Technology, Knowledge and Learning
https://doi.org/10.1007/s10758-026-09954-x

ORIGINAL RESEARCH

What Digital Competencies Should Teachers Possess to Teach Educational Cybersecurity to Students in Schools? Design and Validation of a Teacher Competency Scale

Pablo de la Flor-Bancalero[1] · **Francisco David Guillen-Gamez**[1]

Received: 12 November 2025 / Revised: 18 December 2025 / Accepted: 2 January 2026

Abstract
The purpose of this study was to design and validate an instrument to assess the teaching competencies necessary to didactically teach cybersecurity and safe Internet use in educational contexts. Specifically, the following phases were addressed: content validity, Comprehension validity, construct validity through exploratory factor analysis (EFA) and confirmatory factor analysis (CFA), as well as convergent and discriminant validity, and reliability analysis through various statistical coefficients. The instrument was structured in five dimensions: (1) Basic knowledge about identification and prevention of digital threats, (2) Protection of personal information in digital environments, (3) Secure use of hardware, software and browsers, (4) Password management and authentication, and (5) Continuous updating and training of teachers in cybersecurity. The sample consisted of 754 in-service teachers from different educational levels (Early Childhood Education, Primary, Secondary, Vocational Training, and Adult Education) from all over Spain. The results showed adequate fit indices for the factorial model (KMO = 0.965; χ^2 = 18,410.047; $p < .001$), total explained variance of 82.54% and excellent internal consistency with values greater than 0.70. In addition, satisfactory convergent validity (AVE > 0.50) and discriminant validity (MSV < AVE) values were confirmed. With all these coefficients, the instrument is valid and reliable for diagnosing teachers' self-perceived level of cybersecurity and safe and responsible internet use teaching, with a total of 15 items classified into five latent factors. The instrument offers a practical tool to identify in-service teachers' training needs in educational cybersecurity and to support the planning of professional development and specific training programs based on empirical evidence.

Keywords Teaching competencies · Didactic teaching · Cybersecurity education · Safe use of the internet · Teachers · Scale

✉ Francisco David Guillen-Gamez
davidguillen@uma.es

Pablo de la Flor-Bancalero
Pabloflor@uma.es

[1] Faculty of Education Sciences, Department of Didactics and Educational Organization, University of Malaga (Spain), Blvr. Louis Pasteur, 25, 29010 Málaga, Spain

Published online: 10 February 2026

1 Introduction

The rapid development of ICT has led to a significant increase in cybersecurity risks. Sadik et al. (2020) states that with the emergence of innovations such as the Internet of Things (IoT), 5G networks and artificial intelligence (AI), opportunities for education have arisen, but this has also introduced threats that affect students and teachers. Furthermore, the expansion of new ICTs is so rapid that cyber threats are also constantly evolving (Dubinskiy, 2024), presenting growing challenges for the educational community such as fake news, phishing, malware, and identity theft, which especially affect the youngest (Jyoti, 2025; Blažič & Blažič, 2024; Ascoott, 2020).

In this context, the school becomes a crucial space since "it is essential to "teach the students how to keep the computer safe, secure, and up-to-date" (Ismail et al., 2024, p.5). That is, cybersecurity education from the initial and compulsory educational stages must focus on teaching students how to create secure passwords, be cautious when sharing personal information, and identify potential scams or malicious software (Kaban, 2021). These initiatives coincide with what was proposed by Suson (2019) who highlights the importance of starting this training from an early age to prepare students for more complex challenges in later stages. To achieve this, the awareness programs become a key piece in cybersecurity education training (Patterson et al., 2022), where "teachers are the backbone and key to the success of any learning program, so cybersecurity teachers are expected to be well-organized and welltrained in this regard" (Ismail et al., 2024, p. 5).

In educational research, competence is generally understood as the integrated combination of knowledge, skills, and attitudes that enables individuals to act effectively in specific contexts (Baartman & De Bruijn, 2011). Within the digital domain, this conceptual approach leads to the notion of digital competencies, which refers to the confident, critical, and responsible use of digital technologies for learning, work, and participation in society (Ferrari, 2013; European Commission, 2018). The development of digital competencies therefore goes beyond technical skills and includes pedagogical, ethical, and security-related dimensions, which are essential for navigating contemporary digital environments and for addressing challenges related to cybersecurity in educational settings (Torres Hernández, 2023).

The COVID-19 pandemic showed that both teachers and other educational stakeholders had an intermediate level of digital competencies (Marchisio et al., 2022; Basgall et al., 2023). This situation highlighted various problems, including privacy violations, limitations in device handling skills, massive management of personal data, and attacks on equipment and systems (Torres-Hernández & Gallego-Arrufat, 2022; Guillén-Gámez et al., 2024a, b; Tomczyk et al., 2023). Thus, cybersecurity education is intrinsically linked to the level of digital competencies possessed by teachers. Strengthening these competencies, particularly those related to cybersecurity, is essential for teachers not only to protect their own digital environment, but also to ensure students receive adequate training in safe and responsible internet use (Tomczyk, 2020).

In recent years, scientific research has reinforced the idea that professional teacher training should go beyond technical knowledge and incorporate a broad set of digital and pedagogical competencies (de la Flor Bancalero et al., 2026; Temirkhanova et al., 2024). In this regard, international bodies and frameworks, such as the European Commission (2020), through its Digital Education Action Plan 2021–2027, have identified the strengthening of

teachers' digital competence as a strategic priority for the development of an efficient digital educational ecosystem. Similarly, frameworks such as the European Digital Competence Framework for Educators (DigCompEdu) emphasize digital security and the responsible use of technology as essential components of teachers' professional competence (Redecker, 2017; INTEF, 2022). Furthermore, several empirical studies have shown that the level of digital competencies of teachers directly influences how cybersecurity and the safe use of the Internet are addressed in the classroom, which reinforces the need for systematic teacher training in this area (Takács & Pogátsnik, 2024a; Tomczyk et al., 2023; Guillén-Gámez et al., 2024a, b).

In this order of importance, several authors argue that cybersecurity education aims to develop competencies that foster effective and secure participation in digital environments (Takács & Pogátsnik, 2024a), making teacher training an essential condition for its success (Honomichl & Wagner, 2025). Consequently, the need for valid and reliable psychometric instruments and frameworks to assess teachers' digital competence specifically in relation to educational cybersecurity becomes evident.

Based on a search of various bibliographic databases and web search engines (Google Scholar, Redalyc, Dialnet, Scopus, Web of Science, and Scielo), using keywords such as "frameworks," "digital competencies for teachers," and "cybersecurity," various frameworks were identified that include dimensions linked to cybersecurity education. For example, the National Institute of Educational Technologies and Teacher Training (INTEF, 2022) adapted the DigCompEdu framework in five areas, one of which is dedicated to security (protection of devices, personal data and digital identity, health and environment). Likewise, in the European context, Kelentric et al. (2017) formulated the Professional Digital Competence Framework for Teachers, structured in eight areas, which includes the ethical competence, specifically dedicated to the safe and responsible use of technology and oriented towards building digital citizenship. More recently, the European Union Agency for Cybersecurity (ENISA) has developed frameworks such as the European Cybersecurity Skills Framework (ECSF) or the International Cybersecurity Challenge (ICC) (ENISA, 2023), which facilitate the identification and articulation of tasks, competencies, skills and knowledge associated with the roles of European cybersecurity professionals. However, these frameworks are not specifically aimed at in-service teachers and are not entirely focused on educational cybersecurity.

Therefore, it is necessary for the scientific community to have valid and reliable tools that allow us to determine the level of competency of in-service teachers in teaching and raising awareness about the importance of cybersecurity among students. However, the current scientific literature remains limited regarding instruments designed for in-service teachers, as most focus on students. To verify this, a bibliographic search for psychometric instruments was conducted under the following inclusion criteria: (1) Instruments must have some type of reliability and validation (expert or construct through EFA-exploratory factor analysis or CFA-confirmatory factor analysis, among others); (2) the studies must be recent (approximately from the last five years) so that they cover the latest trends in technology.

Table 1 presents different instruments used to assess digital competencies in cybersecurity, developed with diverse structures and methodological approaches. However, the comparative analysis highlights two main limitations. First, most existing instruments are designed for student populations, while only a few have been specifically validated for in-service teachers. Instruments created for students are mainly focused on the perspective

Table 1 Documentary review on instruments on competencies in educational cybersecurity

Authors	Focus on	Reability	Vality
Yan et al. (2021)	High school students	Cronbach's alpha	Rasch validity
Takács and Pogátsnik (2024b)	Students of technical higher education	Cronbach's alpha	AFE
Bognár and Bottyán (2024)	University students	Cronbach's alpha	EFA & CFA
Offenberger et al. (2019)	University students	Cronbach's alpha	CTT e IRT
Herman et al. (2023)	University students	Cronbach's alpha	CTT e IRT
Santhosh and Thiyagu (2024)	Teacher training college	Cronbach's alpha, Split Half Correlation	EFA & CFA
Guillén-Gámez et al. (2024a, b)	University students	Cronbach's alpha, Spearman-Brown coefficient, Two halves of Guttman, Composite reliability	EFA & CFA
Tise and McGill (2024)	Undergraduate students	Cronbach's alpha	EFA & CFA

CTT, classical test theory; IRT, item response theory; EFA , exploratory factor analysis; CFA , confirmatory factor analysis

of technology users, whereas in-service teachers also have a professional role as educators who plan, guide, and assess learning related to cybersecurity. For this reason, instruments developed for students cannot be directly applied to in-service teachers without affecting their validity. Second, not all instruments have been developed using Likert-type scale questionnaires, nor do they consistently report comprehensive psychometric validation procedures, such as construct validity through EFA and CFA, discriminant validity, or composite reliability. This limits their applicability and comparability across educational contexts and highlights the need for a specifically designed and validated instrument for assessing in-service teachers' competencies in educational cybersecurity.

Consequently, the main contribution of this study, as well as its primary objective, is the design and validation of a psychometric instrument that meets the standards of methodological rigor required in educational research. This instrument seeks to assess in-service teachers' self-perceptions of their competencies to address the teaching of educational cybersecurity in the classroom from a safe and ethical perspective.

2 Method

2.1 Design and Participants

For the psychometric creation of the instrument, an exploratory and descriptive study was carried out, based on the methodological framework of instrumental studies (Pérez y Carretero-Dios, 2005; Meroño et al., 2017). The methodological process was structured in different phases, including the EFA and CFA, with the aim of ensuring the validity and reliability of the instrument.

The study adopted a non-experimental, ex post facto design, using non-probability and purposive sampling. The sample consisted of 754 in-service teachers from all over Spain. Hair et al. (2009) stated that, as a general rule, it is necessary to have a number of observations between five and ten times greater than the number of items. Since the present sample consisted of 754 teachers and the final measurement instrument had 15 items, a ratio of 50.26 was obtained, which is well above the recommended range. From the point of view of the professional profile, the in-service teachers were distributed among the following educational stages: Early Childhood Education (6.50%, $N=49$), Primary Education (30%, $N=226$), Secondary Education (31.60%, $N=238$), Vocational Training (17.50%, $N=132$), Adults (4.80%, $N=36$), Language schools and Music Conservatories (9.70%, $N=73$). Regarding the sociodemographic characteristics of the teachers, the sample consisted of 506 women (67.10%) and 248 men (32.90%).

For data collection, the educational centers were contacted via email. Participants were provided with a link to an online questionnaire, ensuring anonymity, confidentiality, and compliance with ethical research principles at all times. This study was approved by the Ethics Committee of the University of (blind review).

2.2 Preparation of the Questionnaire and Method Used

The instrument construction process was based on an initial theoretical and empirical review of previous research, which can be found in Table 1. From this review, the instrument's conceptual dimensions were defined, which comprehensively address the main areas of competency required by teachers to promote safe cybersecurity practices in schools. The dimensions of the measurement instrument are described below:

1. Basic knowledge about identifying and preventing digital threats. It includes knowledge about malware, phishing, hacking, website security, and handling suspicious files. It also considers teachers' ability to guide students in detecting fraudulent emails, and securely managing sessions on shared devices.
2. Teacher competencies to instruct students in the protection of personal information in digital environments. It includes skills for configuring privacy permissions, restricting unwanted access, and deleting cookies and browsing data. It also covers the ability to introduce students to the use of encryption tools and other security measures aimed at protecting sensitive information.
3. Teacher competencies to instruct students in the safe use of hardware, software and browsers. This includes teachers teaching how to update operating systems and applications, secure Wi-Fi network configuration, firewall use, installation and management of antivirus or anti-malware programs, and the use of browser extensions to block malicious websites. It also includes guidance for students on how to make regular backups.
4. Teacher competencies to instruct students in password management and authentication in digital environments. This assesses the teacher's ability to explain the importance of strong passwords, encourage their regular updating, promote the use of two-factor authentication, and provide guidance on setting up secure recovery options.
5. Continuous training and updating in cybersecurity. This dimension examines teachers' willingness to continually update and provide ongoing training in educational cybersecurity.

2.3 Procedure and Verification of Assumptions

The instrument construction and validation process was carried out in four stages. In the first stage, the item database was developed based on a review of the specialized literature and the main theoretical frameworks related to the topic. Teachers responded on a seven-point Likert-type scale, ranging from 1 ("strongly disagree") to 7 ("strongly agree").

In the second stage, the items' comprehension validity and statistical quality were assessed, analyzing the distribution and normality of the data to ensure item adequacy. In the third stage, the construct validity of the instrument was examined, which was developed in two consecutive phases: AFE and CFA. The EFA was applied with the purpose of identifying the underlying factor structure and refining the instrument, using the Principal Axis Factoring method and Oblimin rotation, which allow explaining most of the common variance, and are robust methods against possible deviations from the assumption of normality (Fabrigar et al., 1999). Subsequently, the CFA was performed using structural equation modeling, employing the polychoric correlation matrix and maximum likelihood estimators, in order to verify the adequacy of the proposed theoretical model (Perry et al., 2015). In the fourth stage, and once the instrument was polished after the CFA, convergent validity was assessed, which reflects the degree to which items in the same factor measure the same latent construct, using the average variance extracted (AVE) (Cheung & Wang, 2017). Discriminant validity was also verified using the MSV index (maximum shared variance squared). Data collection was done through a Google Forms form, and statistical analyses were performed using IBM SPSS Statistics v29 and IBM SPSS AMOS v29.

Once the EFA and CFA were performed, the assumption of multivariate normality was checked. To do this, Mardia's coefficient was used, which is considered acceptable when its value is lower than the result obtained with the formula $p(p+2)$, where p represents the total number of items in the instrument (Raykov & Marcoulides, 2008). The verification was carried out by comparing the multivariate kurtosis value calculated in SPSS-Amos with the theoretical value obtained using this previous formula (Ping & Cunningham, 2013). In this case, with 15 items, the formula yielded a result of 255, while the Mardia coefficient obtained was 70.873. Therefore, since the Mardia coefficient was less than the formula value, we conclude that the multivariate normality assumption was confirmed.

3 Results

3.1 Validity of Understanding: Statistical Analysis of the ítems

Verifying normality is an essential step in the construction of psychometric instruments, since the absence of this assumption can affect the consistency of the measurements (Hair et al., 2010). In this study, the assessment of normality was conducted in two stages. First, with the Mardia coefficient, which was calculated in the previous section; and second, with the specific values for standard deviation, skewness, and kurtosis for each item, which are detailed in Table 2.

First, following the criterion proposed by Meroño et al. (2017), standard deviations were examined as an indicator of the variability of participants' responses, considering values greater than 1 as adequate. The results showed that the standard deviations ranged

Table 2 Coefficients of skewness, kurtosis and standard deviation

	TD	S	K
DIM. 1 - Basic knowledge about identifying and preventing digital threats			
1.1 I know how to teach my students to identify suspicious emails or messages such as phishing.	1.93	−0.476	−0.884
1.2 I know how to teach my students what malware is and how to prevent it from spreading to their devices	2.04	0.047	− 1.279
1.3 I know how to instruct my students on the most common hacking techniques and how to protect themselves from them.	2.02	0.385	− 1.129
1.4 I know how to protect the digital educational materials I share with my students to prevent unauthorized access.	2.06	0.167	− 1.282
1.5 I know how to instruct my students on the importance of logging out of their accounts on shared devices.	2.09	−0.404	− 1.198
1.6 I know how to teach my students to identify suspicious patterns in applications or software to avoid unsafe downloads.	1.97	0.144	− 1.176
1.7 I know how to teach my students to identify and avoid fraudulent websites to protect their personal and financial information.	2.00	0.144	− 1.242
DIM 2 - Teacher competencies to instruct students in the protection of personal information in digital environments			
2.1 I know how to teach my students how to properly configure privacy settings on their social media platforms to protect their personal data.	1.98	0.198	− 1.195
2.2 I know how to teach my students how to block or restrict strangers on social media to protect their personal information.	2.02	− 1.44	− 1.243
2.3 I know how to teach my students to differentiate between secure and unsecured websites before entering any personal information.	1.98	−0.095	− 1.205
2.4 I can instruct my students on how to delete cookies and browsing data to protect their online privacy.	2.10	−0.091	− 1.338
2.5 I know how to teach my students to review and control the permissions they grant to apps and websites to access their personal data.	2.01	0.109	− 1.254
2.6 I know how to teach my students to review and adjust location permissions on the apps they use, preventing them from sharing their location unnecessarily.	2.07	0.037	− 1.340
2.7 I know how to teach my students how to use encryption tools to protect sensitive information they share online, for example on WhatsApp.	1.93	0.704	−0.689
DIM. 3. Teacher competencies to instruct students in the safe use of hardware, software and browsers			
3.1 I can teach my students to regularly update the operating system and apps on their devices to improve security.	2.14	0.139	− 1.389
3.2 I am able to explain to my students how to set up a home Wi-Fi network securely.	2.10	0.179	− 1.333
3.3 I know how to instruct my students on how to activate and use the firewall on their devices to protect themselves from external attacks.	1.99	0.543	− 0.964
3.4 I know how to teach my students how to use security apps, such as antivirus and antimalware, to protect their devices.	2.03	0.277	− 1.222
3.5 I know how to instruct my students on how to use browser extensions that help block malicious websites and misleading ads.	2.02	0.453	− 1.076
3.6 I know how to teach my students how to back up their work to the cloud and to external hard drives or the cloud to prevent data loss.	2.08	−0.281	− 1.255
DIM. 4 - Teacher competencies to instruct students in password management and authentication in digital environments			
4.1 I know how to teach my students to create strong passwords using a combination of letters, numbers, and symbols.	2.01	−0.659	−0.853
4.2 I know how to educate and educate my students about the importance of changing their passwords regularly to keep their accounts secure.	1.96	−0.380	− 1.030

Table 2 (continued)

	TD	S	K
4.3 I know how to teach my students how to enable multi-factor authentication (2FA) on their accounts to add an extra layer of security.	2.05	0.811	−0.705
4.4 I know how to explain to my students the difference between strong and weak passwords, and how to improve weak ones.	2.04	−0.578	−0.986
4.5 I know how to guide my students to set up secure recovery options	2.10	−0.043	− 1.350
DIM.5 - Continuous training and updating in cybersecurity			
5.1 I attend cybersecurity courses to stay up-to-date on the latest digital protection practices.	1.45	1.332	1.243
5.2 I often consult articles and official reports from public agencies to stay up-to-date on new cyber threats and best practices for protection.	1.59	1.002	0.236
5.3 I stay informed about potential digital threats, such as fake news, phishing, ransomware, and attacks on educational networks.	1.73	0.553	− 0.86
5.4 I strive to improve my competencies in data protection and privacy to provide my students with up-to-date and ethical digital security education.	1.79	0.399	−0.797

Own elaboration

from 1.45 (item 5.1) to 2.14 (item 3.1), indicating adequate heterogeneity in the sample responses. Secondly, the coefficients of skewness (S) and kurtosis (K) were examined to identify the shape and symmetry of the distributions. According to Forero et al. (2009)d rez and Medrano (2010), values within the range of ± 1.5 are considered indicators of an acceptably normal distribution. The results showed that all items presented skewness and kurtosis values within the recommended limits, indicating adequate univariate normality in the responses. Consequently, no items needed to be eliminated for violating the normal distribution assumptions. These results confirm the suitability of the data set for subsequent factor analyses.

For the second check, the ability of each item to discriminate within its respective dimension was evaluated using the corrected-correlation coefficient between the item score and the total factor score. This analysis was carried out with the objective of verifying whether the elimination of any item could improve the internal reliability of each dimension (Hajjar, 2018). According to Nunnally & Bernstein (1994), items with values equal to or greater than 0.25–0.30 are considered adequate, while other authors, such as Shaffer et al. (2010) are more demanding and propose eliminating those items with an item-total correlation lower than 0.40. In the creation of this psychometric instrument, the values of the corrected total item correlation ranged from 0.508 (item 5.1) to 0.877 (item 1.7). All items significantly exceeded the 0.40 threshold, indicating adequate discriminatory capacity within each dimension. Furthermore, Cronbach's alpha values if the item were deleted were adequate (between 0.979 and 0.980), demonstrating that the elimination of any item would not have significantly improved the instrument's internal consistency. The detailed results of the analysis are presented in Table 3.

3.2 Explanatory Validity

To examine the construct validity of the instrument, an EFA was carried out, following the procedures applied in previous research with similar characteristics (Guillén-Gámez et al., 2024a, b; Soriano-Alcántara et al., 2025; Guillen-Gámez et al., 2021) and in accordance with the methodological guidelines described by Gümüş and Kukul (2023). The pur-

Table 3 Analysis of the scale discrimination index

	Scale mean if item deleted	Scale variance if item deleted	Corrected item-total correlation	Cronbach's alpha if item deleted
DIM.1				
1.1	105.0345	1982.036	0.761	0.979
1.2	105.8024	1966.831	0.806	0.979
1.3	106.2347	1965.226	0.820	0.979
1.4	105.8223	1967.450	0.791	0.979
1.5	105.0027	1970.104	0.765	0.979
1.6	105.9390	1961.715	0.867	0.979
1.7	105.7851	1957.385	0.877	0.979
DIM. 2				
2.1	105.9443	1961.904	0.860	0.979
2.2	105.4509	1969.815	0.795	0.979
2.3	105.5411	1961.059	0.865	0.979
2.4	105.4801	1957.209	0.832	0.979
2.5	105.8050	1957.031	0.872	0.979
2.6	105.6645	1953.097	0.869	0.979
2.7	106.6777	1981.990	0.762	0.979
DIM. 3				
3.1	105.8554	1952.963	0.840	0.979
3.2	105.9231	1967.402	0.779	0.979
3.3	106.4748	1967.206	0.826	0.979
3.4	106.0690	1957.661	0.861	0.979
3.5	106.2931	1959.172	0.856	0.979
3.6	105.2268	1964.933	0.798	0.979
DIM.4				
4.1	104.6910	1977.353	0.757	0.979
4.2	105.0995	1979.885	0.764	0.979
4.3	106.7838	1983.840	0.704	0.980
4.4	104.8024	1974.924	0.757	0.979
4.5	105.5703	1960.992	0.813	0.979
DIM.5				
5.1	107.4881	2047.727	0.508	0.980
5.2	107.1326	2033.353	0.565	0.980
5.3	106.5093	2011.047	0.661	0.980
5.4	106.1671	2010.285	0.642	0.980

Own elaboration

pose of the EFA is to identify the underlying structure of the latent factors, classifying the items according to their correlation coefficients and factor saturation (Büyüköztürk, 2002). To achieve a well-adjusted model, items with factor loadings below 0.40 were eliminated. Items that did not adequately saturate in the theoretical factor to which they belonged were also excluded (Gümüş & Kukul, 2022; Lloret-Segura et al., 2014).

After applying the principal axis factoring method with oblimin rotation, the pattern matrix presented in Table 5 was obtained. Most of the items showed adequate saturations and were consistent with the theoretical structure, although some presented cross-loadings or were grouped into factors different from those expected. Specifically, items 1.1, 1.5, 1.6

and 1.7 saturated in the factor corresponding to Dimension 2, so they were eliminated as they did not fit their correct dimension. Similarly, item 3.1 was removed for not reaching the established minimum load of 0.40, and item 3.6 was eliminated for incorrectly saturating in Dimension 4. Likewise, Item 4.3 presented a significant loading on Factor 3, which is why it was also eliminated. Consequently, these items were excluded from the final model because they did not meet the criteria for minimum saturation or theoretical congruence.

As a result of the AFE, five clearly defined factors emerged, consistent with the theoretical foundations of the instrument. Factor 1 consisted of items 2.6, 2.5, 2.2, 2.1, 2.4, 2.3, and 2.7, which explained 63.88% of the total variance; Factor 2 consisted of items 5.2, 5.3, 5.4, and 5.1, which explained 7.83% of the total variance; Factor 3 consisted of items 4.1, 4.4, 4.2, and 4.5, explaining 5.15% of the total variance; Factor 4 consisted of items 3.3, 3.2, 3.4, and 3.5, which explained 2.95% of the variance; The last and fifth factor was composed of items 1.3, 1.2 and 1.4, which explained 2.70% of the variance. Together, the six identified factors explained 82.54% of the total variance, demonstrating a high explanatory capacity of the model and a solid factorial structure with the theoretical basis of the instrument. The coefficients for each item are shown in Table 4.

After adjusting and consolidating the EFA model by eliminating items that did not present adequate saturations, various suitability tests were performed to verify the adequacy of the correlation matrix and the sufficiency of the sample size for factor analysis. First, the Kaiser-Meyer-Olkin (KMO) index was calculated, which assesses the proportion of common variance among variables. According to Worthington and Whittaker (2006), values above 0.80 indicate good sampling adequacy. In this study, a KMO value of 0.965 was obtained, which shows excellent suitability of the data for performing factor analysis. For its part, Bartlett's sphericity test was statistically significant ($p < .001$), with a value of $\chi^2 =$ 18,410,047 and 231 degrees of freedom, which demonstrates the existence of sufficient correlations between the items. Together, both indicators confirm that the sample and the data matrix are adequate to continue with the exploratory factor analysis, in accordance with the methodological recommendations of Watkins (2021).

Finally, the last procedure tested within the EFA was the examination of the correlation between the latent factors, in order to verify the unidimensionality of the instrument. Table 5 shows the matrix of factorial correlations obtained through the oblique oblimin rotation, where positive and moderate correlations are observed between the different dimensions. The highest relationships were between Dimension 2 (Privacy and Protection) and Dimension 1 (Awareness and Prevention) ($r = .769$), as well as between Dimension 2 and Dimension 4 (Passwords and Access) ($r = .734$). These results demonstrate the internal consistency of the model and confirm that the dimensions share a common conceptual basis, which justifies the use of an oblique rotation as the factors are not completely independent of each other.

3.3 Confirmatory Validity

In this section, the authors verified whether the internal structure identified in the EFA matched the expected structure based on the theoretical foundations previously presented in the research's conceptual framework (Thompson, 2004). The CFA was conducted using the indicators proposed by Hu and Bentler (1999), which are detailed below.

Table 4 Rotated factor loadings

	Factor 1 (DIM.2 - privacy and protection)	Factor 2 (DIM. 5 - continuing training)	Factor 3 (DIM. 4 - passwords and access)	Factor 4 (DIM. 3 - safe use)	Factor 5 (DIM.1 - awareness and prevention)
DIM.2					
2.6	0.882				
2.5	0.847				
2.2	0.782				
2.1	0.772				
2.4	0.759				
2.3	0.643				
2.7	0.429				
DIM.5					
5.2		0.933			
5.3		0.814			
5.4		0.787			
5.1		0.651			
DIM.4					
4.1			0.893		
4.4			0.854		
4.2			0.746		
4.5			0.462		
DIM.3					
3.3				0.672	
3.2				0.506	
3.4				0.499	
3.5				0.471	
DIM.1					
1.3					0.833
1.2					0.775
1.4					0.424

Own elaboration

Table 5 Factorial correlation matrix

Factor	Factor 1 (DIM.2 - privacy and protection)	Factor 2 (DIM. 5 - continuing training)	Factor 3 (DIM. 4 - passwords and access)	Factor 4 (DIM. 3 - safe use)	Factor 5 (DIM.1 - awareness and prevention)
1 (DIM.2)	1.000				
2 (DIM. 5)	0.587	1.000			
3 (DIM. 4)	0.734	0.425	1.000		
4 (DIM. 3)	0.622	0.453	0.334	1.000	
5 (DIM.1)	0.769	0.601	0.564	0.567	1.000

Own elaboration

The CMIN/df index (discrepancy divided by degree of freedom) allows us to assess the degree of fit between the empirical data and the proposed theoretical model. According to Bentler (1989), values below 5 indicate an acceptable fit, while values below 3 are considered excellent (Kline, 1998). The CFI (Comparative Fit Index) and NFI (Normed Fit Index) indices evaluate the quality of the model fit where values equal to or greater than 0.95 reflect an excellent fit (West et al., 2012). Additionally, the Incremental Fit Index (IFI) and Tucker-Lewis coefficient (TLI) are further measures of incremental fit, where values close to 1 indicate a good match between the model and the data. The Root Mean Square Error of Approximation (RMSEA) estimates the discrepancy between the observed and estimated covariance matrices, adjusted for the degrees of freedom. Values between 0.05 and 0.08 are considered acceptable, while those equal to or less than 0.05 are interpreted as excellent (MacCallum et al., 1996). Finally, RMR (Root Mean Square Residual) measures the overall error of the factor model, with values less than 0.08 being considered adequate (Diamantopoulos & Siguaw, 2000).

The first model evaluated did not meet all the suggested fit criteria; therefore, a second model was estimated. In this second version, items showing excessively high covariances with other items in the instrument were eliminated, following Byrne's (2013) recommendations on reviewing modification indices (MIs) related to interactions between errors. Specifically, items 2.1, 2.2, 2.3, 2.7, 3.2, 4.5, and 5.3 were removed. In the second model, the goodness-of-fit indicators showed adequate values: $\chi^2(80) = 300.078$, CMIN/df = 3.751, IFI = 0.981, CFI = 0.981, TLI = 0.975, NFI = 0.974 and RMSEA = 0.060, with a 90% confidence interval between 0.053 and 0.068. Figure 1 shows the final factor model obtained after the CFA, along with the results regarding the relationships between the latent factors and the items that comprise them. The standardized correlation values derived from the analysis are also included.

3.4 Convergent and Discriminant Validity

Convergent validity is understood as the degree of certainty with which it can be stated that the items included in each dimension coherently represent the same latent characteristic or concept (Cheung & Wang, 2017). To verify this, the average variance extracted (AVE) was calculated, with a value greater than 0.50 considered adequate. As shown in Table 6, the AVE values obtained were 0.853 for Privacy and protection, 0.647 for Continuing training, 0.842 for Passwords and access, 0.852 for Secure use and 0.757 for Awareness and prevention, which indicates a good level of fit. Furthermore, the square roots of the AVE values (located on the diagonal of the matrix) were checked to see if they exceeded the correlations between the latent factors. In this case, the square roots were 0.923, 0.804, 0.917, 0.923, and 0.870, respectively, confirming that each dimension is adequately distinguished from the others.

Furthermore, discriminant validity was assessed using the MSV (maximum squared shared variance) index, the value of which should be lower than the AVE for each factor (Fornell & Larcker, 1981). In this analysis, MSV values ranged from 0.470 to 0.751, all lower than their corresponding AVE. Based on these results, it can be concluded that adequate discriminant validity has been achieved.

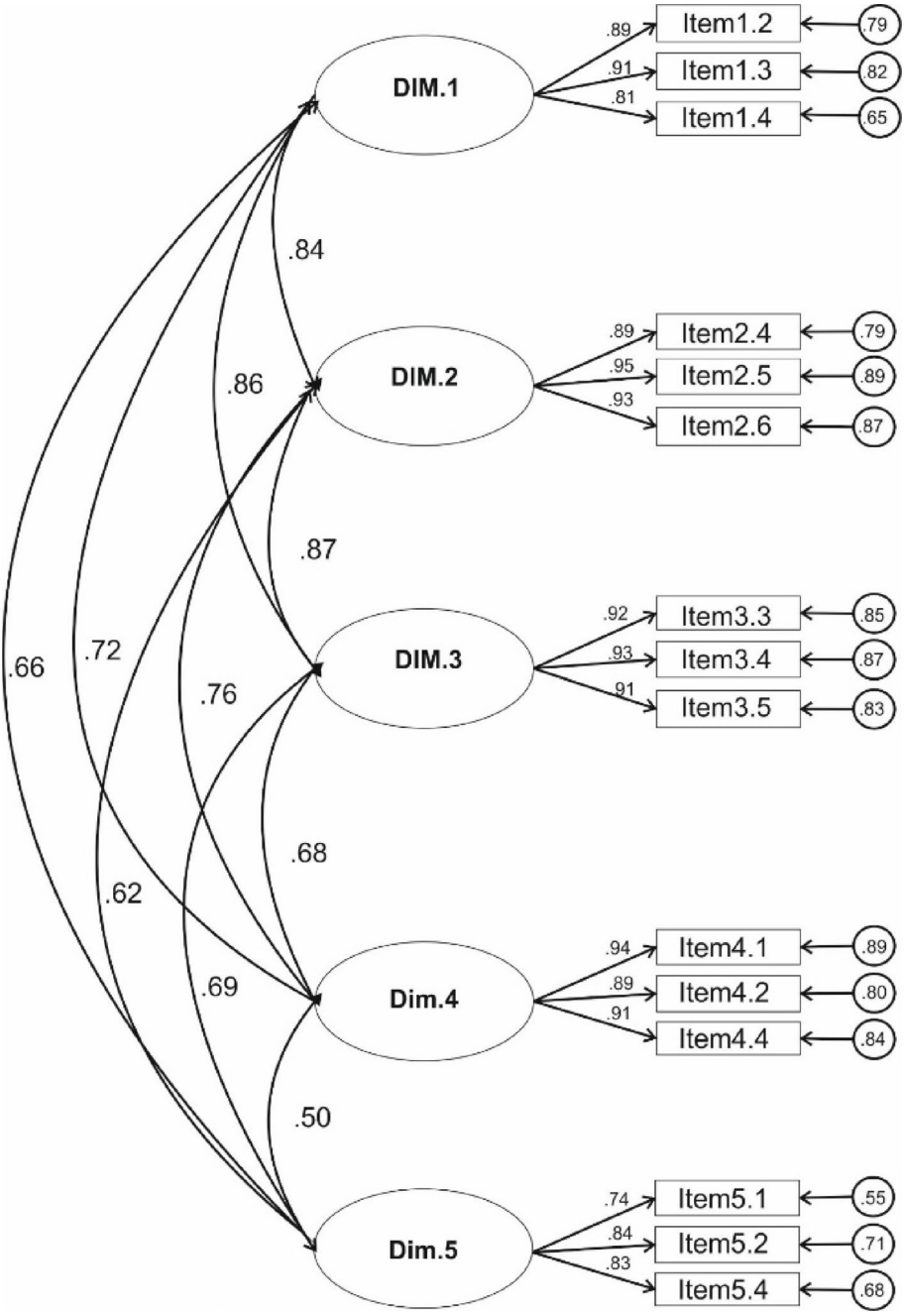

Fig. 1 Final version of the instrument. AFC

Table 6 Convergent and discriminant validity coefficients

	AVE	MSV	DIM.2 (privacy and protection)	DIM.5 (continuing training)	DIM.4 (passwords and access)	DIM.3 (safe use)	DIM.1 (awareness and prevention)
DIM.2 (privacy and protection)	0.853	0.751	0.923				
DIM.5 (continuing training)	0.647	0.470	0.621***	0.804			
DIM.4 (passwords and access)	0.842	0.581	0.762***	0.496***	0.917		
DIM.3 (safe use)	0.852	0.751	0.866***	0.686***	0.683***	0.923	
DIM.1 (awareness and prevention)	0.757	0.744	0.838***	0.661***	0.716***	0.862***	0.870

Own elaboration. *** $p < .001$

Table 7 Reliability coefficients

Dimension	DIM.1	DIM.2	DIM.3	DIM.4	DIM.5	Total
Cronbach's alpha	0.899	0.945	0.945	0.940	0.841	0.959
Spearman-Brown coefficient	0.865	0.948	0.937	0.938	0.845	0.937
Two halves of Guttman	0.763	0.846	0.833	0.842	0.788	0.937
Omega McDonald	0.890	0.942	0.942	0.937	0.820	0.989
CR	0.903	0.945	0.945	0.941	0.846	–

3.5 Analysis of the Internal Consistency of the Instrument (Reliability)

To verify the internal consistency of the instrument, different reliability coefficients were calculated, the results of which are presented in Table 7. Cronbach's alpha coefficient, widely used to assess internal consistency (Zeller & Carmines, 1980), showed very satisfactory values in all dimensions (0.899 in DIM.1, 0.945 in DIM.2 and DIM.3, 0.940 in DIM.4, and 0.841 in DIM.5), as well as for the instrument as a whole (0.959), exceeding the threshold of 0.7 recommended by Nunally (1978). Similarly, the Spearman-Brown coefficient (ranging from 0.865 to 0.948) and Guttman split-half coefficients (ranging from 0.763 to 0.846) showed adequate values. Furthermore, McDonald's Omega coefficient and Composite Reliability (CR) also exceeded the recommended value of 0.7, as suggested by Heinzl et al. (2011). Taken together, these results demonstrate that the instrument can be considered highly reliable.

4 Discussions and Conclusions

Currently, teaching educational cybersecurity is an unavoidable training need in schools, since the accelerated development of ICT has increased the digital risks associated with its use (Sadik et al., 2020; Дубинський, 2024). The emergence of innovations such as the Internet of Things, 5G networks, and artificial intelligence has generated new opportunities for learning, but has also introduced constant threats such as fake news, phishing, malware, and identity theft, which particularly affect young people (Jyoti, 2025; Ascoott, 2020). In

this context, the school is consolidated as a key space to promote cybersecurity education, where it is considered essential to teach students how to protect their devices, create secure passwords and recognize attempts at fraud or malicious software (Ismail et al., 2024; Kaban, 2021; Suson, 2019; Patterson et al., 2022).

Taking this context into consideration, teacher training in cybersecurity becomes essential, since teachers are the foundation for the success of any educational program focused on cybersecurity education. From this perspective, the main purpose of this study was to design and validate an instrument to assess the teaching competencies necessary for instructing students in cybersecurity education. The results obtained confirm that the instrument has adequate psychometric indicators and constitutes a robust tool for analyzing these competencies.

Various techniques were used to validate the scale in order to ensure its robustness. Comprehension validity, construct validity (using EFA and CFA), convergent validity, and discriminant validity were analyzed. The initial version consisted of 29 items, which were refined after verifying dispersion, skewness and kurtosis within the ranges recommended by Pérez and Carretero-Dios (2005), Meroño et al. (2017), Forero et al. (2009) and Hair et al. (2010). The corrected item-total discrimination was verified, with all items remaining above the thresholds suggested in the literature (≥ 0.40), and Bartlett's test of sphericity was applied along with the Principal Axis Factoring method and oblimin rotation for EFA, in line with Fabrigar et al. (1999), Lloret-Segura et al. (2014), Worthington and Whittaker (2006) and Watkins (2021).

As a result of the EFA, the instrument was made up of 22 items distributed in five factors, with KMO = 0.965 and Bartlett's $\chi^2 = 18{,}410.047$; $p < .001$, and was subsequently confirmed by CFA. For the CFA, different fit indices were used, following the recommendations of Hu and Bentler (1999), Bentler (1989), Kline (1998), West et al. (2012), MacCallum et al. (1996), and Diamantopoulos and Siguaw (2000). In the CFA, items with excessive levels of covariance with other items were eliminated, as recommended by Byrne (2013). Convergent and discriminant validity was also verified using AVE (≥ 0.50) and MSV ($<$AVE), in accordance with Fornell and Larcker (1981) and Hair et al. (2010), and internal consistency was estimated using Cronbach's Alpha, McDonald's Omega, Spearman-Brown, Guttman split-half and CR, with values greater than 0.70, in line with Nunnally (1978), Zeller and Carmines (1980) and Heinzl et al. (2011). Finally, an instrument composed of a total of 15 items classified into five latent factors was evidenced.

From a theoretical point of view, this study adds to the literature on teachers' digital competence by clearly defining educational cybersecurity as a competence that can be measured and analyzed. The validated structure of the instrument shows that cybersecurity education involves not only basic knowledge, but also teaching competencies and ongoing professional updating. This contributes to a clearer understanding of how cybersecurity fits within broader digital competence frameworks and provides a useful reference for future research in this field. From a practical point of view, the instrument can be easily used in real educational contexts as a diagnostic tool. Schools and teacher training institutions may apply it to assess teachers' level of preparedness in educational cybersecurity and to identify areas where further training is needed. In addition, the instrument allows institutions to track changes over time and to evaluate the impact of professional development initiatives related to safe and responsible use of digital technologies.

Among the main limitations of the study, it should be noted that the sample focused on teachers from the Spanish education system, so it is recommended to replicate the validation in other countries and educational levels to confirm the invariance of the model. Future research could extend the analysis to the European context, allowing for a comparison of differences and similarities in teacher preparation for teaching educational cybersecurity in different training systems, as well as examining the alignment of the instrument with the digital competencies proposed by the DigCompEdu framework. In this way, international comparisons could be established that contribute to consolidating a broader and more coherent vision of teacher training in cybersecurity education and responsible use of technology. Future research could also use longitudinal studies to examine how teachers' cybersecurity competencies change over time, especially after receiving training. In addition, studies comparing different educational levels could help to better understand how these competencies vary across teaching contexts.

Acknowledgements This scientific article is part of the doctoral thesis of Pablo De La Flor Bancalero, attached to the Doctoral Program in Educational Technology of the University of Malaga (UMA).

Funding Funding for open access publishing: Universidad de Málaga/CBUA. No funding was received for conducting this study.

Data Availability The data used in this study are part of an ongoing project and are not currently available.

Code Availability Not applicable.

Declarations

Conflicts of interest The authors declare that they have no conflicts of interest.

Ethical Approval This study was approved by the corresponding ethical committee.

Human and Animal Participants No human samples or participants were involved in this study.

References

Ascoott, T. (2020). Is media literacy the magic bullet for fake news? The Interpretor.

Baartman, L. K., & De Bruijn, E. (2011). Integrating knowledge, skills and attitudes: Conceptualising learning processes towards vocational competence. *Educational Research Review*, *6*(2), 125–134. https://doi.org/10.1016/j.edurev.2011.03.001

Basgall, L., Guillén-Gámez, F. D., Colomo-Magaña, E., & Cívico-Ariza, A. (2023). Digital competences of teachers in the use of YouTube as an educational resource: Analysis by educational stage and gender. *Discover Education*, *2*(1), 1–13. https://doi.org/10.1007/s44217-023-00054-x

Bentler, P. M. (1989). *EQS structural equations program manual*. BMDP Statistical Software.

Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, *14*(6), 588. https://doi.org/10.3390/educsci14060588

Büyüköztürk, Ş. (2002). Faktör analizi: Temel Kavramlar ve ölçek geliştirmede kullanımı. *Kuram Ve Uygulamada eğitim yönetimi*, *32*(32), 470–483.

Byrne, B. M. (2013). *Structural equation modeling with mplus: Basic concepts, applications, and programming*. Routledge.

Cheung, G. W., & Wang, C. (2017). Current approaches for assessing convergent and discriminant validity with SEM: Issues and solutions. *Academy of Management Proceedings*, *2017(1)*, 12706. https://doi.org/10.5465/AMBPP.2017.12706abstract

de la Flor Bancalero, P., Guillén-Gámez, F. D., Stošić, L., & Giménez-Gualdo, A. M. (2026). Teacher competencies in the willingness to use artificial intelligence pedagogically in the educational process: Good strategies for the smart teacher. *The role of smart education in a complex world* (pp. 65–92). IGI Global Scientific Publishing.

Diamantopoulos, A., & Siguaw, J. A. (2000). *Introduction to LISREL: A guide for the uninitiated*. SAGE.

ENISA, Cybersecurity Skills Frameworks (2023). https://www.enisa.europa.eu//topics/skills-and-competences/skills-development

European Comission (2020). Digital Education Action Plan 2021–2027, Resetting education and training for the digital age. https://education.ec.europa.eu/es/focus-topics/digital-education/plan

European Commission (2018). Council recommendation of 22 May 2018 on key competences for lifelong learning. *Official Journal of the European Union*, *C 189*, 1–13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018H0604(01)

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods*, *4*(3), 272–299. https://doi.org/10.1037/1082-989X.4.3.272

Ferrari, A. (2013). *DIGCOMP: A framework for developing and Understanding digital competence in Europe*. Joint Research Centre https://doi.org/10.2788/52966. European Commission.

Forero, C. G., Maydeu-Olivares, A., & Gallardo-Pujol, D. (2009). Factor analysis with ordinal indicators: A Monte Carlo study comparing DWLS and ULS Estimation. *Structural Equation Modeling*, *16*(4), 625–641. https://doi.org/10.1080/10705510903203573

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Guillen-Gamez, F., Mayorga-Fernández, M. J., & Contreras-Rosado, J. A. (2021). Validity and reliability of an instrument to evaluate the digital competence of teachers in relation to online tutorials in the stages of early childhood education and primary education. *Revista De Educación a Distancia (RED)*, *21*(67), 1–20. https://doi.org/10.6018/red.474981

Guillén-Gámez, F. D., Martínez-García, I., Alastor, E., & Tomczyk, L. (2024a). Digital competences in cybersecurity of teachers in training. *Computers in the Schools*, *41*(3), 281–306. https://doi.org/10.1080/07380569.2024.2361614

Guillén-Gámez, F. D., Tomczyk, Ł., Colomo-Magaña, E., & Mascia, M. L. (2024b). Digital competence of higher education teachers in research work: Validation of an explanatory and confirmatory model. *JOURNAL OF E-LEARNING AND KNOWLEDGE SOCIETY*, *20*(3), 1–12. https://doi.org/10.20368/1971-8829/1135963

Gümüş, M. M., & Kukul, V. (2022). Developing a digital competence scale for teachers: Validity and reliability study. *Education and Information Technologies*. https://doi.org/10.1007/s10639-022-11213-2

Hair, J., Anderson, R., Tathan, R., y, & Black, W. (2009). Análisis multivariante. Pearson.

Hair Jr, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis. In J. F. Hair Jr., W. C. Black, B. J. babin, & R. E. Anderson (Eds.), *Multivariate data analysis: A global perspective* (pp. 785–785). Prentice Hall.

Hajjar, S. T. (2018). Statistical analysis: Internal-consistency reliability and construct validity. *International Journal of Quantitative and Qualitative Research Methods*, *6*(1), 27–38.

Heinzl, A., Buxmann, P., Wendt, O., & Weitzel, T. (Eds.). (2011). *Theory-Guided modeling and empiricism in information systems research*. Springer Science & Business Media.

Herman, G. L., Huang, S., Peterson, P. A., Oliva, L., Golaszewski, E., & Sherman, A. T. (2023). Psychometric evaluation of the cybersecurity curriculum assessment. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (pp. 228–234). https://doi.org/10.1145/3545945.3569762

Honomichl, R., & Wagner, P. (2025). The need for highly trained and qualified k12 teachers to address the growing demand for cybersecurity professionals. In *INTED2025 Proceedings* (pp. 2153–2161). IATED. https://doi.org/10.21125/inted.2025.0611

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure 17 analysis: Conventional criteria versus new alternatives. *Structural Eq. 18 Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Instituto Nacional de Tecnologías Educativas y Formación del Profesorado [INTEF] (2022). Common Digital Competence Framework for Teachers (CDCFT). https://intef.es/wp-content/uploads/2022/03/MRCDD_V06B_GTTA.pdf

Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., & Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey. *Computers in Human Behavior Reports*, *16*, 100501. https://doi.org/10.1016/j.chbr.2024.100501

Jerman Blažič, A., & Jerman Blažič, B. (2024). Teaching and learning cybersecurity for European youth by applying interactive technology and smart education. *Education and Information Technologies*, *30*(7), 9093–9120. https://doi.org/10.1007/s10639-024-13155-3

Jyoti Hazarika, H. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students. *Alexandria*. https://doi.org/10.1177/09557490251340833

Kaban, A. (2021). Secure internet use in information technologies and software course textbooks at primary and secondary schools. *Athens Journal of Education*, *8*(1), 37–52. https://doi.org/10.30958/aje.8-1-3

Kelentric, M., Helland, K., & Arstorp, A. (2017). Framework for teachers' professional digital competence in Norwegian. https://www.udir.no/globalassets/filer/in-english/pfdk_framework_en_low2.pdf

Kline, R. B. (1998). *Principles and practice of structural equation modeling*. Guilford Press.

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. https://doi.org/10.6018/analesps.30.3.199361

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods*, *1*(2), 130–149.

Marchisio, M., Roman, F., Sacchet, M., Spinello, E., Nikolov, L., Grzelak, M., & Moldoveanu, C. E. (2022). Teachers' digital competences before and during the COVID-19 pandemic for the improvement of security and defence higher education. In *16th International Conference e-Learning, EL 2022-Held at the 16th Multi-Conference on Computer Science and Information Systems, MCCSIS 2022* (pp. 68–75). IADIS.

Meroño, L., Calderón, A., Estero, A., J. L., & Méndez Giménez, A. (2017). Diseño y validación Del cuestionario de percepción Del profesorado de Educación primaria sobre El Aprendizaje Del alumnado Basado En competencias (# ICOMpri2). *Revista Complutense De educación*, *29*(1), 215–235. https://doi.org/10.5209/RCED.52200

Nunally, J. C. (1978). *Psychometric theory*. McGraw-Hill.

Nunnally, J., & Bernstein, I. (1994). *Psychometric theory*. McGraw-Hill.

Offenberger, S., Herman, G. L., Peterson, P., Sherman, A. T., Golaszewski, E., Scheponik, T., & Oliva, L. (2019, October). Initial validation of the cybersecurity concept inventory: pilot testing and expert review. In *2019 IEEE Frontiers in Education Conference (FIE)* (pp. 1–9). IEEE. https://doi.org/10.1109/FIE43999.2019.9028652

Patterson, A., Ryckman, L., & Guerra, C. (2022). A systematic review of the education and awareness interventions to prevent online child sexual abuse. *Journal of Child & Adolescent Trauma*, *15*(3), 857–867. https://doi.org/10.1007/s40653-022-00440-x

Pérez, C., y, & Carretero-Dios, H. (2005). Normas para el desarrollo y revisión de estudios instrumentales. *International Journal of clinical and health psychology, 5*(3), 521–551.

Perry, J. L., Nicholls, A. R., Clough, P. J., & Crust, L. (2015). Assessing model fit: Caveats and recommendations for confirmatory factor analysis and exploratory structural equation modeling. *Measurement in Physical Education and Exercise Science*, *19*(1), 12–21. https://doi.org/10.1080/1091367X.2014.952370

Ping, L., & Cunningham, D. (2013). In M. S. Khine (Ed.), *Application of structural equation modeling in educational research and practice*. Sense.

Raykov, T., & Marcoulides, G. A. (2008). *An introduction to applied multivariate analysis*. Routledge.

Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. N. (2020). Toward a sustainable cybersecurity ecosystem. *Computers*, *9*(3), 1–17. https://doi.org/10.3390/computers9030074

Santhosh, T., & Thiyagu, K. (2024). Development and validation of cyber security competency scale for prospective teachers. *Journal of Pedagogical Sociology and Psychology*, *6*(3), 111–124. https://doi.org/10.33902/jpsp.202428783

Soriano-Alcantara, J. M., Guillén-Gámez, F. D., & Ruiz-Palmero, J. (2025). Exploring digital competencies: Validation and reliability of an instrument for the educational community and for all educational stages. *Technology Knowledge and Learning*, *30*(1), 307–326. https://doi.org/10.1007/s10758-024-09741-6

Suson, R. L. (2019). Appropriating digital citizenship in the context of basic education. *International Journal of Education Learning and Development*, *7*(4), 44–66.

Takács, J. M., & Pogátsnik, M. (2024a). The presence of cybersecurity competencies in the engineering education of generation Z. *Acta Polytechnica Hungarica*, *21*(6), 107–127.

Takács, J. M., & Pogátsnik, M. (2024b). A comprehensive study on cybersecurity awareness: Adaptation and validation of a questionnaire in Hungarian higher technical education. *Acta Polytechnica Hungarica*, *21*(10), 533–552.

Temirkhanova, M., Abildinova, G., & Karaca, C. (2024). *Enhancing digital literacy skills among teachers for effective integration of computer science and design education: A case study at Astana international School, Kazakhstan. Frontiers in education* (p. 1408512). Frontiers Media SA.

Thompson, B. (2004). *Exploratory and confirmatory factor analysis: Understanding concepts and applications*. American Psychological Association.

Tise, J. C., & McGill, M. M. (2024). Validation of an Instrument to Measure Self-Efficacy in Information Security. In *Proceedings of the 2024 on ACM Virtual Global Computing Education Conference V. 1* (pp. 214–220). https://doi.org/10.1145/3649165.3690095

Tomczyk, Ł. (2020). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, *25*(1), 471–486. https://doi.org/10.1007/s10639-019-09980-6

Tomczyk, Ł., Guillén-Gámez, F. D., & Llorent, V. J. (2023). Teacher digital and media competence in cyber security-a perspective on individual resilience to online attacks. In *International Conference on New Media Pedagogy* (pp. 1–23). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-63235-8_1

Torres Hernández, N. (2023). *Evaluación de la competencia digital de futuros docentes para el uso seguro y responsable de Internet* (Doctoral dissertation, Universidad de Granada). https://hdl.handle.net/10481/80668

Torres-Hernández, N., & Gallego-Arrufat, 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

Watkins, M. W. (2021). *A step-by-step guide to exploratory factor analysis with SPSS*. Routledge.

West, R. F., Meserve, R. J., & Stanovich, K. E. (2012). Cognitive sophistication does not attenuate the bias blind spot. *Journal of Personality and Social Psychology*, *103*(3), 506–519. https://doi.org/10.1037/a0028857

Worthington, R. L., & Whittaker, T. A. (2006). Scale development research: A content analysis and recommendations for best practices. *The Counseling Psychologist*, *34*(6), 806–838. https://doi.org/10.1177/0011000006288127

Yan, Z., Yang, P., Xue, Y., Lou, Y., & Nealon, M. (2021). Validity and reliability of cybersecurity judgment questionnaire for middle and high school students: A validation study with Rasch analysis. *Human Behavior and Emerging Technologies*, *3*(5), 776–787. https://doi.org/10.1002/hbe2.312

Zeller, R. A., & Carmines, E. G. (1980). *Measurement in the social sciences: The link between theory and data*. Cambridge University Press.

Дубинський, В. (2024). Training of computer science teachers for the formation of cybersecurity skills in students: Actualization of problems and their possible solutions. *Освіта Інноватика Практика*, *12*(10), 6–11. https://doi.org/10.31110/2616-650X-vol12i10-001