Comunicar, n. 61, v. XXVII, 2019 | Media Education Research Journal | ISSN: 1134-3478; e-ISSN: 1988-3478
www.comunicarjournal.com

# Competence of future teachers in the digital security area

## Competencia de futuros docentes en el área de seguridad digital

Dr. María-Jesús Gallego-Arrufat is Full Professor of Educational Technology at the University of Granada (Spain) (mgallego@ugr.es) (https://orcid.org/0000-0002-2296-5431)
Norma Torres-Hernández is Researcher in training (FPU) in the Department of Didactics and School Organization at the University of Granada (Spain) (normath@ugr.es) (https://orcid.org/0000-0003-4744-0313)
Dr. Teresa Pessoa is Associate Professor in the Faculty of Psychology and Education at the University of Coimbra (Portugal) (tpessoa@fpce.uc.pt) (https://orcid.org/0000-0002-5252-3618)

## ABSTRACT

The use of technologies and the Internet poses problems and risks related to digital security. This article presents the results of a study on the evaluation of the digital competence of future teachers in the DigCompEdu European framework. 317 undergraduate students from Spain and Portugal answered a questionnaire with 59 items, validated by experts, in order to assess the level and predominant competence profile in initial training (including knowledge, uses and interactions and attitudinal patterns). The results show that 47% of the participants belong to the profile of teachers at medium digital risk, evidencing habitual practices that involve risks such as sharing information and digital content inappropriately, not using strong passwords, and ignoring concepts such as identity, digital "footprint" and digital reputation. The average valuations of each item in the seven categories show that future teachers have an average competence in the area of digital security. They have good attitudes toward security but less knowledge and fewer skills and practices related to the safe and responsible use of the Internet. Future lines of work are proposed, aimed at responding to the demand for a better prepared and more digitally competent citizenry. The demand for education in security, privacy and digital identity is becoming increasingly important, and these elements form an essential part of initial training.

## RESUMEN

El uso de las tecnologías e Internet plantea problemas y riesgos relacionados con la seguridad digital. Este artículo presenta los resultados de un estudio sobre la evaluación de la competencia digital de futuros docentes en el marco europeo DigCompEdu. Participan 317 estudiantes de Grado de España y Portugal. Se aplica un cuestionario con 59 ítems validado por expertos con el objeto de conocer el nivel y perfil competencial predominante en la formación inicial (incluyendo conocimientos, usos e interacciones y patrones actitudinales). Los resultados muestran que el 47% de los participantes pertenecen al perfil de docentes en riesgo digital medio, evidenciando prácticas habituales que conllevan riesgos tales como compartir información y contenidos digitales de forma inapropiada, no utilizar contraseñas seguras, y desconocer conceptos como identidad, huella o reputación digital. Las valoraciones medias de cada ítem en las siete categorías evidencian que los futuros docentes poseen una competencia media en el área de seguridad digital. Tienen buenas actitudes hacia la seguridad, pero menos conocimientos, habilidades y prácticas relacionadas con el uso seguro y responsable de Internet. Se plantean futuras líneas de trabajo enfocadas a dar respuesta a la exigencia de una ciudadanía mejor preparada y más competente digitalmente. La demanda de formación en seguridad, privacidad e identidad digital está siendo cada vez más importante, reconociéndose que es muy necesaria en la formación inicial.

## KEYWORDS | PALABRAS CLAVE

Digital competence, teacher education, privacy, cyber security, Internet, teachers, university, initial training.
Competencia digital, formación del profesorado, privacidad, seguridad cibernética, Internet, docentes, universidad, formación inicial.

Received: 2019-02-26 | Reviewed: 2019-04-30 | Accepted: 2019-05-10 | Preprint: 2019-07-15 | Published: 2019-10-01
DOI https://doi.org/10.3916/C61-2019-05 | Pages: 53-62

## 1. Introduction

Digital competence takes the form of cognitive, attitudinal, and technical skills that help to mitigate numerous problems and challenges in the knowledge society. Dynamic and transversal, digital competence is considered as a key competence in developing a digital citizenry and as a crucial element in lifelong learning processes (Janssen, Stoyanov, Ferrari, Punie, Pannekeet, & Sloep, 2013).

Digital competence is the ability to use technologies critically and safely for work, leisure, and communication. It involves using them to recover, evaluate, store, produce, present, and exchange information, as well as to communicate and participate in collaboration networks through Internet (Parliament & European Council, 2006). Digital competence includes issues related to technology, information, multimedia, and communication that encourage critical, responsible, creative use of technology—issues fundamental to learning processes and participation in the $21^{st}$ century (Esteve, Gisbert, & Lázaro, 2016; Napal, Peñalva-Vélez, & Mendióroz, 2018).

The framework for development of digital competence in Europe (DigComp) provides the structure for understanding and evaluating digital competence. This framework is consolidated and disseminated internationally through the European Framework for the Digital Competence of Educators (DigCompEdu) (Redecker, 2017). In Portugal and Spain, it is used to evaluate users' digital competence using different levels: basic (level A), intermediate or independent (level B), and advanced or competent (level C), based on the user's knowledge, abilities, and skills.

In Latin America, it is adopted to search for, choose, and process information critically; communicate using various formats; act responsibly; and take advantage of technology to learn and to solve problems (Lueg, 2014). Digital teaching competence (DTC) is the comprehensive set of personal characteristics, knowledge, abilities, and attitudes required to act effectively in various teaching contexts (Tigelaar, Dolmans, Wolfhagen, & Van-der-Vleuten, 2004). It mobilizes abilities and skills related to use of ICT to generate knowledge (Flores-Lueng & Roig, 2016), stimulating more conscious and positive use of these media in education (Pedro & Chacon, 2017).

DTC involves knowing how to use technologies to teach and learn with didactic and pedagogical criteria and moral and ethical sense (Krumsvik, 2009). It is crucial to understand DTC from a holistic perspective—that is, both to integrate ICT properly into the curriculum and classroom and to ensure development of the student's digital competence (Álvarez & Gisbert, 2015; Fernández-Cruz & Fernández-Díaz, 2016; Prendes, Castañeda, & Gutiérrez, 2010).

### 1.1. Safety in DTC

Safety in DTC involves protection of users' information and communication against the problems generated by ICT use (Barrow & Heywood-Everett, 2006). It is related to the privacy, integrity, and efficiency of Internet technology and information (Anderson, 2003). Safety refers to teachers' knowledge, abilities, and attitudes to design and develop learning experiences that promote, model, and train students as digitally responsible citizens.

People who teach play a special leading role in fostering acquisition of digital competence, since the teacher is a model and guide who cares for, orients, and trains others about responsible use of navigation, communication, and collaboration, as well as sharing information through Internet. This role can cause problems, however, due to a mistaken conception, that teachers teach about safety as if students only understood and had a single concept of Internet (Edwards & al., 2018).

DigComp (2016) and DigCompEdu (2017) have provided the foundation for developing a framework for digital competence of educators (MCCDD, 2017). They include competences concerning digital safety, such as protection of personal data and privacy, protection of health, and proper management of digital identity. The framework stresses responsible use, respect for the principles of online privacy that apply to oneself and others, and care for the environment.

In the area of safety, the competent user can "review the safety configuration of systems and applications, react if his/her computer equipment is infected with a virus, configure and/or modify the firewall and safety parameters of his/her electronic devices, encrypt emails and archives, and apply filters to avoid email spam" (http://bit.ly/30qMppL).

Research on digital safety (e-safety, digital safety, Internet safety, or Internet safety) is undertaken in different disciplines, such as Psychology, Education, and Law, and research has proliferated in the past decade (Jones, Mitchell, & Finkelhor, 2013; Shin, 2015; Šimandl & Vanícek, 2017; Chou & Peng, 2011; Napal, Peñalva-Vélez, & Mendióroz, 2018). Yet both in- and preservice teachers show low mastery of topics related to digital safety (De-Waal & Grösser, 2014).

Various reports, studies, and strategic plans attempt to help construct a climate of trust to mitigate or prevent the effects safety -related problems, especially in vulnerable groups, through actions such as incorporation of content on safety and responsible Internet use; design of itineraries to prevent, sensitize, raise awareness of, and improve trust and communication in Internet use; and foster the digital competence of parents and teachers, stressing social and emotional abilities to support and understand children's use of ICT and the problems that can be avoided, among other issues.

### 1.2. Training of preservice teachers in digital safety

Education systems recognize the importance of training teachers in mastery of ICT, particularly concerning safety, but initial training teacher programs usually treat digital competence transversely (Napal, Peñalva-Vélez, & Mendióroz, 2018).

Study programs show a clear dispersion of required subjects on educational technologies, with differing presence across universities, polytechnics, and other institutions of higher education. There is no doubt that the preservice teacher needs knowledge (pedagogical and content-related), abilities (social and technical), and attitudes concerning digital safety and how to teach it. We expect teachers to assume responsibilities in teaching digital safety and orient their students to the rules for Internet behavior, but teachers often lack sufficient preparation to understand risks and unethical behavior (Chou & Peng, 2011). The educator can serve as a model to help improve students' behavior when using technology, have conversations about risks and damage, and influence students significantly through his/her action (Chou & Chou, 2016; Šimandl, 2015; Shin, 2015).

> **Initial training with a coherent approach is necessary, where safety should be taught as a matter of high priority in the educational field, especially in training programs within a common digital competence framework.**

In sum, initial training should be responsive to society's current needs so that professionals adapt to innovation processes and can compete in and for use of technology on the labor market (Tejada & Pozos, 2018). Our new digital culture demands teachers who are useful, practical, and oriented to training critical, responsible citizens. Various studies indicate the pressing need for educational institutions centers to adopt coherent focus that guarantees training to promote safety as a high-priority question in education, especially in teacher training programs (Barrow & Heywood-Everett, 2006; Woollard, Wickens, Powell, & Rusell, 2009; Chou & Peng, 2011; Engen, Giæver, & Mifsud, 2015; Shin, 2015).

Work is being done internationally to improve safety in Asian and European organisms through education and training. In Taiwan, the TAIS program (2006-2010) identified four aspects for the training of competent teachers: safety and protection of communications, suitability of information, online safety and own use of technological devices.

In the EU, organisms such as the British Educational Communications and Technology Agency (BECTA) and various studies in Nordic countries and the Czech Republic stress training teachers and conclude that prior experiences, knowledge, practices, opinions, and perceptions determine how teachers should teach, resolve, and attend to digital safety problems (Engen, Giæver, & Mifsud, 2015; Šimandl & Vanícek, 2017). At global level, UNICEF proposes the importance of consolidating actions and educational measures for and from educational institutions, the shared responsibility of parents and teachers, and the need to dedicate educational resources to education and prevention programs that help

to avoid threats and protect against the dangers of the digital world (United Nations Children's Fund (UNICEF), 2017).

The goals of our study are:

1) To identify preservice teachers' level of digital competence in safety.

2) To describe the competence profile of preservice teachers in different areas of safety (interaction through technologies, sharing of digital information and contents, protection of personal data, protection of health, netiquette, digital identity, and cyberbullying on social networks and Internet).

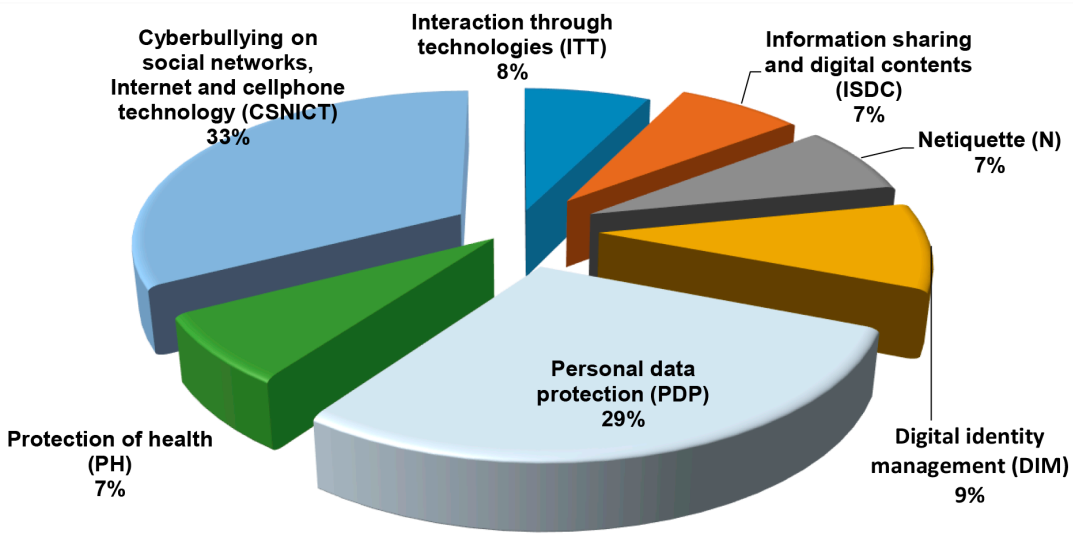
3) To explore differences by sex, gender, and age at which one begins using social networks in each of the different areas in order to determine training needs to improve preservice teachers' digital competence in safety.

4) To provide pedagogical activities in safety appropriate to preservice teachers' strengths and weaknesses.

## 2. Material and methods

We perform a descriptive, transversal study of 317 undergraduates 18-43 years old (M=22.2; DT=4.8). The students are from four Spanish and one Portuguese university; 248 (78.2%) are women and 69 (21.8%) men.

Figure 1. Categories of questionnaire on safety




The survey instrument is an ad hoc questionnaire for preservice teachers designed based on areas of safety from DigComp 2.0, DigCompEdu, the common framework for DTC (INTEF, 2017), the NETS*S project (ISTE, 2007), and a tool for self-diagnosis of digital competences from the Andalusian Regional Government (http://bit.ly/2YnNixx).

The questionnaire has 59 items divided into seven categories (Figure 1) and was validated by eight experts from Spanish and Portuguese universities with teaching and research experience in educational technologies. We obtain an Alpha Cronbach of $\alpha$=.923, as well as values for the criteria of clarity (.916), relevance (.914), and importance (.946). The items are divided into knowledge (K=24 items), abilities and practices (A&P=23 items), and attitudes (A=10 items). Table 1 groups the items under these dimensions. The statistical analysis was performed with SPSS 24.0. Using a two-stage cluster procedure, we classified the participants according to competence levels, with a three-category solution (significance level 5%). We also performed univariate descriptive analysis, calculating the mean and confidence interval at 95%, as well as the standard deviation. For the qualitative variables, we calculated frequency and percentage, and analyzed the relationship among them using the Chi-square test. With the nonparametric

Spearman's rho correlation coefficient, we analyzed the association among the numerical variables. To study the relationship between numerical and dichotomous variables, we applied the nonparametric Mann-Whitney test, calculating the effect size. The relationship between the categorical and numerical variables was analyzed using the nonparametric Kruskal-Wallis test. For the tests with statistically significant results, we used the Mann-Whitney test to compare the categories by pairs.

**Table 1. Dimensions of digital safety questionnaire**

| | |
|---|---|
| Knowledge (K) | Technical knowledge to tag information with other people (ISDC2). Technical knowledge to share information with others (ITTISDCI). Concept of digital identity (DIM1). Concept of digital reputation (DIM4). Knowledge of rules for online communication and behavior (N1). Creation of strong passwords (PDP1). Risks of wrongful appropriation of usernames and passwords (PDP3). Digital fingerprint and safety of browsers to prevent saving of passwords and browsing data (PDP10). Importance of data protection (PDP15). Physical and mental health risks of Internet (PSI). Measures or protocols to protect physical and mental health (PS2). Application of action patterns to avoid risks, abuses, scams, or other problems(PS4). Cases of bullying and abuse of social networks (CSNICT1). Inappropriate use of social networks (CSNICT4). Preventive measures to avoid problems of inappropriate technology use (cyberbullying) (CSNICT5). How to act in case of cyberbullying or other safety problems (CSNICT7). Identifying situations related to network abuses and cyberbullying (CSNICT9). Serious risks and relationship to cyberbullying (CSNICT13). Situations of risk due to technologies and Internet (CSNICT14). Most common social networks at high risk of bullying (CSNICT15). Social effects of cyberbullying and other network problems (CSNICT16). Causes of risks and cyberbullying through Internet, social networks, or technological devices (CSNICT17). Areas of DTC that help to prevent situations of bullying (CSNICT18). |
| Attitudes (A) | Care for one's image on social networks (DIM2). Peer group promotion of digital image protection and care (GID3). Respectful language when writing on different social networks (N2). Care in writing on social networks (N3). Not giving personal information to strangers (PDP7). Bad feeling and rejection on learning of cases of bullying or abuse on social networks (CSNICT2). Having positive attitudes to avoid problems related to Internet use that affect physical or mental health (CSNICT6). Responsibility as a future educator for implementing educational and preventive actions involving safety (CSNICT10). Importance of knowing, practicing, and modelling behavior that encourages responsible Internet use (CSNICT11). |
| Abilities and practices (A&P) | Introduction to social networks (IP3). Places to access Internet (IP4). Use of specific technological devices/tools (ITT1). Number of email accounts used (IMT2). Active participation in social networks (ITT3). Disseminating and resending information easily (ISDC3). Disseminating and resending information without others' consent (ISDC4). Searching for information and updating matters such as identity and data management (DIM5). Use of communication rules and behavior based on social network or email use (N4). Frequent change of passwords (PDP2). Sharing usernames and passwords (PDP4). Use of different passwords to prevent theft (PDP5). Use of unblocking patterns and passwords (PDP6). Use of strong passwords (PDP8). Deactivating options for saving passwords on devices (PDP9). Blocking devices when leaving them or when leaving devices in the presence of others (PDP11). Covering phone and computer cameras when not in use(PDP12). Publishing information that can harm digital image, identity, or reputation (PDP13). Recommending that contacts be careful with their digital identity and reputation (PDP14). Searching for information on data protection and digital reputation (PDP16). Applying measures or protocols to care for physical and mental health (PH3). Sharing information with peer groups or family on problems of bullying and online safety (CSNICT3). Attending training activities (CSNICT8). When to learn appropriate use of ICT? (CSNICT12). |

## 3. Results

### 3.1. Levels of competence in digital safety

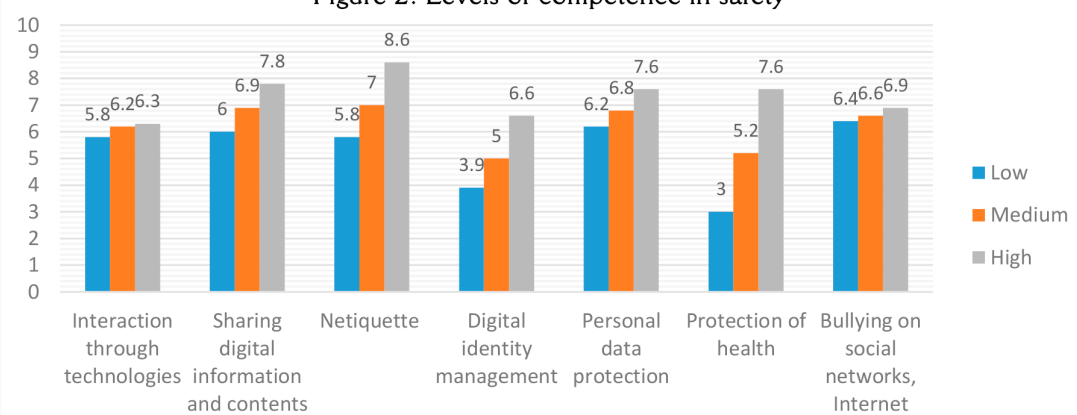
The analysis performed enabled us to identify three groups of digital competences in safety, with high, medium, and low levels, respectively. We compare the mean values for each category on the

questionnaire (Figure 2).

In 34% of cases, we find "digitally secure teachers". These participants use few technological devices, email accounts, and social networks (ITT); share information with the consent of third persons (ISDC); and know, apply, and respect the rules of communication and behavior (N). As to digital identity and reputation, they avoid publishing personal information that could affect their digital image (DIM), and use different passwords, which they change often. They know and use blocking patterns on their devices, avoid having their passwords recorded on devices that are not their own (PDP), and are aware of the importance of not letting Internet abuse affect their health (PH).

The medium level, "teachers at medium digital risk", accounts for 47% of the cases. These participants are able to upload and share information on social networks (ISDC), know communication rules but do not always follow them (N), and care fortheir image on social networks. They may, however, have some personal data on Internet that does not correspond to reality (DIM). They avoid sharing their passwords and personal information on social networks and have information about account protection (PDP). They also have information about the risks Internet or excessive use that social networks pose to physical and mental health and know measures and protocols for protection, although they do not always follow these protocols (PH).

Figure 2. Levels of competence in safety




Among the preservice teachers,18% showed a low level and are thus considered as "teachers at digital risk". These participants are always connected to Internet, have more than five devices, and use different email accounts and more than five social networks (ITT). They are able to upload and share photos and generally do not have difficulty managing social networks (ISDC). They do not know, and thus do not follow, rules for communication and behavior (N). Independently of the group to which they belong, only 7% of survey respondents had participated in some training activity on topics related to digital safety.

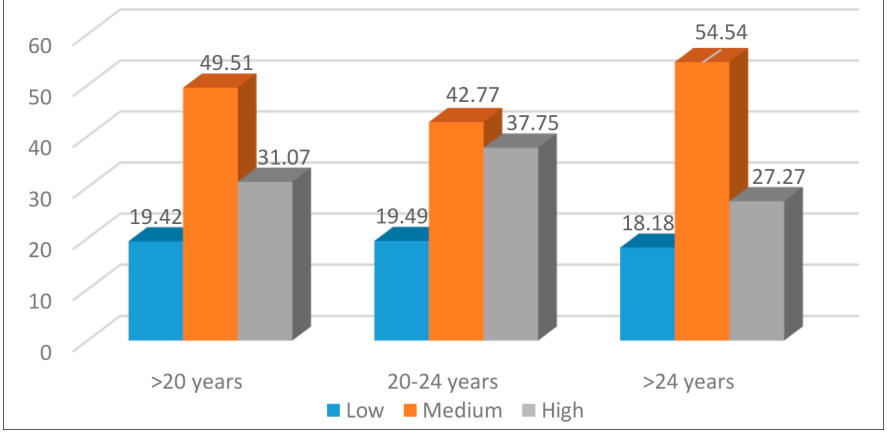
### 3.2. Profiles of competence in safety by age, gender, age at which one began social network use, and places of access to Internet

The age group 20-24 years old constitutes the largest number of participants (50%) in all three levels of safety competence. Students over 24 represent 17%. We can identify "digitally secure preservice teachers", who show greater competence in netiquette (8.62), sharing digital information and content (7.76), personal data protection (7.64), and protection of health (7.64). This group shows lower values for bullying on social networks, Internet, and cellphones (6.87); digital identity management (6.59); and interaction through technologies (6.27).

Figure 3 illustrates this trend. The "preservice teachers at medium digital risk" show high values in the same categories, although the averages are lower: netiquette (6.97); sharing digital information and content (6.88); personal data protection and protection of health (6.76); bullying on social networks, Internet, and cellphones (6.64); and interaction through technologies (6.20). The categories for protection of health (5.24) and digital identity management (4.99) are even lower. The "preservice teachers at digital risk" show

greater competence concerning bullying on social networks, Internet, and cellphones (6.40); personal data protection (6.20); sharing digital information and content (5.94); and netiquette (5.79). They show lower levels of competence, however, in digital identity management (3.93) and protection of health (3.04).

Figure 3. Competence levels by age group




By gender, for all three competence groups, the highest percentage of women show medium-level competence (38% of cases), followed by those with a high level (23%) and a low level (15%). Of the total sample, 9% of men show a high level of competence, 8.5% a medium, and 4.4% a low level. For age at which respondents began to use social networks, individuals who started to use these networks before the age of 12 are significantly related to medium and high levels of competence. Those who started use between 12 and 14 years of age also show medium-level competence. The relationship between level of overall competence and low level of the three groups according to starting age is less significant. Competence level is significantly related to place(s) of access. Most individuals with a low competence level are always connected; groups with intermediate and high competence are connected a smaller percentage of the time. In the group with medium competence, nearly half of participants are connected from one specific place, while a similar percentage is always connected. Participants with high competence are connected more frequently from one place, although nearly half are always connected.

### 3.3. Differences in knowledge, attitude, ability, and practice

The results differ according to the dimensions of the questionnaire. First, knowledge (K) of digital safety had 24 items, with values ranging from 10 (CSNICT14 and 18) to 1.9 (CSNICT17), and an average of 6.7 (Table 2). The participants had the most knowledge on topics on preventing risky situations, personal data protection, and technical knowledge on sharing information with others. They had less knowledge of the rules of online communication and behavior, the effects of cyberbullying, measures or protocols for protection of physical and mental health, and concepts such as digital identity or digital reputation. The average point-values for the dimension attitudes (A) of the preservice teachers toward problems and risks associated with safety range from 10 (CSNICT10) to 6.24 (CSNICT6), with an average of 8.77. These items include the responsibility the teachers perceive when implementing educational and preventive measures related to safety; the need to acquire knowledge, practice, and model behavior that encourages responsible use; and feelings of discomfort and rejection when they learn of cases of abuse on social networks or other problems. Other attitudes involve not giving personal information to strangers, peer group promotion of protecting and caring for one's virtual image, and having positive attitudes to avoid problems related to Internet use that affect physical or mental health.

On the dimension of secure Abilities and Practices (A&P), with 23 items, the averages ranged from 10 (CSNICT1 and CSNICT8) to 2.2 (CSNICT8), with the lowest average as 6.03. These items evaluate secure practices, including care in publishing information that can harm digital image, identity, or reputation; not sharing usernames and passwords; and using different passwords to avoid theft and

blocking devices. Among the least secure practices were applying measures or protocols to care for physical and mental health, using technological devices and tools, disseminating and resending information easily, changing passwords infrequently, applying safety protocols in browsing and personal data protection, and participating in training activities related to safety.

### 3.4. Correlations among study variables

Table 2 (https://doi.org/10.6084/m9.figshare.8150516) displays the nonparametric correlations among the numerical variables in the study. We see that age is positively related to the age at which one began to use social networks and interaction through technologies. These last two variables are also positively related to each other. Interaction through technological is negatively associated with digital identity management and protection of health, and positively associated with overall competence. Sharing digital information and content is positively associated with netiquette; digital identity management; personal data protection; protection of health; bullying on social networks, Internet, and cellphones; and overall competence. Netiquette is positively associated with digital identity management; personal data protection; protection of health; bullying on social networks, Internet, and cellphones; and overall competence. Digital identity management is positively related to personal data protection; protection of health; bullying on social networks, Internet, and cellphones; and overall competence. Personal data protection is also positively associated with protection of health and overall competence. Protection of heath is directly associated with bullying on social networks, Internet, and cellphones; and overall competence. These last two variables are also related to each other.

Analysis of the relationship of sex to age, age at which one began to use social networks, and competence in social networks shows that men start using social networks earlier than women (13.46 years vs. 13.76 years old). Competence in sharing digital information and content is greater among women (7.10) than among men (6.59). Competence in managing digital identity is greater in men (5.72) than in women (5.21). Finally, competence in protecting health is also greater in men (6.27) than in women (5.45). Participants' age is only related to the age at which they began using social networks. The nonparametric Mann-Whitney tests indicate that starting age is lowest in the group under 20 years of age, followed by the group ages 20-24, and finally by those over 24. The age at which one began using social networks is significantly related to interaction through technologies. Participants who began before age 12 have less competence in this dimension than those who started at age 12-14 or later.

## 4. Discussion and conclusions

This study attempts to identify the levels and profiles of preservice teachers in digital safety in order to detect educational needs and propose activities for initial training at the university. To achieve this goal, we designed an instrument to demonstrate content validity and reliability, with a high Alpha Cronbach (Panayides, 2013).

Goal 1: To identify preservice teachers' level of digital competence in safety, we performed a cluster analysis that enabled us to identify three levels of competence, corresponding to the categories of digital safety in the questionnaire. In evaluating the level of digital competence, 36.85% of the preservice teachers scored at medium level, a result similar to that obtained by Fernández-Cruz & Fernández-Díaz (2016) with preservice teachers from so-called "Generation Z" and Napal, Peñalva-Vélez, & Mendióroz (2018) with secondary school preservice teachers.

Goal 2: We describe the competence profile of preservice teachers by differentiating between "digitally secure teachers" (high level), "teachers at medium digital risk" (medium level), and "teachers at digital risk" (low level). In general, women 20-24 years old form the majority and share the common characteristic that 93% have received no training in this area, even if they attempt to use secure practices. Self-taught learning about safety was acquired outside formal education, but we find evidence of the need for formal training (Engen, Giæver, & Mifsud, 2015). The results show little difference by gender on the questionnaire categories (6.49 for men and 6.42 for women), although men have a slightly higher average in ISDC, N, PDP, and CSNCT. As to age, those under 20 are more competent in ISDC and PDP. The high-risk behavior profile is that of the individual who is always connected to Internet (Yan, 2009; Fernández-

Montalvo, Peñalva, & Irazabal, 2015). The results by dimensions of knowledge (6.7), attitude (8.7), and abilities and practices (6.03) indicate greater willingness toward safety but less knowledge and practice related to secure, responsible use of Internet.

Goal 3: Exploring differences enables us to see the need to improve digital competence in safety (in the form of training activities) and prevention and education programs for secure, responsible Internet use (Chou & Peng, 2011; Fernández-Montalvo, Peñalva, & Irazabal, 2015). Such activities can enable the establishment of guidelines to improve secure, healthy abilities, and behavior through the network (Chou & Chou, 2016) —one of the dimensions that still presents considerable difficulties when evaluating digital competence (Napal, Peñalva-Vélez, & Mendióroz, 2018).

Why safety training? Although a significant body of research on digital competence focuses on evaluating technology or information literacy, hardly any studies focus specifically on areas of safety at university or on preservice teachers. We thus agree with Yan (2009) and Shin (2015) that preservice teachers do not receive sufficient training in this area. Our results show minimal training on questions of Internet safety.

Goal 4: This study proposes that safety is a determining factor in the acquisition of digital competence. Guaranteeing responsible, appropriate use of technology is the responsibility of courses in the area of Educational Technology for initial teacher training. Although institutions such as UNESCO, UNICEF, and the OECD, well as DigCompEdu in Europe, INTEF in Spain, and INCoDe.2030 in Portugal recognize digital safety in all areas as a difficult challenge, we understand both its importance in professionalizing educators to be digitally competent, secure, and responsible (Tejada & Pozos, 2018) and the value of information on the daily impact of technology on consumption and the environment for digital citizenship. This study has methodological limitations. The preservice teachers were drawn only from the fields of early childhood and primary education, and their participation in completing the online questionnaire was voluntary. The first of these conditions prevents generalizing the results to other levels of education. The second influenced the sample size.

What topics are crucial for training the future professional? The results of this study enable us to propose the following topics: rules for online communication and behavior (netiquette), measures and protocols to prevent risks on Internet and to care for physical and mental health, concepts related to digital safety (reputation, identity, digital divide and fingerprint), personal data protection in the field of education, and secure protection of devices and password creation.

Despite the limitation that there are few studies specifically on digital safety, we provide empirical evidence of the importance of initial training. This study shows the need for in-depth research on teaching digital safety, as well as for the promotion and inclusion of content on safety in university curricula – a measure already in place in other stages of education, along the lines of the PIES model (Šimandl & Vanícek, 2017), the CIPA program (Yan, 2009), and the TAIS project (Chou & Peng, 2011). Among future lines of research, we propose developing deeper knowledge of curricular inequalities across different university study programs (not only those that train teachers); researching the impact of training on matters of safety for external practices, initial training, and professional practice; and establishing how to teach and evaluate this area of competence beyond the preservice teacher's mere self-perception. Evaluation can be advanced through interdisciplinary studies in Education, Psychology, Medicine, Economics, Law, and Engineering – areas with a close relationship to subcompetences related to safety.

## Funding Agency

This research received institutional support from the Grant FPU17/05164 of the Ministry of Education's University Faculty Training (FPU) programme. Partially funded by University of Granada (Excellence Scientific Unit «Training and Professional Development of Teachers» - Plan of Research and Transfer 2017) and University of Coimbra (Faculty of Psychology and Education Sciences).

## References

Álvarez, J., & Gisbert, M. (2015). Information literacy grade of secondary school teachers in Spain - Beliefs and self-perceptions. [Grado de alfabetización informacional del profesorado de secundaria en España: Creencias y autopercepciones]. *Comunicar*, *45*, 187-194. https://doi.org/10.3916/C45-2015-20

Anderson, J.M. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308-313.

https://doi.org/10.1016/S0167-4048
Barrow, C., & Heywood-Everett, G. (2006). The experience of English educational establishments: Summary and recommendations [online]. British Educational Communications and Technology Agency (BECTA). https://bit.ly/2Gz6aoD
Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education*, *14*(1), 44-53. https://doi.org/10.1016/j.iheduc.2010.03.006
Chou, H.L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, *65*, 334-345. https://doi.org/10.1016/j.chb.2016.08.034
De-Waal, E., & Grösser, M. (2014). On safety and security in education: Pedagogical needs and fundamental rights of learners. *Educar*, *50*(2), 339-361. https://doi.org/10.5565/rev/educar.44
Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L., & Skouteris, H. (2018). Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years. *British Journal of Educational Technology*, *49*(1), 45-55. https://doi.org/10.1111/bjet.12529
Engen, B.K., Giæver, T.H., & Mifsud, L. (2015). Guidelines and regulations for teaching digital competence In schools and teacher education: a weak link? *Nordic Journal of Digital Literacy*, *10*, 172-186. https://bit.ly/2SNLcZM
Esteve, F.M., Gisbert, M., & Lázaro, J.L. (2016). La competencia digital de los futuros docentes: ¿Cómo se ven los actuales estudiantes de educación? *Perspectiva Educacional*, *55*(2), 38-54. https://doi.org/10.4151/07189729-Vol.55-Iss.2-Art.412
Fernández-Cruz, F.J., & Fernández-Díaz, M.J. (2016). Generation Z's teachers and their digital skills. [Los docentes de la Generación Z y sus competencias digitales]. *Comunicar*, *46*, 97-105. https://doi.org/10.3916/C46-2016-10
Fernández-Montalvo, J., Peñalva, A., & Irazabal, I. (2015). Hábitos de uso y conductas de riesgo en Internet en la preadolescencia. [Internet use habits and risk behaviours in preadolescence]. *Comunicar*, *44*, 113-121. https://doi.org/10.3916/C44-2015-12
Flores-Lueg, C., & Roig-Vila, R. (2016). Percepción de estudiantes de Pedagogía sobre el desarrollo de su competencia digital a lo largo de su proceso formativo. *Estudios Pedagógicos*, *42*(3), 129-148. https://doi.org/10.4067/S0718-07052016000400007
Fondo de las Naciones Unidas para la Infancia (Ed.) (2017). Niños en un mundo digital. Estado mundial de la Infancia 2017. https://uni.cf/2FUq60R
Instituto Nacional de Tecnologías Educativas y Formación del Profesorado (Ed.) (2017). *Common digital competence framework for teachers*. Madrid: INTEF. https://bit.ly/1Y88rd6
Janssen, J., Stoyanov, S., Ferrari, A., Punie, Y., Pannekeet, K., & Sloep, P. (2013). Experts' views on digital competence: Commonalities and differences. *Computers & Education*, *68*, 473-481. https://doi.org/10.1016/j.compedu.2013.06.008
Jones, L.M., Mitchell, K.J., & Finkelhor, D. (2013). Online harassment in context: Trends from three youth internet safety surveys. *Psychology of Violence*, *3*(1), 53-69. https://doi.org/10.1037/a0030309
Krumsvik, R. (2009). Situated learning in the network society and the digitised school. *European Journal of Teacher Education*, *32*(2), 167-185. https://doi.org/10.1080/02619760802457224
Lueg, C. (2014). Competencia digital docente: Desempeños didácticos en la formación inicial del profesorado. *Hachetetepé*, *9*, 55-70. https://bit.ly/2Iq3Odu
Napal, M., Peñalva-Vélez, A., & Mendióroz, A. (2018). Development of digital competence in secondary education teachers' training. *Education Sciences*, *8*, 104. https://doi.org/10.3390/educsci8030104
Panayides, P. (2013). Coefficient Alpha: Interpret with caution. *Europe's Journal of Psychology*, *9*(4), 687-696. https://doi.org/10.5964/ejop.v9i4.653
Parlamento y Consejo Europeo (Ed.) (2006). Recomendación 2006/962/CE, de 18 de diciembre de 2006, sobre las competencias clave para el aprendizaje permanente. Diario Oficial L 394 de 30 de diciembre de 2006. https://bit.ly/2PQgYCV
Pedro, K.M., & Chacon, M.C.M. (2017). Pesquisas na internet: Uma análise das competências digitais de estudantes precoces e/ou com comportamento dotado. *Educar em Revista*, *33*(66), 227-240. https://doi.org/10.1590/0104-4060.50335
Prendes, M.P., Castañeda, L., & Gutiérrez, I. (2010). Competencias para el uso de TIC de los futuros maestros. [ICT competences of future teachers]. *Comunicar*, *35*, 175-182. https://doi.org/10.3916/C35-2010-03-11
Redecker, C. (2017). European framework for the digital competence of educators: DigCompEdu. In Punie, Y. (Ed.), *Publications office of the European Union*. https://doi.org/10.2760/159770, https://doi.org/10.2760/159770
Shin, S.K. (2015). Teaching critical, ethical, and safe use of ICT in pre-service teacher education. *Language Learning & Technology*, *19*(1), 181-197. https://doi.org/10125/44408
Simandl, V. (2015). ICT teachers and technical e-safety: Knowledge and routines. *International Journal of Information and Communication Technologies in Education*, *4*(2), 50-65.
Simandl, V., & Vaní ek, J. (2017). Influences on ICT teachers' knowledge and routines in a technical e-safety context. *Telematics and Informatics*, *34*(8), 1488-1502. https://doi.org/10.1016/j.tele.2017.06.012
Tejada, J., & Pozos, K.V. (2018). Nuevos escenarios y competencias digitales docentes: Hacia la profesionalización docente con TIC. *Profesorado*, *22*(1), 41-67. https://bit.ly/2GQmv7H
Tigelaar, D.E., Dolmans, D.H., Wolfhagen, I.H., & Van-Der-Vleuten, C.P. (2004). The development and validation of a framework for teaching competencies in higher education. *Higher Education*, *48*(2), 253-268. https://doi.org/10.1023/B:HIGH.0000034318.74275.e4
Woollard, J., Wickens, C., Powell, K., & Russell, T. (2009). Evaluation of e-safety materials for initial teacher training: Can Jenny's Story'make a difference? *Technology, Pedagogy and Education*, *18*(2), 187-200. https://doi.org/10.1080/14759390902992659
Yan, Z. (2009). Differences in high school and college students' basic knowledge and perceived education of Internet safety: Do high school students really benefit from the Children's Internet Protection Act? *Journal of Applied Developmental Psychology*, *30*(3), 209-217. https://doi.org/10.1016/j.appdev.2008.10.007