del coeficiente V de Aiken y 2) análisis de confiabilidad mediante la estadística descriptiva, análisis factorial y coeficiente alfa de Cronbach y Omega de McDonald.

2.2. Análisis de validación de contenido

Una vez que se definieron las dimensiones e ítems del cuestionario, el primer paso fue comprobar la calidad de los ítems. A través del juicio de expertos se logró obtener una opinión consensuada respecto a la validez de contenido y constructo de las dimensiones y los ítems diseñados (Hult & Khan, 2020; López, 2018). En cuanto a su aplicación, el método se delineó por tres etapas: 1) conformación del grupo de expertos, 2) aplicación del MDDS y 3) descripción de los resultados de la validación (Martinez et al., 2019).

2.3. Conformación del grupo de expertos

En este estudio, participaron investigadores externos al grupo que diseñó el cuestionario con el fin de evitar sesgos en la validación. Se determinó que los participantes tendrían que cumplir con el siguiente perfil: 1) tener el grado de doctorado, 2) tener experiencia en publicación de artículos científicos de alto impacto, y 3) haber participado en la validación de al menos un instrumento. Se logró convocar a 21 profesionales que se ajustaban a las características deseables, de los cuales 15 completaron el proceso de validación. En la Tabla 2 se pueden observar los perfiles.

Código	Línea de investigación	Citas en Google Scholar	Institución
Ex1	Emprendimiento educativo	689	Universidad Autónoma de Nuevo León
Ex2	Pensamiento complejo y educación 4.0	431	Universidad Politécnica Metropolitana de Hidalgo
Ex3	Educación en línea	368	University of Leicester
Ex 4	Gamificación y tecnología educativas	265	Universidad de Salamanca
Ex	Inclusión digital	225	Colegio de Sonora
Ex6	Procesos cognitivos y emocionales en educación	211	Universidad Autónoma de Tamaulipas
Ex7	Empresas familiares	201	Universidad Popular Autónoma de Veracruz
Ex8	Estudios de género	201	Universidad Autónoma del Estado de Hidalgo
Ex9	Alfabetización digital	138	Universidad Autónoma del Estado de Hidalgo
Ex 10	Comercio internacional	114	Universidad Politécnica Metropolitana de Hidalgo
Ex11	Psicología ambiental	102	Universidad Autónoma de Nuevo León
Ex12	Psicología educativa	79	Instituto Tecnológico de Sonora
Ex13	Educación	71	Universidad Autónoma de Nuevo León
Ex14	Innovación educativa	63	Tecnológico de Monterrey
Ex15	Diseño y evaluación de interfaces instruccionales	31	Tecnológico de Monterrey

Tabla 2. Participantes en el MDDS. Fuente: Elaboración propia.

2.4. Aplicación del MDDS

Los expertos participaron en dos iteraciones: en la primera, se realizó un análisis cuantitativo de los ítems del instrumento tomando en cuenta la escala mostrada en la Tabla 3, se midió la valoración general de la escala, la validez de constructo (CTR) representada por la opinión acerca de si los ítems reflejan el significado conceptual de la alfabetización en seguridad digital, así como la validez de contenido (CNT), es decir, si el ítem fue bien redactado y es útil para evaluar la alfabetización desde el enfoque del pensamiento complejo. En la segunda iteración, se les solicitó valorar de forma cualitativa la calidad y claridad de la redacción de cada ítem con el fin de mejorarlos (López de Arana, Aramburuzabala y Opazo, 2020).

Escala	Valoración de la escala	Interpretación (CTR)	Interpretación (CNT)
1	Totalmente en desacuerdo	No es pertinente	No es tiene claridad
2	En desacuerdo	Es poco pertinente	Es poco claro
3	De acuerdo	Es pertinente	Tiene claridad
4	Totalmente de acuerdo	Tiene alta pertinencia	Tiene alta claridad

Tabla 3. Valoraciones de la escala. Fuente: Elaboración propia.

2.5. Análisis de confiabilidad

Para realizar el análisis de confiabilidad se utilizó una muestra compuesta por 254 estudiantes universitarios del Estado Federativo de Nuevo León, México. Se accedió a la muestra de forma intencionada considerando la disponibilidad para participar en el estudio. El 87% son mujeres, 12% de hombres y 2 personas se declararon no binarias. Sus edades oscilan entre los 18 y 58 años con un promedio de 21.7 años. En la Tabla 4 se muestran los análisis estadísticos realizados.

Prueba	Objetivo	Etapa
V de Aiken	Evaluar la pertinencia y claridad de los ítems	Validación
Análisis factorial	Explorar la distribución de los reactivos	Análisis de confiabilidad
Omega de McDonald	Analizar la confiabilidad del instrumento	

Tabla 4. Pruebas estadísticas realizadas. Fuente: Elaboración propia.

3. Resultados

3.1. Resultados de validación y confiabilidad

El instrumento se validó a través del método Delphi utilizando el juicio de expertos, esta estrategia busca

el consenso entre los jueces y recoge comentarios respecto a los ítems (Ayub et al., 2020), posteriormente se utilizó el coeficiente v de Aiken (Aiken, 1980) para conocer la pertinencia y claridad de los ítems. Finalmente, se realizó un análisis factorial para corroborar la correcta distribución de los ítems en las categorías correspondientes y se utilizó el coeficiente Omega de McDonald para conocer la consistencia interna del instrumento (Ventura-León & Caycho-Rodríguez, 2017).

3.1.1. Etapa inicial: construcción del instrumento

La revisión de la literatura identificó que variables como la ciudadanía digital, la construcción del conocimiento, los derechos digitales, la identidad digital y la privacidad emergen como elementos de la seguridad digital, a su vez, esta propuesta incorpora las conductas de sexting, ciberacoso y protección de datos para ver su relación con los componentes (ver Tabla 5). Se diseñó un instrumento tipo Likert con cuatro opciones de respuesta que van desde "totalmente en desacuerdo" hasta "totalmente de acuerdo" y se integró de ocho subescalas, la propuesta inicial contempló 81 ítems que se fueron sintetizando conforme avanzaron las etapas.

Factor	Definición
Ciudadanía digital	Seguir las normas de comportamiento en el mundo digital de forma segura, responsable y respetuosa (Ata & Yıldırım, 2019).
Construcción del conocimiento	Utilizar distintos recursos y herramientas tecnológicas para cumplir objetivos de aprendizaje de forma segura (Nasrullah & Baharman 2018).
Derechos digitales	Expandir los derechos del mundo real al entorno digital enriqueciéndolos y garantizando una convivencia sana (Postigo, 2013).
Identidad digital	Gestionar un perfil en línea con toda la información que se genera a partir de las interacciones relacionadas a una persona (Moreno Rodríguez et al., 2018).
Privacidad	Proteger los datos generados en internet asegurando un uso autorizado de la información (Pangrazio & Selwyn, 2019).
Sexting	El sexting consiste en intercambiar mensajes con contenido sexual de forma consensuada (Gamito Gomez et al., 2019).
Ciberacoso	El ciberacoso implica utilizar medios digitales para molestar a una persona (Rodríguez de Dios & Igartua, 2018).
Protección de datos	La protección de datos consiste en cuidar la seguridad de la información, las cuentas y los equipos al navegar en internet (Cañón et al., 2017).

Tabla 5. Factores incluidos en el instrumento. Fuente: Elaboración propia.

3.1.2. Etapa Intermedia: validación del instrumento

La validación de los ítems se realizó a través del método Delphi, donde por medio del juicio de 15 expertos se logró obtener un consenso entre los 81 ítems de las ocho subescalas, en la Tabla 6 se presentan los valores obtenidos. Además de evaluar la pertinencia y claridad, se invitó a los jueces a realizar anotaciones o propuestas de redacción para cada uno de los ítems, sus comentarios fueron analizados individualmente y en algunos casos utilizados para mejorar los ítems conservando la esencia original. En la Tabla 7 se presentan algunos ejemplos.

Elemento/ Ítems	1P	1C	2P	2C	3P	3C	4P	4C	5P	5C	6P	6C	7P	7C	8P	8C	9P	9C	10P	10C	11P	11C
Ciudadanía digital	.86	.78	.78	.69	.89	.78	.81	.72	.92	.86	.97	.94	.94	.92	.94	.92	.97	.94	.97	.89		
Construcción del conocimiento	.94	.81	.92	.83	.81	.78	.78	.75	.89	.78	.94	.92	.92	.94	.92	.92	.86	.75	.94	.97		
Derechos digitales	.94	.86	.97	.97	.97	.92	.97	.89	.92	.92	.92	.94	.94	.97	1	.92	.83	.89	.83	.86		
Identidad digital	.86	.92	.89	.89	.94	.89	.97	.97	.94	.89	.94	.92	.97	.92	.94	.86	.94	.94	.94	.97		
Privacidad	.89	.83	.89	.89	.86	.83	.86	.86	.94	.81	.92	.92	.89	.89	.92	.92	.94	.89	.94	.94		
Sexting	.89	.89	.89	.86	.86	.89	.86	.81	.89	.92	.89	.92	.78	.83	.78	.86	.83	.92	.78	.92	.81	.89
Ciberacoso	.92	.86	.92	.89	.94	.89	.86	.86	.89	.89	.89	.89	.89	.89	.89	.83	.86	.83	.89	.89		
Protección de datos	.94	.89	.97	.97	1	.97	.92	.92	1	1	.92	.81	.92	.89	1	1	1	1	.97	94		

P= pertinencia y C= claridad

Tabla 6. Coeficientes de la V de Aiken en la versión inicial del instrumento. Fuente: Elaboración propia.

George-Reyes, C. E.; Rocha-Estrada, F. J.; Glasserman-Morales, L. D.; Avello-Martínez, R. (2024). Evaluación de la seguridad digital para la complejidad en estudiantes universitarios: diseño y validación del instrumento Complex-ADS. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(1), 37-50. https://doi.org/10.54988/cisde.2024.1.1311

Ítem original	Versión modificada
1. Mis competencias digitales me permiten navegar, buscar, recopilar, organizar, sintetizar y crear información en internet	1. He desarrollado competencias digitales para sintetizar la información que encuentro en internet
2. He participado en redes de colaboración con mis compañeros y profesores para apoyar el proceso de aprendizaje	2. He participado en redes de colaboración con mis compañeros dentro de un entorno académico para apoyar el proceso de aprendizaje (grupos para comunicarnos, foros, etc.)
3. He colaborado en la construcción del conocimiento al participar en congresos académicos	3. He colaborado en la construcción del conocimiento al presentar alguno de mis trabajos en eventos académicos (congresos, talleres, webinars, etc.)
4. He contribuido en la construcción del conocimiento al escribir y socializar ensayos académicos	Parecida a la anterior. Eliminar
5. Busco respuestas y soluciones a los desafíos de la sociedad actual utilizando herramientas tecnológicas	5. Busco incorporar en mis actividades escolares el uso de tecnología
6. Tengo un blog, videoblog, canal, podcast, página o red social en la que difundo mis actividades académicas	Sin modificación
7. Evalúo la precisión, credibilidad y relevancia de la información u otros recursos que encuentro en internet	Similar a un ítem de ciudadanía digital. Eliminar
8. Utilizo aplicaciones y herramientas digitales para alcanzar mis objetivos aprendizaje	8. Uso aplicaciones y herramientas digitales para alcanzar mis objetivos de aprendizaje
9. Utilizo múltiples formas expresivas o lenguajes para comunicar y difundir la información en medios digitales	9. Utilizo múltiples formas expresivas como emojis o memes para comunicarme en medios digitales
10. Considero que la comunicación se hace más efectiva cuando se utilizan medios digitales en lugar de presenciales	10. Considero que la comunicación se hace más efectiva cuando se utilizan medios digitales en lugar de tradicionales

Tabla 7. Ajustes realizados en algunos ítems de construcción del conocimiento. Fuente: Elaboración propia.

Este ejercicio de análisis detallado por ítem se repitió en cada subescala, se eliminaron 12 reactivos considerados similares a otros y se reformularon 48 con las recomendaciones de los expertos, concluyendo con un instrumento compuesto por 69 ítems, además, se incorporaron tres preguntas abiertas por sugerencia de los jueces. Tras esta validación, se continuó con la aplicación de la escala a una muestra de estudiantes universitarios para conocer la consistencia interna del instrumento y su organización en factores, los resultados se presentan a continuación.

3.1.3. Etapa final: Análisis factorial y confiabilidad

La última fase se llevó a cabo utilizando un formulario de Google, que es una herramienta para crear formularios en línea que no requiere registro de los encuestados y permite analizar las respuestas en tiempo real. Se contempló una muestra intencional de profesores universitarios y se estableció un primer contacto para detallar las características del estudio, posteriormente, se les invitó a compartir la encuesta con sus alumnos y se recibieron respuestas por un periodo de seis semanas. Para analizar los resultados se utilizó el programa SPSS en su versión 26, se codificaron los datos y se realizaron las pruebas que se presentan a continuación.

Con el objetivo de garantizar que los ítems del instrumento se asociaron de acuerdo con constructos de la teoría se realizó un análisis factorial exploratorio de los resultados. Se usó el índice Kaiser Meyer Olkin (KMO) para evaluar la bondad de ajuste de los datos y su adecuación para realizar un análisis factorial, obteniendo un valor de .756 con una significancia en la esfericidad de Barlett de .000, por lo que no existe similitud de la matriz y es aceptable el análisis factorial (Méndez Martínez & Rondón Sepulveda, 2012). Además, se utilizó un diagrama de sedimentación para identificar de manera gráfica los componentes que más explicaban la varianza de los datos, donde se apreció que los primeros 8 componentes explican el 42% de la variación (ver Figura 3).

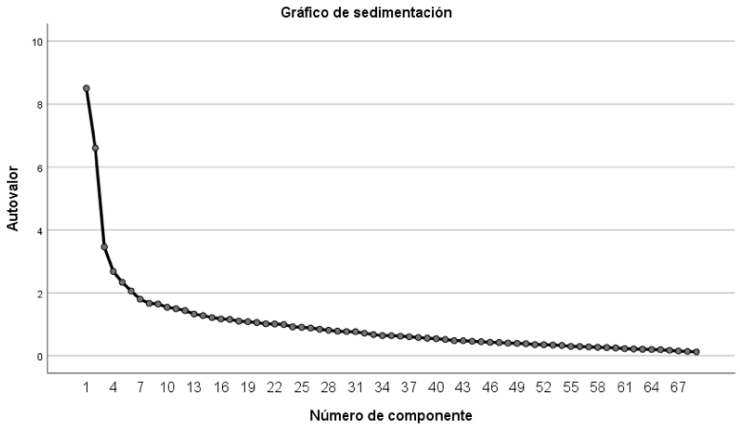

Figura 3. Gráfico de sedimentación resultado de las cargas factoriales. Fuente: Elaboración propia.

Se utilizó el método de componentes principales con extracción de ocho factores y una rotación varimax al tener una expectativa sobre cómo se agruparán las variables (Hair et al., 2010), sin embargo, al analizar los ítems, los constructos se organizaron principalmente en siete factores y se volvió a correr el análisis con esta consideración (ver Tabla 8).

Ítem	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7
1 cd	0.211					**0.371**	
4 cd				0.439	-0.164	**0.509**	
5 cd	0.179	-0.163		0.165	0.188	**0.402**	0.19
6 cd						**0.643**	-0.136
7 cd		0.118				**0.471**	
9 cd						**0.589**	0.243
1 cc				**0.49**		0.43	0.122
2 cc	0.123	0.11		**0.467**	-0.118	0.309	0.105
4 cc	0.136			**0.49**		0.372	
5 cc	**0.509**	-0.22			-0.167	0.144	-0.228
6 cc	0.294			**0.613**		0.186	
2 dd	0.165	0.223	0.21	**0.481**			
5 dd	0.406		-0.131	**0.462**	-0.109	0.144	
1 id	**0.428**					0.128	0.232
2 id	**0.662**	-0.118					
3 id	**0.503**	-0.107				0.212	
5 id	**0.417**			0.122	-0.152	0.131	
8 id	**0.602**			0.118			
1 p		0.157	-0.219	-0.178	**0.526**		
2 p	-0.155		0.207	-0.168	**0.503**		0.199
3 p	-0.324	0.237			**0.499**		
5 p	-0.167	0.103			**0.564**		
6 p	0.31				**0.45**	-0.111	-0.186

George-Reyes, C. E.; Rocha-Estrada, F. J.; Glasserman-Morales, L. D.; Avello-Martínez, R. (2024). Evaluación de la seguridad digital para la complejidad en estudiantes universitarios: diseño y validación del instrumento Complex-ADS. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(1), 37-50. https://doi.org/10.54988/cisde.2024.1.1311

Ítem	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7
8 p		0.136			**0.605**		
1 s	-0.105		**0.714**		0.108		
2 s	0.125		**0.831**				
3 s			**0.819**		0.107		
6 s	-0.105	0.495	**0.51**	0.226			
7 s		0.158	**0.576**	0.108	0.107	-0.114	
8 s		0.366	**0.417**	0.276		-0.138	
1 ca		**0.624**	0.138	0.177			
2 ca	-0.256	**0.65**					0.131
3 ca	-0.119	**0.803**	0.217				
4 ca		**0.747**	0.117		0.115		
5 ca		**0.757**			0.15		
6 ca		**0.74**			0.113		-0.101
1 pd	0.27			0.327	0.143		**0.354**
3 pd	0.352			0.213	0.162		**0.475**
5 pd			-0.162				**0.603**
6 pd	-0.134	0.252	-0.197	0.208	0.302	-0.162	**-0.334**
7 pd	0.209	-0.236			-0.143		**0.395**
8 pd		0.145	-0.134	0.103	-0.121		**0.42**

cd= ciudadanía digital, cc= construcción del conocimiento, dd= derechos digitales, id= identidad digital, p= privacidad, s= sexting, ca= ciberacoso, pd= protección de datos.

Tabla 8. Carga factorial de los ítems. Fuente: Elaboración propia.

Se analizaron detalladamente cada uno de los ítems para ver cómo se podrían agrupar de acuerdo con sus cargas factoriales. Los componentes construcción del conocimiento y derechos digitales fueron los que alcanzaron menos ítems, con cuatro cada uno, tras revisar la redacción se tomó la decisión de eliminar el componente de derechos digitales y colocar sus ítems en otros factores según la carga de cada uno de ellos. También, se contempló utilizar la misma cantidad de ítems en cada componente para medir los constructos, como sugieren Lloret-Segura y colaboradores para evitar ser redundantes en la misma idea (2014), por lo que para determinar cuáles ítems incluir en cada factor se fueron eliminando los reactivos con las cargas factoriales más bajas hasta alcanzar seis ítems por factor. En la Tabla 9 se presentan los coeficientes de la V de Aiken y la carga factorial de la versión final del instrumento.

Elemento	V de Aiken		Carga factorial	Elemento	V de Aiken		Carga factorial
	Pertinencia	Redacción			Pertinencia	Redacción	
1 cd	.86	.78	0.371	4 cd	.97	.94	0.643
2 cd	.81	.72	0.509	5 cd	.94	.92	0.471
3 cd	.92	.86	0.402	6 cd	.97	.89	0.589
1 cc	.94	.81	0.490	4 cc	.92	.92	0.613
2 cc	.92	.83	0.467	5 cc	.97	.97	0.481
3 cc	.89	.78	0.490	6 cc	.92	.92	0.462
1 id	.86	.92	0.428	4 id	.94	.89	0.417
2 id	.89	.89	0.662	5 id	.94	.92	0.509

Elemento	V de Aiken		Carga factorial	Elemento	V de Aiken		Carga factorial
	Pertinencia	Redacción			Pertinencia	Redacción	
3 id	.94	.89	0.503	6 id	.94	.97	0.602
1 p	.89	.83	0.526	4 p	.94	.81	0.564
2 p	.89	.89	0.503	5 p	.92	.92	0.450
3 p	.86	.83	0.499	6 p	.92	.92	0.605
1 s	.89	.89	0.714	4 s	.83	.92	0.510
2 s	.89	.86	0.831	5 s	.78	.92	0.576
3 s	.89	.92	0.819	6 s	.81	.89	0.417
1 ca	.92	.86	0.624	4 ca	.78	.86	0.747
2 ca	.89	.89	0.650	5 ca	.86	.83	0.757
3 ca	.78	.83	0.803	6 ca	.89	.89	0.740
1 pd	.94	.89	0.354	4 pd	.92	.81	0.334
2 pd	1	.97	0.475	5 pd	.92	.89	0.395
3 pd	1	1	0.603	6 pd	1	1	0.420

cd= ciudadanía digital, cc= construcción del conocimiento, id= identidad digital, p= privacidad, s= sexting, ca= ciberacoso, pd= protección de datos.

Tabla 9. Coeficientes de la V de Aiken y carga factorial en la versión final del instrumento. Fuente: Elaboración propia.

Finalmente, para evaluar la confiabilidad del instrumento se utilizó el índice Omega de McDonald, alcanzando un valor de .834, los valores entre .70 y .90 demuestran una alta consistencia interna, por lo tanto, indican que miden de manera confiable las percepciones de los participantes (Campo-Arias & Oviedo, 2008; Ventura-León & Caycho-Rodríguez, 2017). Este instrumento cuenta con 42 reactivos tipo Likert con cuatro opciones de respuesta y consta de siete subescalas, las primeras cuatro corresponden a los componentes de la alfabetización en seguridad digital, se integran de la ciudadanía digital, la construcción del conocimiento, la identidad digital y la privacidad, mientras que las últimas tres hacen referencia a las conductas de sexting, ciberacoso y protección de datos. El instrumento final se puede observar en la Tabla 10.

Dimensión	Ítem
Ciudadanía digital	1. He realizado algún trámite utilizando plataformas digitales (documentos de identidad como pasaporte o clave única de registro de población-CURP, servicios fiscales como pago de impuestos o actualización de datos, etc.)
	2. Mis estándares de conducta me han permitido participar con cordialidad en ambientes digitales (redes sociales, plataformas virtuales, foros, etc.)
	3. Generalmente puedo diferenciar la información verdadera de la falsa a través de su autor o de dónde se publicó
	4. He realizado sin problemas compras en internet utilizando plataformas como Mercado libre, Amazon, Marketplace de Facebook, tiendas departamentales en línea, etc.
	5. Puedo descargar los programas y las aplicaciones que necesito sin pedir ayuda
	6. Considero que tengo las habilidades para manipular fácilmente distintos dispositivos digitales (computadora, teléfono inteligente, tableta, etc.)
Construcción del conocimiento	1. He desarrollado competencias digitales para sintetizar la información que encuentro en internet
	2. He participado en redes de colaboración con mis compañeros dentro de un entorno académico para apoyar el proceso de aprendizaje (grupos para comunicarnos, foros, etc.)
	3. Busco incorporar en mis actividades escolares el uso de tecnología
	4. Uso aplicaciones y herramientas digitales para alcanzar mis objetivos de aprendizaje
	5. Respeto los derechos de autor al citar las obras digitales que utilizo en mi proceso de aprendizaje
	6. He expresado libremente mis opiniones respecto a temas que me interesan utilizando las redes sociales

George-Reyes, C. E.; Rocha-Estrada, F. J.; Glasserman-Morales, L. D.; Avello-Martínez, R. (2024). Evaluación de la seguridad digital para la complejidad en estudiantes universitarios: diseño y validación del instrumento Complex-ADS. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(1), 37-50. https://doi.org/10.54988/cisde.2024.1.1311

Dimensión	Ítem
Identidad digital	1. Reconozco que eliminar mis registros de navegación (cookies, historial, etc.) ayuda a borrar el rastro que deja mi actividad en internet
	2. Monitoreo periódicamente los resultados que arroja una búsqueda de mi nombre en internet para conocer mi identidad digital
	3. He tomado acciones para personalizar mis perfiles y distinguirme de homónimos (personas que se llaman igual que yo)
	4. He diseñado diferentes identidades digitales de acuerdo con el contexto para el que las utilizo (personal, académico, profesional, etc.)
	5. Tengo un blog, videoblog, canal, podcast, página o red social en la que difundo mis actividades académicas
	6. Modifico mis contraseñas constantemente para cuidarme del robo de identidad
Privacidad	1. He compartido intencionalmente alguna de mis contraseñas con otras personas
	2. Publico fotografías de mi entorno en las redes sociales (casa, escuela, trabajo, etc.)
	3. Comparto información personal como direcciones o teléfonos en plataformas digitales
	4. Mis perfiles en redes sociales son públicos, es decir, cualquier persona puede acceder a mi información
	5. Acepto los términos y condiciones de uso en aplicaciones, programas y páginas sin leerlos en su totalidad
	6. He ingresado a mis cuentas personales de correo, plataformas digitales o redes sociales desde equipos de acceso público (bibliotecas o cibercafés)
Sexting	1. He recibido mensajes con contenido sexual de forma consensuada (texto, imágenes, audio o video)
	2. He enviado mensajes con contenido sexual de forma consensuada (texto, imágenes, audio o video)
	3. He realizado sexting
	4. Sextear es una actividad frecuente en mis prácticas sociales
	5. Sextear es parte de estar en una relación de pareja
	6. Considero que sextear es una actividad segura
Ciberacoso	1. He realizado comentarios desagradables o hirientes hacia otras personas a través de medios digitales
	2. He realizado amenazas por medios digitales
	3. He hecho declaraciones dañinas, falsas o crueles sobre una persona en internet
	4. He utilizado un perfil falso para pretender ser otra persona y causar problemas
	5. He participado en la propagación de rumores sobre alguna persona dentro de plataformas digitales
	6. He publicado un comentario, fotografía o video en el perfil de alguien dentro de una red social con la intención de insultar o humillar
Protección de datos	1. La mayoría de las veces diseño contraseñas seguras para ingresar a mis cuentas (correo, redes sociales, apps, etc.)
	2. Descargo información, software o archivos de internet solo de sitios confiables y acreditados
	3. Evito abrir enlaces en correos electrónicos de desconocidos
	4. He compartido información en sitios web sin verificar que cumplan con los protocolos de seguridad (SSL, "https: //", un icono de candado junto a la dirección)
	5. Tengo el hábito de pasar el cursor sobre un enlace de internet antes de darle clic para ver a dónde se dirige
	6. Instalo en mi teléfono móvil o tableta aplicaciones solo desde repositorios oficiales como App Store, Play Store, App Gallery, Aurora Store, etc.

Tabla 10. Instrumento final Complex-ASD. Fuente: Elaboración propia.

4. Conclusiones

La pandemia del COVID-19 obligó a las personas a trasladarse a entornos virtuales para continuar con sus actividades, sin embargo, no todas contaban con los conocimientos necesarios para desenvolverse en estos escenarios de forma segura. En este contexto, el sexting, el ciberacoso, las noticias falsas y el robo de identidad, entre otras amenazas, son cada vez más frecuentes (Gamito et al., 2017; Na-Nan et al., 2019; Tomczyk, 2019). Hoy en día, las herramientas tecnológicas son indispensables para todo tipo de actividades y las

amenazas digitales se han vuelto más difíciles de detectar, por lo que la seguridad digital se ha vuelto un requisito indispensable para cualquier usuario que quiera utilizar las nuevas tecnologías de forma segura (Vitak et al., 2018). Así, todas las personas que deseen participar de forma activa en la sociedad requieren adquirir una alfabetización en seguridad digital que les permita reconocer y afrontar los peligros de la red.

Esta investigación identificó que la ciudadanía digital, la construcción del conocimiento, la identidad digital y la privacidad son elementos clave para desarrollar la alfabetización en seguridad digital. Lo anterior coincide con lo reportado por otros autores interesados en el tema (Ata & Yıldırım, 2019; Moreno Rodríguez et al., 2018; Nasrullah & Baharman 2018; Pangrazio & Selwyn, 2019), sin embargo, también se proponen las conductas de sexting, ciberacoso y protección de datos para ver de qué manera son influenciadas por los componentes de la alfabetización en seguridad digital. Además, la seguridad digital se observa desde el pensamiento complejo y sus subdimensiones del pensamiento científico, crítico, sistémico e innovador, por lo que a partir de ellas también se pueden desarrollar las habilidades para hacerle frente a los peligros de la red (Miranda, et al., 2021).

Para validar el instrumento se utilizó el método Delphi a través del juicio de expertos, donde los evaluadores alcanzaron un consenso respecto a la claridad y pertinencia de los ítems de las subescalas mediante la prueba V de Aiken, en la Tabla 5 se pueden observar las principales aportaciones de los expertos para mejorar la calidad de la redacción de los ítems, lo que ayudo a tener un instrumento que aporta claridad y pertinencia para evaluar la alfabetización en seguridad digital.

Se realizó un análisis factorial exploratorio para verificar la correcta distribución de cada uno de los ítems, los correspondientes a la subescala derechos digitales tuvieron cargas factoriales bajas, o se orientaron a otros componentes, por lo que se tomó la decisión de eliminar ese elemento, finalizando con un instrumento de siete componentes con cuarenta y dos (42) reactivos. El análisis factorial permite conocer la distribución de los ítems de acuerdo con los constructos y es utilizado en el diseño de pruebas psicométricas (Méndez Martínez & Rondón Sepulveda, 2012). Finalmente se calculó la consistencia interna con el índice Omega de McDonald, obteniendo un puntaje de .834. Esta prueba considera con una alta consistencia interna los valores entre .70 a .90 y fue seleccionada porque prioriza la factorización de los datos sobre la varianza (Ventura-León & Caycho-Rodríguez, 2017). Además, el índice Omega de McDonald es una alternativa al Alpha de Cronbach cuando el número de ítems es muy grande, en este caso es más eficiente.

Sin embargo, como puede observarse en la Tabla 6, durante el análisis factorial uno de los elementos clave reconocidos por la teoría como un componente de la alfabetización en seguridad digital no tuvo cargas lo suficientemente fuertes, ya que solamente dos ítems de los derechos digitales tuvieron puntajes altos, sin embargo, esto no comprometió la calidad el instrumento ya que el coeficiente V de Aiken para cada ítem estuvo cercano a 0.9.

De acuerdo con los resultados que se muestran en la Tabla 7, se puede observar que la validación fue exitosa debido a que las valores del coeficiente de V de Aiken supera el 0.8 para todos los ítems, por lo que se concluye que la escala Complex-ADS cuenta con las propiedades psicométricas para evaluar la seguridad digital en los escenarios emergentes de aprendizaje de forma confiable. Esta propuesta se construyó a partir de los cuatro habilitadores del pensamiento complejo, por lo que los estudiantes que tengan estas habilidades bien desarrolladas podrán participar en la sociedad del conocimiento de forma segura.

El instrumento diseñado es una aportación no solamente al área de la seguridad digital, sino también al pensamiento estratégico, por lo anterior tiene posibilidades para ser utilizado no solamente en el nivel de educación superior, sino adaptado en cualquier nivel educativo con el fin de identificar niveles de alfabetización en seguridad digital y a partir de ello elaborar propuestas formativas que permitan escalar las habilidades indispensables para construir una cultura que prevenga el riesgo en el ciberespacio.

Una de las limitaciones del instrumento tiene que ver con el contexto geográfico para el cual fue diseñado,

es decir, para estudiantes latinoamericanos, sin embargo, representa una semilla para realizar revalidaciones que lo posicionen en el contexto internacional. Futuras investigaciones podrían aplicar este instrumento para conocer cómo se desarrolla la alfabetización en seguridad digital en distintas poblaciones con el fin de realizar estudios comparados que permitan encontrar divergencias y convergencias en el estudio de la alfabetización en seguridad digital. Además, cada uno de los componentes o comportamientos también puede ser utilizado de forma independiente para integrarse a otras escalas.

Agradecimientos

Los autores agradecen el apoyo financiero del Tecnológico de Monterrey a través del "Challenge-Based Research Funding Program 2022". Project ID # I004 - IFE001 - C2-T3 – T.

Cómo citar este artículo / How to cite this paper

George-Reyes, C. E.; Rocha-Estrada, F. J.; Glasserman-Morales, L. D.; Avello-Martínez, R. (2024). Evaluación de la seguridad digital para la complejidad en estudiantes universitarios: diseño y validación del instrumento Complex-ADS. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(1), 37-50. https://doi.org/10.54988/cisde.2024.1.1311

Referencias

Aiken, L. (1980). Content Validity and Reliability of Single Items or Questionnaires. Educational and Psychological Measurement, 40(4), 955-959. doi:10.1177/001316448004000419.

Alammary, A.; Alshaikh, M.; Pratama, A. R. (2022). Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic. PeerJ Computer Science, 8. doi:10.7717/peerj-cs.1021.

Ata, R.; Yıldırım, K. (2019). Turkish Pre-service Teachers' Perceptions of Digital Citizenship in Education Programs. Journal of Information Technology Education: Research, 18, 419-436. doi:10.28945/4392.

Ayub, E.; Mohamad, S.; Wei, G.; Luaran, J. (2020). A learning design strategy framework for content transformation using fuzzy delphi method. International Journal of Information and Education Technology, 10(12), 882-888. doi:10.18178/ijiet.2020.10.12.1474.

Cañón, V.; Clavijo, A.; Godoy, L.; Letouzé, E.; Pestre, G.; Ricard, J. (2017). Definición de la estrategia big data para el estado colombiano y para el desarrollo de la industria de big data en colombia. (http://datapopalliance.org/wp-content/uploads/2019/11/Documento2_VersionFinal_DNP.pdf).

DQInstitute (2018). Impact and research defining global standards for digital intelligence. (www.dqinstitute.org/impact-research).

Figueroa Saavedra, C. S.; Díaz Franco, M. V.; Zúñiga Faria, C. A.; Reyes Herrera, C. M.; Molina Contreras, J. E.; Lagos Hernández, R. (2019). Alfabetización digital en alumnos de la carrera de Fonoaudiología. Revista Cubana de Educación Médica Superior, 33(3), 1-14. (https://www.medigraphic.com/pdfs/educacion/cem-2019/cem193i.pdf).

Gamito Gomez, R.; Aristizabal Llorente, P.; Vizcarra Morales, M. T. (2019). Multi-screen society: an educational challenge for family and school. Prisma Social, (25), 398-423. (https://revistaprismasocial.es/article/view/2689).

Gamito, R.; Aristizabal, P.; Olasolo, M. (2017). La necesidad de trabajar los riesgos de internet en el aula. Profesorado. Revista de Currículum y Formación de Profesorado, 21(3), 409-426. (https://www.redalyc.org/pdf/567/56752489020.pdf).

George-Reyes, C.; Valerio-Ureña, G. (2022). Validación de un instrumento para medir las competencias digitales docentes en entornos no presenciales emergentes. Edutec. Revista Electrónica de Tecnología Educativa, (80), 181-197. doi:10.21556/edutec.2022.80.2315.

Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T. (2018). Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74(10), 4986-5002. doi:10.1007/ s11227-018-2337-2.

Hair, J. F. Jr.; Black, W. C.; Babin, B. J.; Anderson, R. E. (2010). Multivariate data analysis (7th ed.). Upper Saddle River, NJ: Prentice Hall. (https://digitalcommons.kennesaw.edu/facpubs/2925/).

Hirschprung, R. S.; Tayro, S.; Reznik, E. (2022). Optimising technological literacy acquirement to protect privacy and security. Behaviour and Information Technology, 41(5), 922-933. doi:10.1080/0144929X.2020.1842907.

Hult, D.; Khan, S. (2020). Social psychology and pandemics: Exploring consensus about research priorities and strategies using the delphi method. Asian Journal of Social Psychology, 23(4), 363-371. doi:10.1111/ajsp.12442.

Instituto Nacional de Estadística y Geografía (2022). Estadísticas a propósito del día mundial del internet (17 de mayo). (https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2022/EAP_Internet22.pdf).

ISACA. (2015). State of Cybersecurity: Implications for 2015. CyberSecurity Nexus. (https://www.isaca.org/education/online-events/lms_wvs0619).

Ismailova, R.; Muhametjanova, G. (2016). Cyber crime risk awareness in Kyrgyz Republic. Information Security Journal: A Global Perspective, 25(1-3), 32-38. doi:10.1080/19393555.2015.1132800.

Ismailova, R.; Muhametjanova, G.; Medeni, T. D.; Medeni, I. T.; Soylu, D.; Dossymbekuly, O. A. (2019). Cybercrime risk awareness

rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan. Information Security Journal: A Global Perspective, 28(4-5), 127-135. doi:10.1080/19393555.2019.1685142.
Kopecky, K.; Szotkowski, R. (2017). Cyberbullying, cyber aggression and their impact on the victim – The teacher. Telematics and Informatics, 34(2), 506-517. doi:10.1016/j.tele.2016.08.014.
List, A. (2019). Defining Digital Literacy Development: An Examination of Preservice Teachers' Beliefs. Computers & Education, 138, 146-158. doi:10.1016/j.compedu.2019.03.009.
Lloret-Segura, S.; Ferreres-Traver, A.; Hernández-Baeza, A.; Tomás-Marco, I. (2014). El análisis factorial exploratorio de los ítems: una guía práctica, revisada y actualizada. Anales de Psicología/Annals of Psychology, 30(3), 1151-1169. doi:10.6018/analesps.30.3.199361.
Lopez de Arana, E.; Aramburuzabala, P.; Opazo, H. (2020). Diseño y validación de un cuestionario para la autoevaluación de experiencias de aprendizaje-servicio universitario. Educación XX1, 23(1), 319-347. doi:10.5944/educXX1.23834.
López, E. (2018). The delphi method in current educational research: A theoretical and methodological review. Educación XX1, 21(1), 17-40. doi:10.5944/educXX1.15536.
Macià Bordalba, M.; Garreta Bochaca, J. (2018). Accesibilidad y alfabetización digital: barreras para la integración de las TIC en la comunicación familia/escuela. Revista de Investigación Educativa, 36(1), 239-257. doi:10.6018/rie.36.1.290111.
Maqsood, S.; Chiasson, S. (2021). Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. ACM Transactions on Privacy and Security, 24(4). doi:10.1145/3469821.
Martínez, I.; Padilla, M.; Suárez, M. (2019). Aplicación de la metodología Delphi a la identificación de factores de éxito en el emprendimiento. Revista de Investigación Educativa, 37(1), 129-146. doi:10.6018/rie.37.1.320911.
Méndez Martínez, C.; Rondón Sepúlveda, M. A. (2012). Introducción al análisis factorial exploratorio. Revista colombiana de psiquiatría, 41(1), 197-207. doi:10.1016/S0034-7450(14)60077-9.
Mikelic Preradovic, N.; Lešin, G.; Šagud, M. (2016). Investigating Parents' Attitudes towards Digital Technology Use in Early Childhood: A Case Study from Croatia. Informatics in education, 15(1), 127-146. doi:10.15388/infedu.2016.07.
Miranda, J.; Navarrete, C.; Noguez, J.; Molina, J.; Ramírez, M.; Navarro, S.; Bustamante, R.; Rosas, J.; Molina, A. (2021). The core components of education 4.0 in higher education: Three case studies in engineering education. Computers & Electrical Engineering, 93, 107278. doi:10.1016/j.compeleceng.2021.107278.
Moreno Rodríguez, M. D.; Gabarda Méndez, V.; Rodríguez Martín, A. M. (2018). Alfabetización informacional y competencia digital en estudiantes de magisterio. Profesorado, Revista de currículum y formación del profesorado, 22(3), 253-270. doi:10.30827/profesorado.v22i3.8001.
Na-Nan, K.; Roopleam, T.; Wongsuwan, N. (2019). Validation of a digital intelligence quotient questionnaire for employee of small and medium-sized Thai enterprises using exploratory and confirmatory factor analysis. Kybernetes, 49(5), 1465-1483. doi:10.1108/K-01-2019-0053.
Nasrullah & Baharman (2018). Exploring Practical Responses of M3LC for Learning Literacy. Journal of Physics Conference Series, 954(1). doi:10.1088/1742-6596/954/1/012007.
Pangrazio, L.; Cardozo-Gaibisso, L. (2020). Beyond cybersafety: The need to develop social media literacies in pre-teens. Digital Education Review, (37), 49-63. doi:10.1344/der.2020.37.49-63.
Pangrazio, L.; Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. New Media & Society, 21(2), 419-437. doi:10.1177/1461444818799523.
Postigo, H. (2013). The Digital Rights Movement: the Role of Technology in Subverting Digital Copyright. The MIT Press.
Ramírez, M.; Castillo, I.; Sanabria, J.; Miranda, J. (2022). Complex Thinking in the Framework of Education 4.0 and Open Innovation—A Systematic Literature Review. Journal of Open Innovation: Technology, Market, and Complexity, 8(4). doi:10.3390/joitmc8010004.
Reilly, C. A. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. Computers and Composition, 61. doi:10.1016/j.compcom.2021.102652.
Rochas, F.; George-Reyes, C.; Glasserman, L. (2022). Security as an emerging dimension of digital literacy for education: A systematic literature review. Journal of E-Learning and Knowledge Society, 18(2), 22-33. doi:10.20368/1971-8829/1135440.
Rodríguez de Dios, I.; Igartua, J. J. (2018). Skills of digital literacy to address the risks of interactive communication. En Information and Technology Literacy: Concepts, Methodologies, Tools, and Applications, 9(1), 621-632. doi:10.4018/JITR.2016010104.
Salado, L.; Amavisca, S.; Richart, R.; Rodríguez, R. (2019). Alfabetización digital de estudiantes universitarios en las modalidades presencial y virtual. Revista Electrónica de Investigación e Innovación Educativa, 5(1), 30-47. doi:10.5281/zenodo.3629574.
Tomczyk, L. (2019). What do teachers know about digital safety?. Computers in the Schools. 36(3), 167-187. doi:10.1080/07380569.2019.1642728.
Valle Martínez, M. D.; Basilio Rivera, R. (2020). La experiencia de la Escuela Nacional Preparatoria frente a la pandemia de COVID-19. Revista mexicana de bachillerato a distancia, 24(12), 28. doi:10.22201/cuaed.20074751e.2020.24.76820.
Vázquez, J.; Castillo, I.; Ramírez, M.; Millán, A. (2022). Development of the perception of achievement of complex thinking: A disciplinary approach in a Latin American student population. Education Sciences 12, 289. doi:10.3390/educsci12050289.
Ventura-León, J. L.; Caycho-Rodríguez, T. (2017). El coeficiente Omega: un método alternativo para la estimación de la confiabilidad. Revista Latinoamericana de Ciencias Sociales, niñez y juventud, 15(1), 625-627. (https://www.redalyc.org/journal/773/77349627039/html/).
Vitak, J.; Liao, Y.; Subramaniam, M.; Kumar, P. (2018). 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1-25. doi:10.1145/3274445.