REVISTA ELECTRÓNICA INTERUNIVERSITARIA DE FORMACIÓN DEL PROFESORADO
CONTINUACIÓN DE LA ANTIGUA REVISTA DE ESCUELAS NORMALES

http://revistas.um.es/reifop

Recepción: 12 de febrero de 2024
Aceptación: 28 de mayo de 2024

Villén-Contreras, R., Rodríguez-Moreno, J. & Agreda-Montoro, M. (2024). Validación y estudio piloto de una escala para la competencia en seguridad digital del profesorado en centros educativos desde un enfoque PLS-SEM. *Revista Electrónica Interuniversitaria de Formación del Profesorado, 27*(3), 69-84.

DOI: https://doi.org/10.6018/reifop.614841

Validación y estudio piloto de una escala para la competencia en seguridad digital del profesorado en centros educativos desde un enfoque PLS-SEM

Rafael Villén-Contreras, Javier Rodríguez-Moreno, Miriam Agreda-Montoro

Universidad de Jaén, España

Resumen

Ante los retos y desafíos actuales, como son los riesgos y amenazas inherentes al uso de internet y los dispositivos inteligentes, se hace indispensable ser competentes en seguridad digital y comportarnos éticamente en los entornos digitales. Por ello, el estudio ha tenido como objetivo diseñar y validar el instrumento COSEDI, basado en el Marco Europeo de Competencias Digitales para la Ciudadanía (DigComp). Para ello, se ha realizado un análisis basado en el modelado de ecuaciones estructurales (PLS-SEM), con una metodología de corte no experimental y cuantitativa. La muestra representativa ha quedado conformada por 497 profesores del sistema educativo público de Andalucía. Los resultados muestran la validez y fiabilidad del instrumento a través de la demostración de las relaciones causales entre los constructos de protección de datos y privacidad, protección de dispositivos, protección medioambiental y protección de la salud y el bienestar, así como la pertenencia de las variables observadas que los conforman, a través de los valores de las cargas factoriales y significancia. Por tanto, el modelo avala la idea de que las cuatro variables latentes tienen una influencia las unas sobre las otras, siendo la relación entre la protección de datos y privacidad y la protección de dispositivos la más fuerte y significativa, mientras que la más débil se da entre la protección de datos personales y protección medioambiental.

Palabras clave: Formación de profesores; competencia digital; competencia en seguridad digital y ética; DigComp.

Contacto:

Javier Rodríguez Moreno, jrmoreno@ujaen.es, Campus Las Lagunillas, s/n, Edificio C5-Despacho 228, 23071, Jaén, España.

Validation and pilot study of a scale for assessing faculty digital security competence in educational institutions using a PLS-SEM approach

Abstract

Given the current challenges and issues, such as the risks and threats inherent in the use of the internet and smart devices, it is essential to be competent in digital security and behave ethically in digital environments. Therefore, the study aimed to design and validate the COSEDI instrument based on the European Framework for Digital Competence for Citizens (DigComp). To achieve this, an analysis based on structural equation modelling (PLS-SEM) was conducted, employing a non-experimental and quantitative methodology. The representative sample consisted of 497 teachers from the public education system in Andalusia, with a pilot study involving 60 teachers, who were excluded from the final analysis. The results demonstrate the validity and reliability of the instrument by illustrating the causal relationships between the constructs of data and privacy protection, device protection, environmental protection, and health and well-being protection. This is further supported by the inclusion of observed variables, as evidenced by the values of factor loadings and significance. Thus, the model supports the idea that the four latent variables influence each other, with the relationship between data and privacy protection and device protection being the strongest and most significant, while the weakest relationship is observed between the protection of personal data and environmental protection.

Key words: Teacher training; digital competence; digital security and ethics competence; DigComp.

Introducción

La integración de las tecnologías en el ámbito educativo ha supuesto una revolución en los procesos de enseñanza-aprendizaje, lo cual ha permitido que emerjan multitud de oportunidades ligadas a la innovación, pero también ha ocasionado la aparición de nuevos retos y desafíos en la actualidad. En este contexto, la competencia digital se ha erigido como un factor clave en la formación de las personas a nivel global. Esto ha provocado que se desarrollen diferentes marcos a nivel internacional, en concreto la Unión Europea, ha desarrollado diversos marcos detallados para el desarrollo de dicha competencia. Así pues, nos encontramos con el Marco Europeo de Competencia Digital para la Ciudadanía—DigComp— (Vuorikari et al., 2022), el Marco Europeo para la Competencia Digital Docente—DigCompEDU— (Redecker, 2017) y el Marco Europeo para Organizaciones Educativas digitalmente competentes—DigCompOrg— (Kampylis et al., 2015). En este escenario, las habilidades y capacidades para hacer un uso efectivo y óptimo de las tecnologías, comprendiendo su impacto en los diferentes entornos donde se desenvuelve el individuo, y se ha convertido en un requisito esencial para participar plenamente en la sociedad.

Desde un enfoque plural y global se plantea la necesidad de educar en una ciudadanía competente digitalmente, y eso pasa indispensablemente por supera el mero uso instrumental de la tecnología o enfatizar solo en la creación de recursos, materiales o el propio conocimiento; el uso de la tecnología requiere también de reflexión. Por tanto, el rol del profesorado adquiere suma importancia como facilitador del cambio y redes digitales, por lo que es indiscutible poseer un alto nivel de competencia digital (Spyropoulou & Kameas, 2020).

A este respecto, aparece una de las áreas esenciales a trabajar para la formación de la ciudadanía y, por ende, de profesorado y alumnado, la cual es la seguridad digital. La competencia digital no solo es utilizar las tecnologías de manera adecuada, sino también emplearlas de manera responsable, crítica y ética (Gallego et al., 2019; Rodríguez, 2018). Por ello, la importancia de abordar la seguridad en el ámbito educativo se ha vuelto más crucial que nunca, quedando patente desde la pandemia de la COVID19 y todas las consecuencias que ha traído consigo.

Dicha dimensión queda referida a la protección de la información y la comunicación de las personas contra las amenazas y situaciones problemáticas generadas por el uso de las TIC (Vuorikari et al., 2022). Ésta queda ligada a términos como la privacidad, la integridad, la eficacia y optimización de la información y tecnología derivada de internet (Honig & Salmon, 2021). La convergencia de la competencia digital y la seguridad proporciona un enfoque sólido para la formación y personas capaces de abordar los desafíos digitales de manera integral (Matarrita et al., 2022)

Las amenazas y los riesgos cibernéticos, la inteligencia artificial, el aumento progresivo del ciberacoso, la explosión del uso de redes sociales y dispositivos móviles a edades cada vez más tempranas, y la apremiante necesidad de proteger la privacidad de las personas (Gumus et al., 2023), han llevado a la sociedad a poner el foco de atención en el desarrollo de estrategias efectivas para el aumento de la seguridad. Diversos estudios afirman que después de recibir la formación adecuada en seguridad digital, existe un aumento en la conciencia y el desarrollo de prácticas seguras en línea (Ferrag et al., 2019; Khan et al., 2023), por lo que es indispensable el desarrollo de experiencias formativas que promuevan, modelen y formen a la comunidad educativa como individuos responsables digitalmente (Amador et al., 2021; Gallego et al., 2019; Torres, 2023).

No obstante, no podemos referirnos a la seguridad sin anexarla a la ética digital, ya que estos dos términos se encuentran intrínsecamente conectados, ya que la primera se convierte en la infraestructura de la segunda. Por ende, mientras que la primera aborda la protección de la información, la confidencialidad y disponibilidad de datos e infraestructuras en entornos digitales (Khan et al., 2023); la segunda implica aplicar las premisas éticas necesarias para promocionar un comportamiento ético en línea, la equidad en el acceso a la tecnología y reflexionar sobre las implicaciones éticas de las decisiones que tomamos en su uso y los comportamientos en línea (Burr et al., 2020; Floridi, 2021). Por tanto, podemos decir que la seguridad digital asienta los cimientos para unos patrones conductuales éticos en el contexto digital, al comprender las implicaciones que tienen nuestras acciones en ellos (Kumar & Nanda, 2019).

Actualmente, las investigaciones llevadas a cabo sobre la temática expuesta no son tan numerosas como aquellas que han estudiado el nivel de la competencia digital ciudadana o la competencia digital docente (Cabero et al., 2022; Guillén et al., 2023), sobre todo ésta última, siendo la mayoría de las ocasiones en contextos universitarios y analizándola desde la perspectiva del profesorado en formación inicial. Al igual ocurre con respecto al estudio de la competencia en seguridad, como área de la competencia digital, pese observado aumento en los últimos años que indican la relevancia que está adquiriendo (Gallego et al., 2019; Grande de Prado et al., 2021; Khan et al., 2023; Torres & Gallego, 2022), prevalecen aquellos dirigidos a estudiantes de titulaciones universitarias referentes a educación; los cuales coinciden en la existencia de carencias formativas respecto a esta área. Sin embargo, aún son pocos las investigaciones que se centran en el profesorado de los centros escolares con profesorado en servicio, los cuales inciden en la interconexión existente entre la competencia digital ciudadana y la competencia digital docente (Chong & Pao, 2022; Gabarda et al., 2021; Ivy et al., 2019).

Por ello, el objetivo de este estudio ha sido diseñar y validar las características psicométricas de un instrumento que evalúe, a través de un modelo de causalidad, los factores o elementos que intervienen en la adquisición de la competencia en seguridad digital del profesorado del sistema público de educación andaluz, en relación a la protección de dispositivos, protección de datos personales y privacidad, protección medioambiental y protección de la salud y el bienestar.

Metodología

La metodología de investigación desarrollada es de corte no experimental y de naturaleza descriptiva, abordándose desde un enfoque transversal y materializado a través del método por encuesta, optando por un diseño ex post facto, y concretándose en el diseño y construcción de un cuestionario. El objetivo principal ha sido el de analizar la validez y fiabilidad del instrumento, el cual evalúa el nivel de competencia digital en el área de seguridad que posee el profesorado andaluz dentro del Marco Común Europeo de Competencia Digital para la Ciudadanía—DigComp. De igual manera, se pretende vincular las relaciones causales entre las variables para determinar la influencia de las diferentes dimensiones que componen el área de seguridad, constatando así los cambios que producen las variables independientes en las variables dependientes. Para ello, se establecen los siguientes objetivos específicos:

1. Validar la estructura propuesta del modelo de medición, verificando su validez y fiabilidad.
2. Evaluar la relación entre las variables del estudio mediante la validación del modelo propuesto.
3. Analizar los resultados obtenidos del estudio piloto con el fin de validar y enriquecer la comprensión de las variables identificadas en el estudio.

Población y muestra

El tamaño muestral ha sido determinado a través de un muestreo simple aleatorio, de una población total de n=107.837 de docentes, y donde todos los miembros de la población han tenido las mismas oportunidades de ser seleccionados (Hernández et al., 2014). Para ello, se implementó la fórmula para poblaciones finitas para obtener una muestra representativa, con un nivel de confianza del 95% y un margen de error del 5%, obteniendo una muestra representativa de la población, y habiéndose llevado a cabo un estudio piloto con un total de 60 docentes que fueren eliminados para el análisis final.

La muestra ha quedado conformada por un total de 497 docentes del sistema educativo público andaluz, de los cuales más del 60% son mujeres, respecto al 33% de hombres, y destacando el 1.4% residual que prefiere no decirlo. Con una media de edad de 44.89 años.

Instrumento

El instrumento fue diseñado ad hoc partiendo del Marco Común Europeo de Competencia Digital para la Ciudadanía—DigComp—en referencia al área de seguridad y las cuatro dimensiones que la componen (Vuorikari et al., 2022), dando lugar al cuestionario sobre la Competencia en Seguridad Digital "COSEDI".

En una primera fase, el instrumento fue sometido a la validación de contenido a través de juicio de expertos, siguiendo la propuesta de Escobar y Cuervo (2008), evaluando la claridad, coherencia, relevancia y suficiencia del cuestionario. De esta manera, se depuraron aquellos

ítems con una menor relación con el objetivo de estudio y se reformularon aquellos que daban lugar a confusión o mantenían cierta dificultad para ser comprendidos.

En una segunda fase, tras la revisión del juicio de expertos, el instrumento fue administrado a un grupo de docentes para llevar a cabo un estudio piloto, esto permite identificar problemáticas no previstas y perfeccionar el instrumento. Siguiendo a Viechtbauer et al. (2015) y su fórmula propuesta, se seleccionaron un total de 60 docentes del sistema educativo público andaluz, previo consentimiento informado para el tratamiento de los datos. Se realizó un análisis factorial exploratorio (AFE) para examinar la estructura subyacente del conjunto de variables, en este caso ítems, para identificar las dimensiones o variables latentes que explican la variabilidad que se puede observar en las respuestas de los encuestados. Se ponderaron y marcaron como punto de corte aquellas dimensiones cuya suma conjunta de las cargas fuese superior a 1 como valor propio y se desarrolló el método de extracción de los componentes principales.

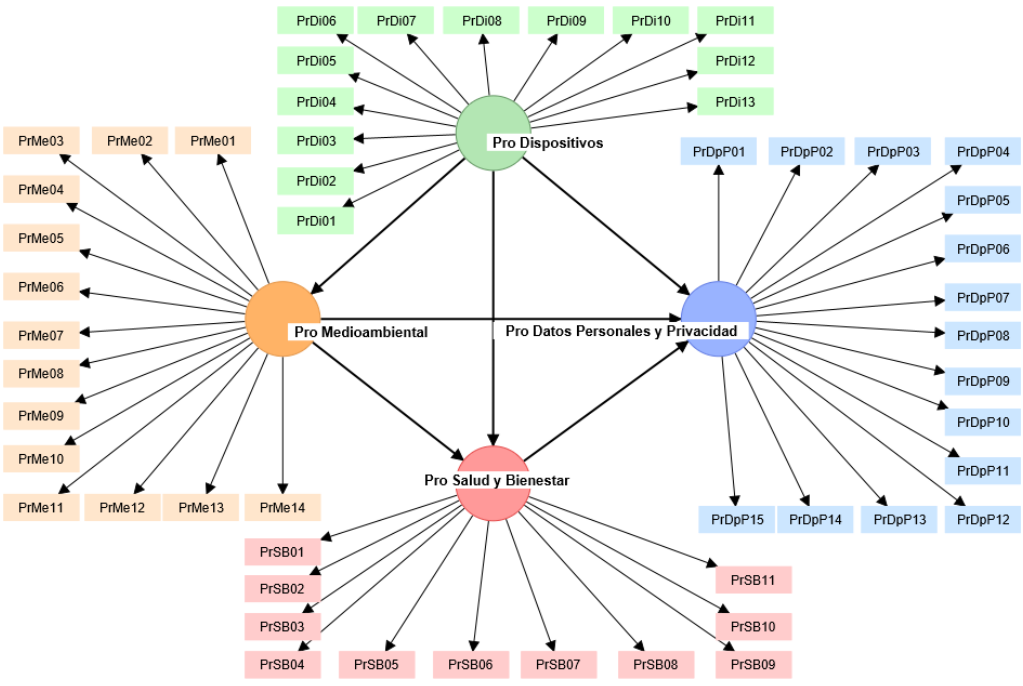
Por tanto, el instrumento de medición se compone de un total de 53 ítems repartidos en 4 dimensiones, mediante una escala tipo Likert de 4 puntos (1=Nunca; 2= A veces; 3= Casi siempre; 4= Siempre):

- PrDpP: Protección de datos personales y privacidad (15 ítems).
- PrDi: Protección de dispositivos (13 ítems).
- PrMe: Protección medioambiental (14 ítems).
- PrSB: Protección de la salud y el bienestar (11 ítems).

La causalidad a analizar sobre qué elementos o factores influyen en la adquisición de la competencia de seguridad atendiendo a la competencia digital, incluidas las relaciones que se generan entre ellos, queda recogida en la Figura 1., la cual representa la hipótesis del modelo propuesto.

Figura 1.

Hipótesis del modelo planteado. Fuente: Elaboración Propia. RStudio (2020).



Procedimiento de recogida de análisis de datos

La versión final del instrumento se trasladó a formato digital para facilitar su aplicación a la población seleccionado. El profesorado participante en el estudio piloto fue eliminado de la base de datos muestral, por lo que el instrumento no les fue aplicado, evitando así sesgos y posibles errores en el estudio. De igual manera, atendiendo a la legislación vigente y a los principios éticos de investigación, los participantes fueron informados asegurando la anonimización de las respuestas, la confidencialidad y su tratamiento únicamente para fines de investigación.

El análisis estadístico se ha efectuado mediante el paquete estadístico IBM-SSPS Statistics v.26 (IBMCorp, 2019), concretamente para el modelizado de ecuaciones estructurales fue utilizado el programa SmartPLS4 (Becker et al., 2022; Ringle et al., 2024). Dicho análisis se llevó a cabo en distintas fases, en primer lugar se analizaron de forma univariante cada uno de los ítems computando las respuestas de todas las observaciones, se estimó el poder discriminativo de los ítems a partir de un análisis univariante, se comprobaron las medidas de centralidad (media y mediana) de distribución de los resultados (asimetría, curtosis y normalidad), así como, la dispersión de los valores (desviación estándar, valores máximos y mínimos y rango intercuartílico), también se empleó el análisis bivariante (correlaciones de Pearson y Rho de Spearman).

En la siguiente fase del análisis se emplearon técnicas estadísticas multivariantes, en este caso el análisis factorial exploratorio que permite la identificación de las variables o factores latentes que permiten agrupar los ítems de la escala en cuestión, para comprobar si la estructura a priori se ajustaba con la original propuesta se realizó un análisis factorial confirmatorio que permite la comprobación de los supuestos teóricos.

Para la estimación del modelo se ha empleado el método PLS-SEM utilizando el software SmartPLS4. El enfoque PLS-SEM es de análisis multivariante que se utiliza para estimar modelos con constructos o variables latentes. Se ha realizado un análisis de multicolinealidad así como de los pesos de las componentes y los ítems. Se ha analizado la capacidad predictiva del mismo y las distintas relaciones entre las variables latentes. Por tanto, se ha realizado el siguiente análisis: a) Evaluación de la colinealidad de los constructos, b) Estudio de los coeficientes beta o path de las ecuaciones estructurales, c) Estudio de las hipótesis objeto de estudio y su interpretación, d) Calculo del tamaño del efecto de cada una de las asociaciones. Todo ello para la validación del modelo propuesto (Figura 1.)

Resultados

Validez y fiabilidad del modelo de medida

Con el fin de alcanzar el objetivo basado en la validación de la estructura del modelo propuesto, se confirma que la fiabilidad de los constructos verifica que los indicadores o ítems que se han asociado a cada una de las variables latentes, en este caso estudios, indican que valores por encima de .6 y .7 son aceptables para modelos exploratorios. Para la herramienta creada todos los valores están por encima de .770, si tenemos en cuenta la fiabilidad compuesta, todos los valores están por encima .827 lo que se considera fiable (González & Pazmiño, 2015).

Por otro lado, la validez discriminante permite verificar que los constructos sean diferentes entre ellos, se espera que los valores estén por encima de 0.5, en nuestro caso ninguna de las variables latentes cumple dicho criterio, por lo que podemos decir que los constructos guardan relación entre sí. Con respecto al Fornell and Lacker's, no en todos los casos los

valores de la diagonal son superiores a los valores de cada constructo, por ejemplo, para PrDpP, el valor de la diagonal (raíz cuadrada de AVE) es inferior que el poder discriminante de PrDi y PrSB. Atendiendo a los valores HTMT todos los valores están por debajo de .850, por lo que a través de este indicador sí podríamos afirmar que tenemos fiabilidad.

Tabla 2

Validez por constructos

Constructo	Alfa Cronbach	Fiabilidad Compuesta	AVE
PrDpP	.858	.883	.336
PrDi	.859	.885	.376
PrMe	.895	.911	.424
PrSB	.771	.827	.310

Nota: PrDpP: Protección Datos Personales y Privacidad. PrDi: Protección Dispositivos. PrMe: Protección Medioambiental. PrSB: Protección Salud y bienestar.

Tabla 3

Validez discriminante por constructos

Constructos	PrDpP	PrDi	PrMe	PrSB
Fornell and Lacker's				
PrDpP	.579			
PrDi	.692	.613		
PrMe	.484	.392	.651	
PrSB	.677	.601	.570	.557
HTMT				
PrDi	.788			
PrMe	.546	.429		
PrSB	.800	.727	.668	

Nota: PrDpP: Protección Datos Personales y Privacidad. PrDi: Protección Dispositivos. PrMe: Protección Medioambiental. PrSB: Protección Salud y bienestar. HTMT: Heterotrait-Monotrait Ratio.

Validación del modelo estructural

Las dimensiones o factores del cuestionario se construyeron a partir de las consideraciones derivadas del análisis de la literatura establecida.

Se plantearon las siguientes hipótesis:

- H1. La percepción o puntuaciones en la autopercepción de la Protección de los Dispositivos influye en la Autopercepción de la Protección de Datos Personales y Privacidad.
- H2. La percepción o puntuaciones en la autopercepción de la Protección de los Dispositivos influye en la Autopercepción de la Protección del Medioambiente.
- H3. La percepción o puntuaciones en la autopercepción de la Protección de los Dispositivos influye en la Autopercepción de la Protección de Salud y Bienestar.
- H4. La percepción o puntuaciones en la autopercepción de la protección Medioambiental influye en la Autopercepción de la Protección de Datos Personales y Privacidad.
- H5. La percepción o puntuaciones en la autopercepción de la protección Medioambiental influye en la Autopercepción de la Protección de Salud y Bienestar.

- H6. La percepción o puntuaciones en la autopercepción de la Protección de Salud y Bienestar influye en la Autopercepción de la Protección de Datos Personales y Privacidad.

Tabla 4
Valores coeficientes Path (beta) modelo SEM según hipótesis.

	PrDpP	PrDi	PrMe	PrSB
PrDpP	-			
PrDi	.437	-		
PrMe	.113	.392	-	
PrSB	.349	.446	.396	-

Nota: PrDpP: Protección Datos Personales y Privacidad. PrDi: Protección Dispositivos. PrMe: Protección Medioambiental. PrSB: Protección Salud y bienestar.

Por ello, respecto al objetivo referido a evaluar la relación entre las variables del estudio mediante la validación del modelo propuesto, en la Tabla 5 se muestran los pesos path de las hipótesis que se han establecido de manera previa, así como el grado de significatividad de las relaciones planteadas, el tamaño del efecto, el valor de multicolinealidad y el intervalo de confianza. Respecto a la colinealidad de los indicadores (VIF) o prueba de factor de inflación de la varianza, todos los valores son menores de 2 por lo que se cumple el criterio empírico que obliga a que todos los VIF debe ser inferiores a 5 (Alin, 2010; Lavery et al., 2019). Se obtienen en todos los casos significancia estadística, por lo que en todos se reporta que es cierta la hipótesis de partida, a tener en cuenta que para H4: PrMe → PrDpP el resultado sigue siendo altamente significativo, aunque con un tamaño de efecto pequeño como vemos a continuación. Por otro lado, siguiendo a Cohen (2013), se consideran tres magnitudes en el tamaño del efecto: pequeño (f^2=.02), mediano (f^2=.15) y grande (f^2=.35). Siendo esto así, se muestra que las relaciones causales observamos como el tamaño más alto se corresponde a H3: PrDi → PrSB (.333) lo que es un tamaño de efecto mediano, seguido de H1: PrDi→ PrDpP y H5: PrMe → PrSB con valores de .299 y .262 respectivamente (medianos). Del resto de hipótesis, H2: PrDi→ PrMe y H6: PrSB → PrDpP presentan tamaños de .182 y .152 que son menores que los anteriores, pero siguen siendo medianos, por último, H4: PrMe → PrDpP presenta un tamaño de efecto pequeño (.021).

Tabla 5
Valores coeficientes Path (beta), efectos sugeridos y tamaños de efecto PLS-SEM según hipótesis

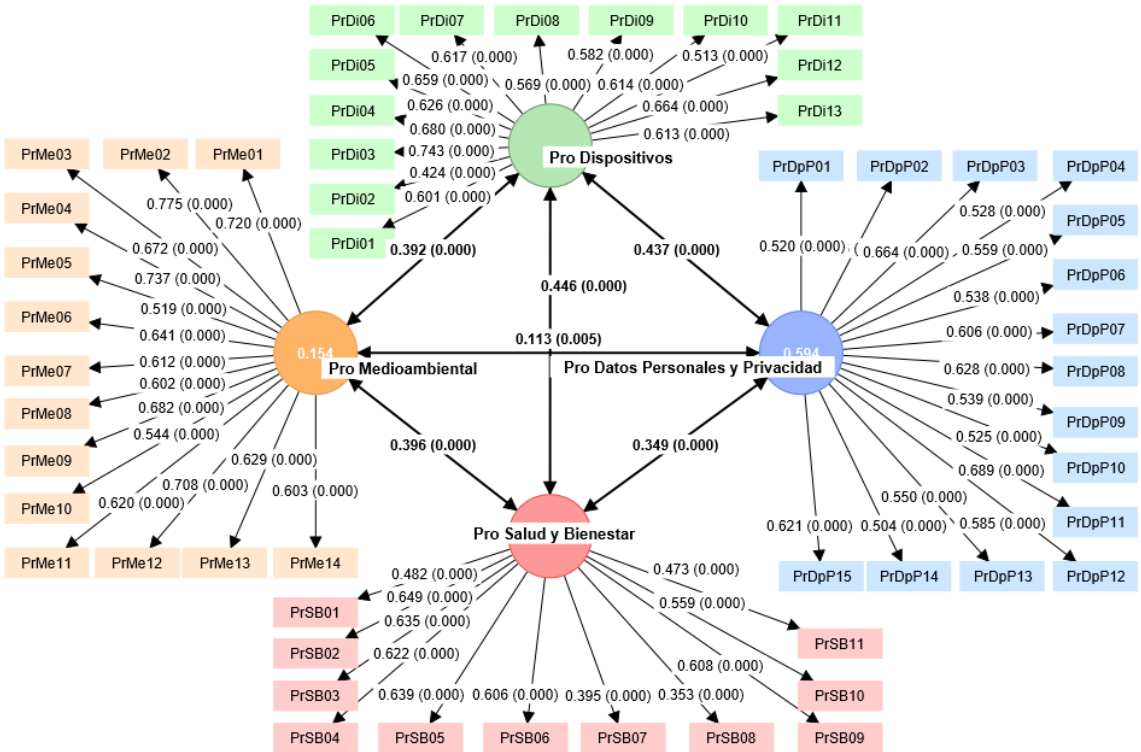
Hipótesis	Efecto Sugerido	Path Coefficients (β)	Confidence Interval	t-value (Bootstrap)	Support	f^2	VIF
H1: PrDi → PrDpP	+	.439***	[.358 - .516]	10.841 (.000)	Si	.299	1.575
H2: PrDi → PrMe	+	.397***	[.321 - .469]	10.42 (.000)	Si	.182	1.000
H3: PrDi → PrSB	+	.448***	[.375 - .518]	12.24 (.000)	Si	.333	1.182
H4: PrMe → PrDpP	+	.112***	[.034 - .191]	2.81 (.005)	Si	.021	1.491
H5: PrMe → PrSB	+	.396***	[.329 - .463]	11.52 (.000)	Si	.262	1.182
H6: PrSB → PrDpP	+	.351***	[.258 - .448]	7.24 (.000)	Si	.152	1.975

Nota: PrDpP: Protección Datos Personales y Privacidad. PrDi: Protección Dispositivos. PrMe: Protección Medioambiental. PrSB: Protección Salud y bienestar. ns = No significativo; * p < 0.05, ** p < 0.01, *** p < 0.001.

Los resultados obtenidos nos indican que el 59.4% de la varianza de la variable latente "protección de datos y privacidad" es explicada por el 43.7% por la "protección de dispositivos"; influida, aunque con moderación por el resto de las variables que se han propuesto en el modelo. Por otro lado, observamos como la influencia de la variable "protección medioambiental", respecto a la "protección de datos personales y privacidad" obtiene un 11.3%, siendo la más baja de todas. En cuanto a la relación entre las variables latentes de "protección de dispositivos" y "protección de la salud y el bienestar", se obtiene una varianza explicada de 44.6%. La tendencia se mantiene respecto a las variables latentes "protección medioambiental" y "protección de la salud y el bienestar", con una varianza de 39.6%. En referencia a la "protección de datos y privacidad" se observa cómo es explicada por la "protección de la salud y el bienestar" (34.9%). Por último, la variable latente "protección de dispositivos" queda explicada en un 33.2% por la variable "protección medioambiental". De esta manera, podemos concluir que las cuatro variables latentes tienen efecto entre sí, manteniendo una clara correlación entre ellas.

Figura 2.

Modelo ecuaciones estructurales. PLS-SEM con cargas, pesos path y significancia estadística (p-valor).



Competencia digital en seguridad y ética digital del profesorado

Para ofrecer una panorámica general del perfil competencial del profesorado en servicio se muestran los resultados más relevantes obtenidos tras la implementación del estudio piloto, llevado a cabo para la validación del instrumento, para dar respuesta así al objetivo 3, analizar

los resultados obtenidos del estudio piloto con el fin de validar y enriquecer la comprensión de las variables identificadas en el estudio. Para el establecimiento del nivel de competencia, nos basamos en los valores indicados en el DigComp, donde 1 es básico, 2 es intermedio, 3 es avanzado y 4 es altamente avanzado.

En la dimensión PrDi referida a la protección de dispositivos, el profesorado mantiene un nivel competencial cercano al avanzado ($\bar{x} = 2.73 \pm 0.86$). En la tabla 6 se presentan las medias ($\bar{x}$) y desviación estándar (S) de los ítems que se han destacado de acuerdo a los valores obtenidos. De esta manera, en la tabla 6 se muestra como el profesorado posee un nivel intermedio en cuanto a la protección de las cámaras de sus dispositivos cuando no se hace uso de ellas ($\bar{x} = 2.26 \pm 1.13$); no obstante, la desviación estándar nos indica cierta dispersión en las respuestas. En el otro extremo, nos encontramos con un nivel cercano al altamente avanzado cuando los docentes garantizan el acceso a sus dispositivos mediante diferentes métodos de seguridad ($\bar{x} = 2.67 \pm 0.75$).

En referencia a la dimensión PrDpP relacionada con la protección de datos personales y privacidad, los docentes obtienen un perfil competencial avanzado ($\bar{x} = 3.05 \pm 0.99$). De manera concreta, destacan con un nivel cercano al altamente avanzado respecto a no compartir ningún dato de información personal en sitios o web desconocidas ($\bar{x} = 3.83 \pm 0.55$); mientras que tienen una competencia básica en relación a incluir una doble capa de seguridad para el acceso a cuentas o aplicaciones ($\bar{x} = 1.64 \pm 0.83$).

Tabla 6
Nivel competencial en seguridad y ética digital.

Dimensión 1. Protección de dispositivos (PrDi)		
	$\bar{x}$	S
PrDi05. Me aseguro de que el cortafuegos está activo cuando utilizo medios electrónicos de uso público en el centro de trabajo.	2.29	±1.10
PrDi07. Considero necesario garantizar la accesibilidad a mis dispositivos mediante la utilización de métodos de seguridad como la huella digital, un patrón de desbloqueo o un código numérico	3.67	±.75
PrDi10. Considero importante cubrir la cámara de mis dispositivos cuando no estoy haciendo uso de ella.	2.26	±1.13
PrDi11. Me preocupa extraviar o sufrir el robo de alguno de mis dispositivos electrónicos.	3.53	±.77
Dimensión 2. Protección de Datos personales y privacidad (PrDpP)		
	$\bar{x}$	S
PrDpP01. Trato de no compartir información personal contraseñas, números de tarjetas de crédito, datos de identificación personal, etc. en sitios web o aplicaciones que son desconocidas.	3.83	±0.55
PrDpP06. Antes de brindar información personal, me aseguro de leer minuciosamente las políticas de privacidad de los sitios web y aplicaciones.	2.02	±0.91
PrDpP09. Evalúo el uso adecuado y respetuoso de mis datos personales y los de mi alumnado en relación a los derechos y privacidad digital.	3.64	±0.70
PrDpP15. Incluyo una doble capa de seguridad o doble factor de seguridad 2FA para el acceso a mis cuentas y/o aplicaciones digitales.	1.64	±0.83
Dimensión 3. Protección de la salud y el bienestar (PrSB)		
	$\bar{x}$	S
PrSB08. Considero el ciberacoso como una amenaza real para mi alumnado.	3.80	±0.63
PrSB09. 41. Soy consciente de que los grupos vulnerables como los niños/as o personas con falta de apoyo social corren un mayor riesgo de victimización en los entornos digitales.	3.69	±0.52
Dimensión 4. Protección medioambiental (PrMe)		
	$\bar{x}$	S

PrMe04. Enseño en el aula a proteger el medio ambiente del impacto de las tecnologías digitales, concienciando sobre la importancia de reducir nuestra huella ecológica.	2.72	±0.93
PrMe05. Cuando realizo compras en línea, verifico que las empresas contribuyen a los Objetivos de Desarrollo Sostenible ODS	1.67	±0.79
PrMe06. Valoro la importancia de reciclar correctamente los dispositivos al final de su vida útil, minimizando el impacto ambiental y permitiendo la reutilización de componentes valiosos.	3.15	±0.84

En tercer lugar, centrándonos en la dimensión PrSB basada en la protección de la salud y el bienestar, los participantes obtienen una competencia avanzada ($\bar{x} = 3.20 \pm 0.71$). A este respecto, el profesorado destaca con niveles de competencia cercanos a altamente avanzado en referencia a la concienciación sobre la amenaza del ciberacoso para su alumnado ($\bar{x} = 2.80 \pm 0.63$); así como en la concienciación existente en cuanto a la vulnerabilidad digital del alumnado con falta de apoyo social ($\bar{x} = 2.69 \pm 0.52$).

Por último, en cuanto a la dimensión PrMe orientada hacia la protección medioambiental, el profesorado tiene un nivel de competencia básico, aunque hay que destacar que se acerca a un nivel avanzado ($\bar{x} = 2.83 \pm 1.00$). Específicamente, vemos como la muestra mantiene un nivel básico en cuanto a la verificación de empresas que contribuyan a los ODS cuando realizan compras en línea ($\bar{x} = 1.67 \pm 0.79$); mientras que poseen un nivel avanzado respecto a la importancia del reciclaje de los dispositivos para la minimización del impacto ambiental ($\bar{x} = 3.15 \pm 0.84$). En último lugar, se observa como los docentes llevan a cabo prácticas en su aula dirigidas a la protección del medio ambiente del impacto tecnológico ($\bar{x} = 2.72 \pm 0.93$), con un nivel intermedio, acercándose al avanzado.

Por tanto, el modelo propuesto en este estudio posibilita la obtención de una serie de conclusiones, en primer lugar a la significatividad del propio modelo para analizar la competencia en seguridad, dentro del marco DIGCOMP, del profesorado en servicio del sistema público andaluz de educación, la cual resulta de la interrelación entre las diferentes variables latentes o dimensiones: protección de datos personales y privacidad, protección de dispositivos, protección medioambiental y protección de la salud y el bienestar. En este estudio concreto, las dimensiones concuerdan con el Marco Común Europeo de Competencias Digitales para la Ciudadanía (Vuorikari et al., 2022), en el área de seguridad y uso responsable de la tecnología, cuyo instrumento diseñado ha quedado validado a través del modelado de ecuaciones estructurales expuesto, cumpliendo así con los objetivos del estudio.

Discusión

Queda constancia de la relevancia que adquiere la seguridad como parte de la competencia digital, tanto docente como ciudadana, y cómo un nivel alto en competencia en seguridad digital aumenta la conciencia del profesorado sobre las amenazas subyacentes del uso de internet como el ciberacoso, el sexting, la suplantación de la identidad y el grooming, entre otras (Gumus et al., 2023). A este respecto, comienzan a haber estudios que indican una brecha digital de género en cuanto a esta área, siendo las mujeres aquellas que atienden de manera más pormenorizada a cuestiones relativas a la seguridad (Novella & Cloquell, 2021; Pérez et al., 2021).

Así, los sistemas educativos comienzan a dar una importancia merecida a la seguridad en Internet y al uso responsable de la tecnología, y aunque la formación universitaria y la

administración pública asumen en sus ofertas formativas, la formación relativa a la competencia digital de forma transversal, pareciera ser que aquella relativa a la seguridad presenta ciertas carencias (Griffiths & Stockman, 2022; Más et al., 2022).

Por último, esta investigación presenta una serie de limitaciones, la aplicación del instrumento se ha llevado a cabo en un territorio en concreto, Andalucía, aunque se ha obtenido un tamaño muestral representativo, no pueden generalizarse los resultados a otros contextos debido a las peculiaridades que pueden presentar otras regiones o, incluso países. En segundo lugar, no se han tenido en cuenta para este análisis variables predictivas como pueden ser el género, la edad, la experiencia docente y la etapa educativa, entre otras; lo cual puede ser interesante para obtener un modelo de mayor complejidad y profundidad.

Este estudio abre posibles y futuras líneas de investigación En concreto, nos referimos a la inclusión de las variables predictivas mencionadas anteriormente, pero también a la influencia de la seguridad digital en el resto de áreas de la competencia digital marcadas por el DigComp y DigCompEdu, para observar la relación o influencia existente entre la competencia digital ciudadana del profesorado respecto a su práctica profesional. Otra línea de investigación es replicar el estudio en otros contextos para poder establecer comparativas entre el profesorado de las diferentes regiones del territorio español. Ello puede ayudar al desarrollo profesional y actualización pedagógica del conjunto docente, pero también a la administración pública para delimitar las acciones que se requieren para cubrir las carencias formativas de su profesorado; así como a las instituciones de Educación Superior a asegurar el desarrollo de la competencia en seguridad digital y ética en los docentes en formación inicial.

Conclusiones

El modelo propuesto en este estudio posibilita la obtención de una serie de conclusiones, en primer lugar a la significatividad del propio modelo para analizar la competencia en seguridad, dentro del marco DIGCOMP, del profesorado en servicio del sistema público andaluz de educación, la cual resulta de la interrelación entre las diferentes variables latentes o dimensiones: protección de datos personales y privacidad, protección de dispositivos, protección medioambiental y protección de la salud y el bienestar. En este estudio concreto, las dimensiones concuerdan con el Marco Común Europeo de Competencias Digitales para la Ciudadanía (Vuorikari et al., 2022), en el área de seguridad y uso responsable de la tecnología, cuyo instrumento diseñado ha quedado validado a través del modelado de ecuaciones estructurales expuesto, cumpliendo así con los objetivos del estudio.

Verificación de la validez y fiabilidad del modelo

Los valores de fiabilidad han quedado probados a través de la validez de los constructos, donde la protección de dispositivos obtiene un alfa de Cronbach de .859, la protección de datos personales y privacidad un valor de .858, la protección medioambiental un .895; y la protección de la salud y el bienestar un .771. De manera global, a partir de la fiabilidad compuesta, se observa como los valores superan el .827, lo que indica un alto grado de validez y fiabilidad del instrumento de medición.

Validación del modelo y análisis entra las variables

El modelo avala la idea de que las cuatro variables latentes tienen una influencia las unas sobre las otras, siendo la relación entre la protección de datos y privacidad y la protección de dispositivos la más fuerte y significativa, mientras que la más débil se da entre la protección de datos personales y protección medioambiental. De igual manera, se comprueba la

pertenencia de las variables observadas o indicadores a cada uno de los constructos, con valores de carga que superan el 0.4 y significatividad por debajo del .05 (p-valor).

Por tanto, podemos concluir que un profesorado con una competencia sólida en seguridad digital es indispensable, ya que como defienden Matarrita et al (2022), la protección de información sensible, tanto propia como del alumnado, es esencial para prevenir los riesgos sobrevenidos por posibles violaciones de datos, por lo que la formación en seguridad digital actúa como escudo para salvaguardar dichos datos. De hecho, varios estudios indican que el profesorado tiende a almacenar datos sensibles en sus dispositivos personales, lo cual puede aumentar los riesgos de acceso no autorizado a ellos (Witsenboer et al., 2022). De igual manera, la capacidad para reconocer y poder enfrentar las amenazas inherentes a los espacios cibernéticos, protege a las infraestructuras educativas de ataques, la mayoría de ellas conectadas a través de las intranets de los centros, pero también permite el empoderamiento del profesorado para proporcionar la formación necesaria a sus estudiantes (Attai, 2020; Latorre & Tnibar, 2023).

Referencias

Alin, A. (2010). Multicollinearity. *WIREs Computational Statistics, 2*(3), 370-374. https://doi.org/10.1002/wics.84

Amador, M. P., Torres, C. A., Lagunes, A., Angulo, J., Argüello, C. A., & Medina, H. (2021). Marcos de competencias digitales relacionados con seguridad para docentes. *Pädi Boletín Científico de Ciencias Básicas e Ingenierías del ICBI, 9*(Especial), Article Especial. https://doi.org/10.29057/icbi.v9iEspecial.7490

Attai, L. (2020). Student Data Privacy: Managing Vendor Relationships. Rowman & Littlefield.

Becker, J.-M., Cheah, J.-H., Gholamzade, R., Ringle, C. M., & Sarstedt, M. (2022). PLS-SEM's most wanted guidance. *International Journal of Contemporary Hospitality Management, 35*(1), 321-346. https://doi.org/10.1108/IJCHM-04-2022-0474

Betín, A.B., Rodríguez, A., Caurcel, M.J. y Gallardo, C.P. (2022). Statistical validation of the "ECODIES" questionnaire to measure the digital competence of Colombian high school students in the subject of Mathematics. *Mathematics*, 11, 33, 11, 33. https://doi.org/10.3390/math11010033

Betín, A. B., Rodríguez, A., Caurcel, M. J., & Gallardo, C. P. (2023). Effectiveness of a digital literacy program in High School Basic education students. *Espiral. Cuadernos del Profesorado, 16*(34), 12-27. https://doi.org/10.25115/ecp.v16i34.9516

Burr, C., Taddeo, M., & Floridi, L. (2020). The Ethics of Digital Well-Being: A Thematic Review. *Science and Engineering Ethics, 26*(4), 2313-2343. https://doi.org/10.1007/s11948-020-00175-8

Cabero, J., Guillén, F. D., Ruiz, J., & Palacios, A. (2022). Teachers' digital competence to assist students with functional diversity: Identification of factors through logistic regression methods. *British Journal of Educational Technology, 53*(1), 41-57. https://doi.org/10.1111/bjet.13151

Chong, E. K., & Pao, S. S. (2022). Promoting digital citizenship education in junior secondary schools in Hong Kong: Supporting schools in professional development and action research. *Asian Education and Development Studies, 11*(4), 677-690. https://doi.org/10.1108/AEDS-09-2020-0219

Cohen, J. (2013). Statistical Power Analysis for the Behavioral Sciences. Academic Press.

Matarrita, D., Trejos, B., Qin, H., Joo, D., & Debner, S. (2022). Conceptualizing community resilience: Revisiting conceptual distinctions. En *Community Development for Times of Crisis* (pp. 34-55). Routledge.

Escobar, J., & Cuervo, Á. (2008). Validez de contenido y juicio de expertos: Una aproximación a su utilización. *Avances en medición, 6*(1), 27-36.

Ferrag, M. A., Maglaras, L., Janicke, H., & Smith, R. (2019, septiembre 1). *Deep Learning Techniques for Cyber Security Intrusion Detection: A Detailed Analysis*. 6th International Symposium for ICS & SCADA Cyber Security Research 2019. https://doi.org/10.14236/ewic/icscsr19.16

Floridi, L. (2021). Digital Ethics Online and Off: Molding the digital future as it simultaneously shapes us. *American Scientist, 109*(4), 218-223. https://doi.org/10.1511/2021.109.4.218

Gabarda, V., García, E., Ferrando Rodríguez, M. de L., & Chiappe, A. (2021). El profesorado de Educación Infantil y Primaria: Formación tecnológica y competencia digital. *Innoeduca: international Journal of Technology and Educational Innovation, 7*(2), 19–31. https://doi.org/10.24310/innoeduca.2021.v7i2.12261

Gallardo, C. P., Rodríguez, A., Caurcel, M. J., y Capperucci, D. (2020). Adaptación y validación de un instrumento de evaluación sobre la utilización de herramientas digitales en las aulas de Educación Especial. *Studi sulla Formazione, 23*(2), 161-173. http://10.13128/ssf-12058

Gallego, M.J., Torres, N., & Pessoa, T. (2019). Competence of future teachers in the digital security area. *Comunicar, 61*, 57-67. https://doi.org/10.3916/C61-2019-05

González, J., & Pazmiño, M. (2015). Cálculo e interpretación del Alfa de Cronbach para el caso de validación de la consistencia interna de un cuestionario, con dos posibles escalas tipo Likert. *Revista Publicando, 2*(1), 62-67.

Grande de Prado, M., García, F. J., Corell, A., & Abella, V. (2021). Evaluación en Educación Superior durante la pandemia de la COVID-19. *Campus Virtuales, 1*(10), 49-58.

Griffiths, P., & Stockman, C. (2022). Expanding AI's Impact with Organizational Learning. MIT Academic Conferences and publishing limited.

Guillén, F. D., Colomo, E., Ruiz, J., & Tomczyk, Ł. (2023). Teaching digital competence in the use of YouTube and its incidental factors: Development of an instrument based on the UTAUT model from a higher order PLS-SEM approach. *British Journal of Educational Technology, 0*(0), 1-23. https://doi.org/10.1111/bjet.13365

Gumus, M. M., Cakir, R., & Korkmaz, O. (2023). Investigation of pre-service teachers' sensitivity to cyberbullying, perceptions of digital ethics and awareness of digital data security. *Education and Information Technologies, 28*(11). https://doi.org/10.1007/s10639-023-11785-7

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación. McGraw Hill España. https://dialnet.unirioja.es/servlet/libro?codigo=775008

Honig, C. A., & Salmon, D. (2021). Learner Presence Matters: A Learner-Centered Exploration into the Community of Inquiry Framework. *Online Learning, 25*(2), 95-119.

Ivy, J., Lee, S. B., Franz, D., & Crumpton, J. (2019). Seeding Cybersecurity Workforce Pathways with Secondary Education. *Computer, 52*(3), 67-75. https://doi.org/10.1109/MC.2018.2884671

Kampylis, P., Punie, Y., & Devine, J. (2015). *Promoting Effective Digital-Age Learning—A European Framework for Digitally-Competent Educational Organisations* (JRC98209; JRC Research Reports). Joint Research Centre. https://publications.jrc.ec.europa.eu/repository/handle/JRC98209

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal, 36*(2), 373-405. https://doi.org/10.1057/s41284-022-00343-4

Kumar, V., & Nanda, P. (2019). Social Media to Social Media Analytics: Ethical Challenges. *International Journal of Technoethics (IJT), 10*(2), 57-70. https://doi.org/10.4018/IJT.2019070104

Latorre, M. J., & Tnibar, C. (2023). Digital Security in Educational Training Programs: A Study Based on Future Teachers' Perceptions. *Information technologies and learning tools, 95*(3), Article 3. https://doi.org/10.33407/itlt.v95i3.5204

Lavery, M. R., Acharya, P., Sivo, S. A., & Xu, L. (2019). Number of predictors and multicollinearity: What are their effects on error and bias in regression? *Communications in Statistics Simulation and Computation, 48*(1), 27-38. https://doi.org/10.1080/03610918.2017.1371750

Más, V., Gabarda, V., & Peirats, J. (2022). Competencia digital del profesorado de Educación Secundaria: Análisis del estado del arte. *REIDOCREA, 11*(35), 418-430. https://doi.org/10.30827/Digibug.76068

Novella, C., & Cloquell, A. (2021). The ethical dimension of digital competence in teacher training. *Education and Information Technologies, 26*(3), 3529-3541. https://doi.org/10.1007/s10639-021-10436-z

Pérez, A., García, R., & Lena, F. J. (2021). Brecha digital de género y competencia digital entre estudiantes universitarios. *Aula abierta, 50*(1), 505-514.

Redecker, C. (2017, noviembre 28). *European Framework for the Digital Competence of Educators: DigCompEdu*. JRC Publications Repository. https://doi.org/10.2760/178382

Ringle, Christian M., Wende, Sven, & Becker, Jan-Michael. (2024). SmartPLS 4. Monheim am Rhein: SmartPLS. Retrieved from https://www.smartpls.com

Rodríguez, A. (2018). Editorial. Expansión postmoderna tecnológica, escuela inclusiva tecnológica. *RETOS XXI,* 2, 6-12. https://doi.org/10.33412/retoxxi.v2.1.2055

Rodríguez, A., Caurcel, M.J., Gallardo-Montes, C.d.P. y Crisol, E. (2021). Psychometric Properties of the Questionnaire "Demands and Potentials of ICT and Apps for Assisting People with Autism" (DPTIC-AUT-Q). *Education Sciences*, 11 (586). https://doi.org/10.3390/educsci11100586

RStudio Team. (2020). RStudio: Integrated Development for R. RStudio, PBC, Boston, MA URL http://www.rstudio.com/

Spyropoulou, N. D., & Kameas, A. D. (2020). *Methodology for the Development of a Competence Framework for STE(A)M Educators*. EDEN Conference Proceedings. https://doi.org/10.38069/edenconf-2020-ac0014

Torres, N. (2023). Análisis de Marcos de Competencia Digital Docente para la Formación inicial de profesorado en seguridad digital. *Revista de Estilos de Aprendizaje, 16*(31). https://doi.org/10.55777/rea.v16i31.5407

Torres, N., & Gallego, M.-J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and information technologies, 27*(6), 8583-8602. https://doi.org/10.1007/s10639-022-10978-w

Viechtbauer, W., Smits, L., Kotz, D., Budé, L., Spigt, M., Serroyen, J., & Crutzen, R. (2015). A simple formula for the calculation of sample size in pilot studies. *Journal of Clinical Epidemiology, 68*(11), 1375-1379. https://doi.org/10.1016/j.jclinepi.2015.04.014

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes* (JRC Research Reports JRC128415). Joint Research Centre. https://econpapers.repec.org/paper/iptiptwpa/jrc128415.htm

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education, 186*, 104536. https://doi.org/10.1016/j.compedu.2022.104536