Comunicar, nº 61, v. XXVII, 2019 | Revista Científica de Educomunicación | ISSN: 1134-3478; e-ISSN: 1988-3293
www.revistacomunicar.com | www.comunicarjournal.com

Competencia de futuros docentes en el área de seguridad digital

Competence of future teachers in the digital security area

Dra. María-Jesús Gallego-Arrufat es Catedrática de Tecnología Educativa en la Universidad de Granada (España) (mgallego@ugr.es) (https://orcid.org/0000-0002-2296-5431)
Norma Torres-Hernández es Personal Investigador en Formación (FPU) del Departamento de Didáctica y Organización Escolar de la Universidad de Granada (España) (normath@ugr.es) (https://orcid.org/0000-0003-4744-0313)
Dra. Teresa Pessoa es Profesora Titular de la Facultad de Psicología y de Ciencias la Educación de la Universidad de Coimbra (Portugal) (tpessoa@fpce.uc.pt) (https://orcid.org/0000-0002-5252-3618)

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.

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.

PALABRAS CLAVE | KEYWORDS

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

Recibido: 2019-02-26 | Revisado: 2019-04-30 | Aceptado: 2019-05-10 | Preprint: 2019-07-15 | Publicado: 2019-10-01
DOI https://doi.org/10.3916/C61-2019-05 | Páginas: 57-67

1. Introducción

Con la competencia digital se evidencian destrezas cognitivas, actitudinales y técnicas que pueden ayudar a mitigar numerosos problemas y retos de la sociedad del conocimiento. Su naturaleza es dinámica y transversal, y se considera competencia clave en el desarrollo de la ciudadanía digital y fundamental en los procesos de aprendizaje para toda la vida (Janssen, Stoyanov, Ferrari, Punie, Pannekeet, & Sloep, 2013). Ser competente digitalmente es hacer un uso crítico y seguro de las tecnologías para el trabajo, el ocio y la comunicación e implica usarlas para recuperar, evaluar, almacenar, producir, presentar e intercambiar informaciones, así como para comunicar y participar en redes de colaboración a través de Internet (Parlamento & Consejo Europeo, 2006). Incluye aspectos tecnológicos, informacionales, multimedia y comunicativos que favorecen el uso crítico, responsable y creativo de la tecnología, fundamentales en los procesos de aprendizaje y participación de la sociedad del siglo XXI (Esteve, Gisbert, & Lázaro, 2016; Napal, Peñalva-Vélez, & Mendióroz, 2018).

El marco para el desarrollo de la competencia digital en Europa (DigComp) proporciona la estructura para su comprensión y valoración, y se consolida y expande internacionalmente con el marco europeo para la competencia digital de los educadores (DigCompEdu) (Redecker, 2017). En Portugal y España se emplea para evaluar la competencia digital del usuario, con diferentes niveles competenciales, básico (nivel A), medio o independiente (nivel B) y avanzado o competente (nivel C), en función de los conocimientos, habilidades y destrezas que este posee. En Iberoamérica se adopta para buscar, seleccionar y procesar críticamente información, comunicar usando diversos soportes, actuar con responsabilidad y aprovechar la tecnología para aprender y resolver problemas (Lueg, 2014).

La competencia digital docente (CDD) es el conjunto integrado de características personales, conocimientos, habilidades y actitudes necesarios para la actuación eficaz en diversos contextos docentes (Tigelaar, Dolmans, Wolfhagen, & Van-der-Vleuten, 2004). Moviliza habilidades y destrezas relacionadas con el uso de las TIC para generar conocimiento (Flores-Lueng & Roig, 2016) potenciando una utilización más consciente y positiva de los medios en educación (Pedro & Chacon, 2017). Conlleva saber usar las tecnologías para enseñar y aprender con criterios didácticos y pedagógicos y con sentido moral y ético (Krumsvik, 2009). Resulta fundamental entenderla desde una perspectiva holística, es decir, tanto para integrar las TIC adecuadamente en el currículo y en el aula, como para asegurar el desarrollo de la competencia digital del alumnado (Álvarez & Gisbert, 2015; Fernández-Cruz & Fernández-Díaz, 2016; Prendes, Castañeda, & Gutiérrez, 2010).

1.1. El área de seguridad en la Competencia Digital Docente

La seguridad adquiere un significado de protección de la información y comunicación de los usuarios contra los problemas generados por el uso de las TIC (Barrow & Heywood-Everett, 2006). Está relacionada con la privacidad, la integridad y la eficiencia de la tecnología e información de Internet (Anderson, 2003). Se refiere a los conocimientos, habilidades y actitudes del profesorado para diseñar y desarrollar experiencias de aprendizaje para promover, modelar y formar al alumnado como ciudadanos digitalmente responsables. Para adquirir esta competencia, el papel de quien enseña alcanza especial protagonismo, porque su figura es modelo y guía que cuida, orienta y forma sobre el uso responsable en la navegación, comunicación y colaboración y compartir información a través de Internet. Sin embargo, puede ser un problema debido a una concepción errónea por la que los docentes enseñan sobre la seguridad pretendiendo que el alumnado solo entienda o tenga un concepto sobre Internet (Edwards & al., 2018). DigComp (2016) y DigCompEdu (2017) han sido base para elaborar el marco de referencia de la competencia digital docente (MCCDD, 2017). Incluyen competencias sobre seguridad digital, como la protección de datos personales y el respeto a la privacidad, la protección de la salud, y la adecuada gestión de la identidad digital. Destacan el uso responsable, el respeto a los principios de privacidad en línea aplicables a sí mismo y a otros y el cuidado del medio ambiente. En el área de seguridad, el usuario competente es capaz de revisar la configuración de seguridad de los sistemas y las aplicaciones; reaccionar si su equipo informático se infecta con un virus, y configurar, modificar el cortafuegos y los parámetros de seguridad de sus dispositivos electrónicos; encriptar correos y archivos; aplicar filtros para evitar el spam del correo (http://bit.ly/30qMppL).

Las investigaciones sobre seguridad digital (e-safety, digital security, Internet safety o Internet security) se abordan desde diferentes disciplinas como Psicología, Educación y Derecho, y su producción aumenta en la última década (Jones, Mitchell, & Finkelhor, 2013; Shin, 2015; Šimandl & Vanícek, 2017; Chou & Peng, 2011; Napal, Peñalva-Vélez, & Mendióroz, 2018). Tanto el profesorado en servicio como los futuros docentes muestran bajo dominio en temas relacionados con la seguridad digital (De-Waal & Grösser, 2014).

Distintos informes, estudios y planes estratégicos buscan ayudar a construir un clima de confianza para mitigar o prevenir los efectos de los problemas relacionados con la seguridad, especialmente en colectivos vulnerables, mediante acciones como la incorporación de contenidos sobre seguridad y uso responsable de Internet; el diseño de itinerarios para la prevención, sensibilización, concienciación y mejora de la confianza y comunicación en el uso de Internet; el fomento de la competencia digital de padres y profesorado enfatizando habilidades sociales y emocionales para apoyar y entender el uso que hacen los menores de las TIC y los problemas que se pueden evitar, entre otros.

1.2. Formación de futuros docentes en seguridad digital

Los sistemas educativos reconocen la importancia de la formación del profesorado para el dominio de las TIC y en particular sobre la seguridad, aunque en los programas de formación inicial del profesorado el tratamiento de la competencia digital suele ser transversal (Napal, Peñalva-Vélez, & Mendióroz, 2018).

En los planes de estudio se observa una clara dispersión de las asignaturas obligatorias de tecnologías en la educación, y su presencia es distinta en universidades, institutos politécnicos u otros centros de Educación Superior. Indudablemente, el futuro docente necesita conocimientos (pedagógicos y de contenido), habilidades (sociales y técnicas) y actitudes vinculadas a la seguridad digital y cómo enseñarla.

Es necesaria una formación inicial con un enfoque coherente donde se enseñe la seguridad como una cuestión de alta prioridad en el ámbito educativo, en especial en programas de formación en un marco común de competencia digital.

Se espera que los docentes asuman responsabilidad en la enseñanza de la seguridad digital y orienten a los estudiantes sobre las normas de comportamiento en Internet, aunque es frecuente carecer de una preparación adecuada para entender los riesgos y los comportamientos poco éticos (Chou & Peng, 2011). El educador puede servir de modelo, ayudar a mejorar los comportamientos de los estudiantes cuando utilizan la tecnología, dialogar sobre riesgos y daños, e influir significativamente a través de su propia actuación (Chou & Chou, 2016; Šimandl, 2015; Shin, 2015).

En suma, la formación inicial debería responder a las necesidades actuales de la sociedad a fin de que los profesionales se adapten a los procesos de innovación y sean capaces de competir en y para el uso de la tecnología en el mercado laboral (Tejada & Pozos, 2018). Se reclama una nueva cultura digital para el docente útil, práctica y orientada a la formación de ciudadanos críticos y responsables.

Diversos estudios señalan la necesidad apremiante de que los centros de formación adopten un enfoque coherente que garantice la formación para promover la seguridad como una cuestión de alta prioridad en el ámbito educativo y en especial en programas de formación docente (Barrow & Heywood-Everett, 2006; Woollard, Wickens, Powell, & Rusell, 2009; Chou & Peng, 2011; Engen, Giæver, & Mifsud, 2015; Shin, 2015).

Se trabaja internacionalmente para mejorar la seguridad en organismos asiáticos y europeos a través de la educación y la formación. En Taiwán el programa TAIS (2006-2010) identificó cuatro aspectos para formar docentes competentes: la seguridad y protección de comunicaciones, la idoneidad de la información, la seguridad en línea y la propia del uso de dispositivos tecnológicos.

En la UE, organismos como British Educational Communications and Technology Agency (BECTA) y distintos estudios en países nórdicos y República Checa enfatizan la formación del profesorado, concluyendo que experiencias previas, conocimientos, prácticas, opiniones y percepciones determinarán cómo deberán los docentes enseñar, resolver y atender la problemática sobre seguridad digital (Engen, Giæver, & Mifsud, 2015; Šimandl & Vanícek, 2017). A nivel mundial, UNICEF plantea la importancia de la consolidación de acciones y medidas educativas para y desde los centros educativos, la responsabilidad compartida de padres y profesorado y la necesidad de destinar recursos educativos a programas educativos y preventivos que ayuden a evitar amenazas y a proteger contra los peligros del mundo digital (UNICEF, 2017).

Los objetivos del estudio son:

1) Identificar el nivel de competencia digital en el área de seguridad de los futuros docentes.

2) Describir el perfil competencial que tienen los futuros docentes en los diferentes ámbitos de la seguridad (interacción con tecnologías, compartir información y contenidos digitales, protección de datos personales, protección de la salud, netiqueta, identidad digital y acoso en redes sociales e Internet).

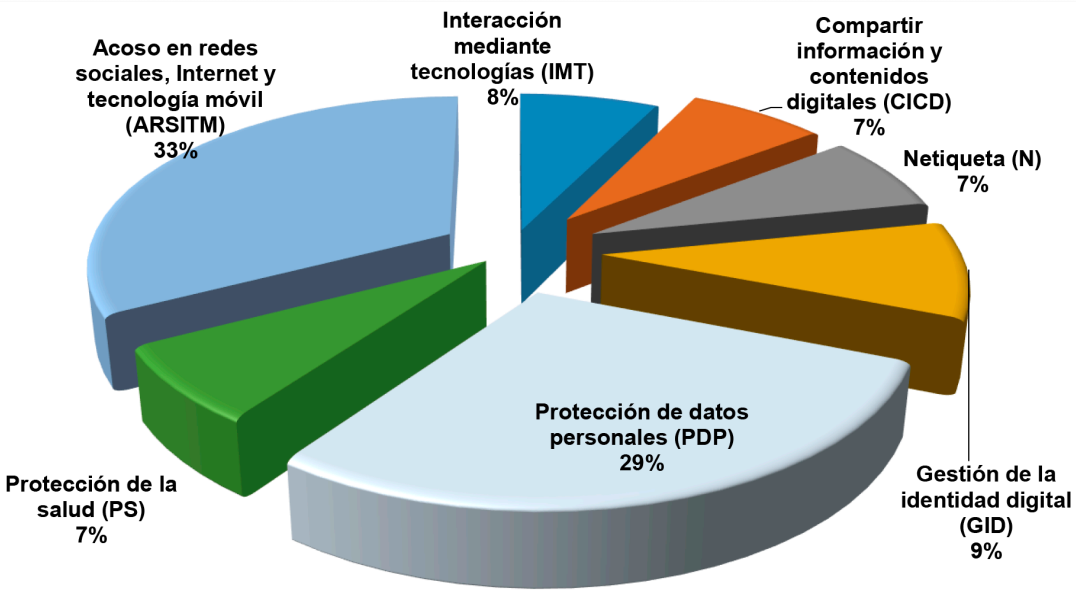
3) Explorar diferencias según sexo, género y edad de inicio en redes sociales en cada uno de los diferentes ámbitos, a fin de detectar necesidades formativas para mejorar su competencia digital en el área de seguridad.

4) Proponer acciones pedagógicas en el área de seguridad, apropiadas a las fortalezas y debilidades evidenciadas por los futuros docentes.

2. Material y métodos

Se realiza un estudio descriptivo y transversal en el que participaron 317 estudiantes de Grado entre 18 y 43 años de edad (M=22,2; DT=4,8), procedentes de cuatro universidades españolas y una portuguesa, de los cuales 248 (78,2%) son mujeres y 69 (21,8%) son hombres.

Figura 1. Categorías del cuestionario sobre seguridad



El instrumento es un cuestionario elaborado ad hoc para futuros docentes, diseñado a partir de las áreas de seguridad de DigComp 2.0, DigCompEdu, del marco común de competencia digital docente (INTEF, 2017), del proyecto NETS*S (ISTE, 2007), así como de la herramienta de autodiagnóstico de las competencias digitales de la Junta de Andalucía (http://bit.ly/2YnNixx).

El cuestionario, con 59 ítems distribuidos en siete categorías (Figura 1), ha sido validado por ocho expertos de universidades de España y Portugal con experiencia docente e investigadora en tecnologías

en educación. Obtiene un Alfa de Cronbach α=.923, y en los criterios de claridad (.916), pertinencia (.914) e importancia (.946) respectivamente. Los ítems se distribuyen en conocimientos (C=24 ítems), habilidades y prácticas (HyP=23 ítems) y actitudes (A=10 ítems), agrupándose en las dimensiones de la Tabla 1.

Tabla 1. Dimensiones cuestionario seguridad digital

Conocimientos (C)	Conocimientos técnicos para etiquetar información con otras personas (CICD2). Conocimientos técnicos para compartir información con otras personas (CICDI). Concepto de identidad digital (GID1). Concepto de reputación digital (GID4). Conocimiento sobre reglas de comunicación y comportamiento en red (N1). Creación de contraseñas seguras (PDP1). Riesgos sobre apropiación indebida de nombres de usuario y contraseñas (PDP3). Huella digital y seguridad de los navegadores para evitar guardar contraseñas y datos de navegación (PDP10). Importancia de la protección de datos (PDP15). Riesgos en salud física y psicológica por uso de Internet (PSI). Medidas o protocolos para proteger salud física y psicológica (PS2). Aplicación de patrones de actuación que eviten riesgos, abusos, estafas u otros problemas (PS4). Casos de acoso y abuso en redes sociales (ARSITM1). Uso inadecuado de redes sociales (ARSTM4). Medidas preventivas para evitar problemas sobre uso inadecuado de tecnologías (ciberacoso o ciberbullying) (ARSITM5). Cómo actuar en caso de ciberacoso u otro problema relacionado con seguridad (ARSITM7). Identificar situaciones sobre temas relacionados con abusos en la red y ciberacoso (ARSITM9). Riesgos de mayor incidencia y relación con ciberacoso (ARSITM13). Situaciones de riesgo a través de las tecnologías e Internet (ARSITM14). Red social más común de alto riesgo para acosar (ARSITM15). Efectos sociales por ciberacoso y otros problemas en la red (ARSITM16). Causas que generan riesgos o acoso a través de Internet, redes sociales o dispositivos tecnológicos (ARSITM17). Áreas de competencia digital docente que ayudan a prevenir situaciones de acoso (ARSITM18).
Actitudes (A)	Cuidar la imagen en redes sociales (GID2). Promover en el grupo de iguales la protección y el cuidado de la imagen digital (GID3). Respetar el lenguaje al escribir en diferentes redes sociales (N2). Cuidar escritura en redes sociales (N3). No dar información personal a desconocidos (PDP7). Sentimientos de malestar y rechazo al conocer casos de acoso o abuso en redes sociales (ARSITM2). Tener actitudes positivas que eviten problemas relacionados con el uso de Internet que afecten la salud física o psicológica (ARSITM6). Responsabilidad como futuro educador para implementar acciones educativas y preventivas relacionadas con la seguridad (ARSITM10). Importancia de poseer conocimientos, practicar y dar ejemplo de conductas que favorezcan uso responsable de Internet (ARSITM11).
Habilidades y prácticas (HyP)	Inicio en redes sociales (IP3). Lugares de acceso a Internet (IP4). Uso de determinados dispositivos/herramientas tecnológicas (IMT1). Número de cuentas de correo electrónico utilizadas (IMT2). Participación activa en redes sociales (IMT3). Difundir y reenviar con facilidad información (CICD3). Difundir y reenviar información sin consentimiento de otras personas (CICD4). Buscar información y actualización en temas como la identidad y gestión de datos (GID5). Uso de reglas de comunicación y comportamiento en función de qué red social o correo se utiliza (N4). Cambio frecuente de contraseñas (PDP2). Compartir nombres de usuario y contraseñas (PDP4). Uso de contraseñas diferentes para evitar robo (PDP5). Uso de patrones de desbloqueo y contraseñas (PDP6). Uso de contraseñas seguras (PDP8). Desactivar opciones para guardar contraseñas en dispositivos (PDP9). Bloqueo de dispositivos al alejarse o dejar dispositivos cuando se está con otras personas (PDP11). Cubrir cámara de teléfonos y ordenadores si no se utilizan (PDP12). Publicación de información que pueda dañar imagen, identidad o reputación digital (PDP13). Recomendar a contactos tener cuidado con su identidad y reputación digital (PDP14). Búsqueda de información sobre protección de datos y reputación digital (PDP16). Aplicar medidas o protocolos para cuidar salud física y psicológica (PS3). Compartir información con grupos de iguales o familia relacionada con problemas de acoso y seguridad en redes (ARSITM3). Asistencia a acciones formativas (ARSITM8). ¿Cuándo aprender al uso adecuado de las TIC? (ARSITM12).

El análisis estadístico se realiza con SPSS 24.0. Mediante un procedimiento clúster bietápico, se realiza la clasificación de los participantes en niveles de competencia, con una solución de tres categorías (nivel de significación 5%).

También se realiza un análisis descriptivo univariante, calculando la media e intervalo de confianza al 95%, así como la desviación típica. Para las variables cualitativas se ha calculado la frecuencia y porcentaje. La relación entre ellas se analiza mediante el test chi-cuadrado. Mediante el coeficiente de correlación no paramétrica Rho de Spearman se analiza la asociación entre las variables numéricas. Para estudiar la relación de las variables numéricas y las dicotómicas aplicamos la prueba no paramétrica de Mann-Whitney, calculando el tamaño del efecto.

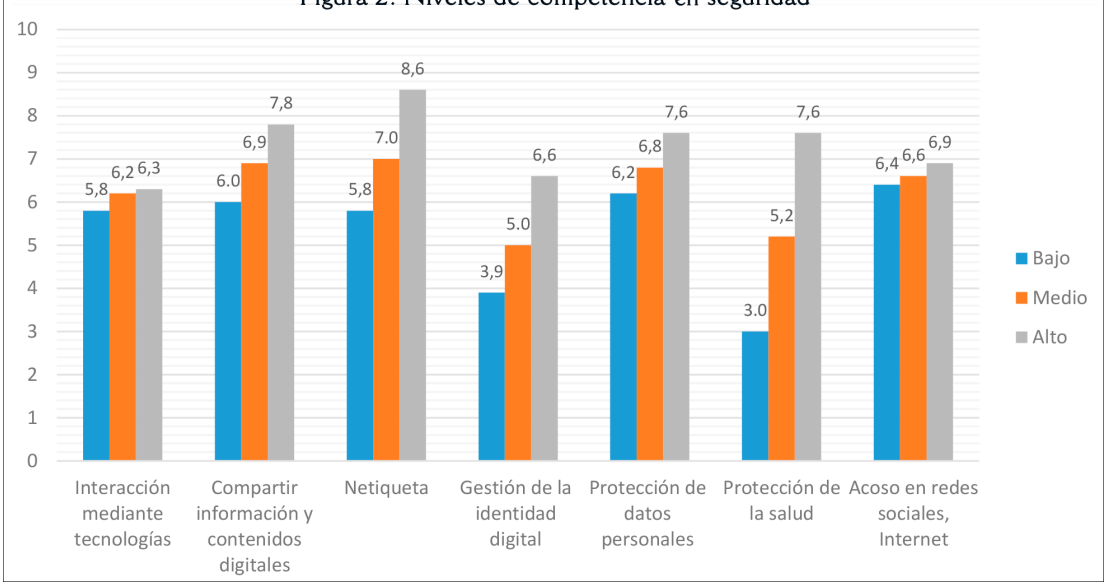
La relación entre las variables categóricas y numéricas se analiza a través de la prueba no paramétrica de Kruskal-Wallis. En las pruebas que resultan estadísticamente significativas se ha utilizado el test de Mann-Whitney para comparar las categorías por pares.

3. Resultados

3.1. Niveles de competencia en seguridad digital

El análisis realizado permite identificar tres grupos de competencia digital en el área de seguridad con niveles alto, medio y bajo, respectivamente. Se comparan las valoraciones medias para cada una de las categorías del cuestionario (Figura 2).

Figura 2. Niveles de competencia en seguridad



El 34% de los casos son «docentes digitalmente seguros». Se caracterizan por usar pocos dispositivos tecnológicos, cuentas de correo electrónico y redes sociales (IMT); compartir información con el consentimiento de terceras personas (CICD); y conocer, aplicar y respetar normas de comunicación y comportamiento (N). En cuanto a la identidad y reputación digital, evitan publicar información personal que pueda afectar a su imagen digital (GID). Utilizan diferentes contraseñas que procuran cambiar frecuentemente. Saben y practican patrones de bloqueo en sus dispositivos y cómo evitar que sus contraseñas se queden grabadas en equipos ajenos (PDP) y son conscientes de la importancia de evitar que el abuso de Internet afecte su salud (PS).

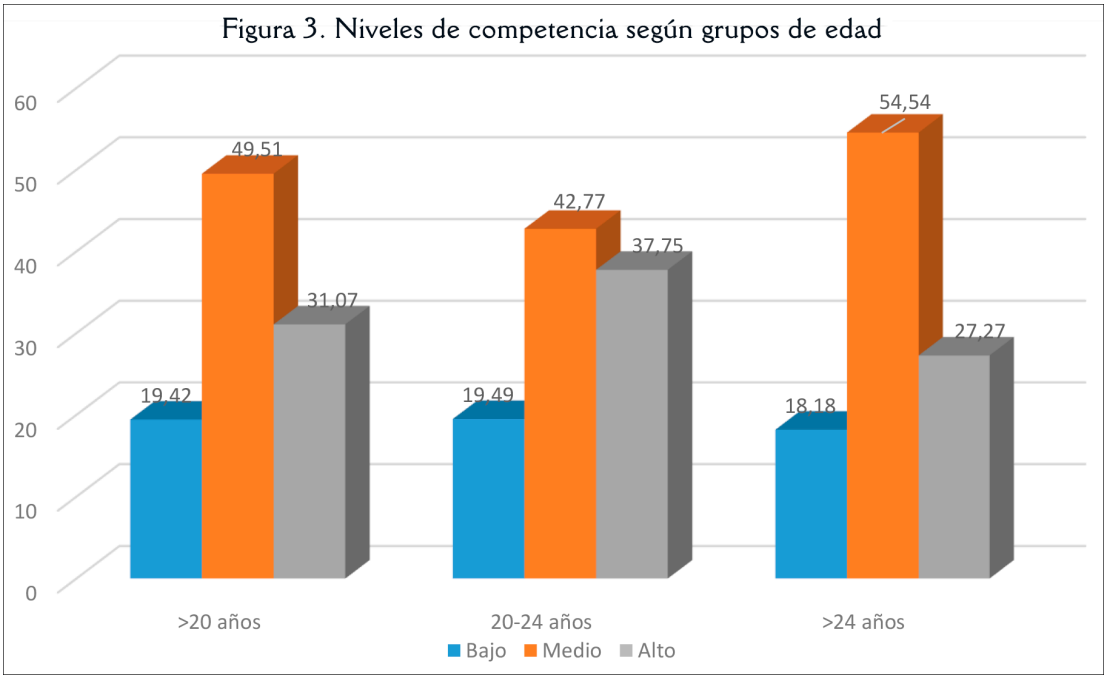
El nivel medio, «docentes en riesgo digital medio», constituye el 47% de los casos. Se consideran con capacidad de subir y compartir información en redes sociales (CICD), conocen normas en la comunicación, aunque en ocasiones no las usan (N) y cuidan su imagen en redes sociales, pero pueden tener algún dato personal en Internet que no se corresponde con la realidad (GID). Evitan compartir sus contraseñas e información personal en redes sociales, y poseen información acerca de la protección de cuentas (PDP).

Tienen información sobre los riesgos que Internet o el uso excesivo que las redes sociales tienen para la salud física y psicológica y conocen medidas y protocolos de protección aun cuando no siempre las aplican (PS). El 18% de los casos se ubica en el nivel bajo, «docentes en riesgo digital». Todo el tiempo están conectados, manejan más de cinco dispositivos, usan diferentes cuentas de correo y más de cinco redes sociales (IMT). Se consideran capaces de subir y compartir fotos y por lo general no encuentran dificultades en el manejo de las redes sociales (CICD). Desconocen y, por tanto, no suelen aplicar normas de comunicación y comportamiento (N). Con independencia del grupo al que pertenecen, solo el 7% ha participado en alguna acción formativa sobre temas relacionados con la seguridad digital.

3.2. Perfiles de competencia en seguridad

Teniendo en cuenta la edad, en el grupo 20-24 años se concentra el mayor número de participantes (50%) en los tres niveles de competencia en seguridad. Los mayores de 24 años representan el 17%. Se distinguen los «futuros docentes digitalmente seguros», que muestran una mayor competencia en netiqueta (8,62), en compartir información y contenidos digitales (7,76), protección de datos personales (7,64) y protección de la salud (7,64), aunque con menor puntuación en acoso en redes sociales, Internet y teléfonos móviles (6,87), gestión de la identidad digital (6,59) e interacción mediante tecnologías (6,27).

Figura 3. Niveles de competencia según grupos de edad



En la Figura 3 se aprecia esta tendencia. Los «futuros docentes en riesgo digital medio» obtienen valoraciones altas en las mismas categorías, aunque con medias menores: netiqueta (6,97), compartir información y contenidos digitales (6,88), protección de datos personales y protección de la salud (6,76), acoso en redes sociales, Internet y teléfonos móviles (6,64) e interacción mediante tecnologías (6,20). Aún son más bajas en las categorías protección de la salud (5,24) y gestión de la identidad digital (4,99). Los «futuros docentes en riesgo digital» muestran mayor competencia en acoso en redes sociales, Internet y teléfonos móviles (6,40), protección de datos personales (6,20), compartir información y contenidos digitales (5,94) y netiqueta (5,79). Muestran menor nivel competencial en los ámbitos de gestión de la identidad digital (3,93) y protección de la salud (3,04).

Según el género, en los tres grupos de competencia hay más mujeres, con un nivel medio de competencia el 38% de los casos, nivel alto el 23% y bajo el 15%. El grupo de hombres con un nivel alto representa el 9% del total, y tienen niveles medio y bajo el 8,5% y 4,4% respectivamente. De acuerdo a la edad de inicio en redes sociales, el nivel de competencia medio y alto tiene una relación significativa

con quienes comenzaron a usarlas antes de los 12 años. También se observa en el nivel medio de quienes comenzaron entre 12-14 años. La relación entre nivel de competencia total y nivel bajo de los tres grupos de edad de inicio en redes sociales es menos significativa.

El nivel de competencia se relaciona significativamente con los lugares de acceso. La mayor parte de quienes tienen un nivel de competencia bajo están permanentemente conectados. El porcentaje es menor en los grupos con competencia media y alta. En el grupo con competencia media, casi la mitad se conectan desde un lugar determinado, mientras que un porcentaje similar se conecta permanentemente. Los participantes con competencia alta se conectan con más frecuencia desde un lugar, aunque casi la mitad lo hace con conexión permanente.

3.3. Diferencias en conocimientos, actitudes, habilidades y prácticas

Se evidencian diferencias en los resultados según las dimensiones del cuestionario. En la primera, conocimientos (C) sobre la seguridad digital, se han tenido en cuenta 24 ítems, cuyas valoraciones oscilan entre 10 (ARSITM14 y 18) y 1,9 (ARSITM17), obteniendo una media de 6,7. Las temáticas en las que los participantes poseen en mayor medida conocimientos son aquellas que ayudan a prevenir situaciones de riesgo, protección de datos personales y conocimientos técnicos para compartir información con otros. Menos conocimiento tienen sobre las reglas de comunicación y comportamiento en la red, los efectos sociales del ciberacoso, medidas o protocolos para proteger la salud física y psicológica y conceptos como identidad digital o reputación digital.

Las puntuaciones medias en la dimensión actitudes (A) de los futuros docentes sobre problemas y riesgos asociados con la seguridad varían entre 10 (ARSITM10) y 6,24 (ARSITM6), con una media de 8,77. Se considera la responsabilidad que perciben para implementar acciones educativas y preventivas relacionadas con la seguridad, la necesidad de adquirir conocimientos, practicar y dar ejemplo de conductas que favorezcan el uso responsable y sentimientos de malestar y rechazo cuando conocen casos de abuso en redes sociales u otros problemas. Otras actitudes implican no dar información personal a desconocidos, promover en el grupo de iguales la protección y el cuidado de la imagen virtual, tener actitudes positivas para evitar problemas relacionados con el uso de Internet que afecten la salud física o psicológica.

En la dimensión Habilidades y Prácticas seguras (HyP), con 23 ítems, las medias varían entre 10 (ARSITM1 y ARSITM8) y 2,2 (ARSITM8), y tiene el promedio más bajo (6,03). En ellos se valoran las prácticas seguras entre las que se encuentran el cuidado en la publicación de información que puede dañar imagen, identidad o reputación digital, evitar compartir nombres de usuario y contraseñas, uso de contraseñas diferentes para evitar robo y bloqueo de dispositivos. Y entre las prácticas menos seguras la aplicación de medidas o protocolos para cuidar la salud física y psicológica, uso de dispositivos y herramientas tecnológicas, difundir y reenviar información con facilidad, cambio de contraseñas poco frecuente, aplicación de protocolos de seguridad en navegación y de protección de datos personales y participación en acciones formativas relacionadas con seguridad.

3.4. Correlaciones entre variables del estudio

La Tabla 2 (https://doi.org/10.6084/m9.figshare.8150516.v1) recoge las correlaciones no paramétricas entre las variables numéricas del estudio. Se observa que la edad está positivamente relacionada con la edad de inicio en redes sociales y la interacción mediante tecnologías. Estas dos últimas variables están positivamente relacionadas entre sí. La interacción mediante tecnologías se asocia negativamente con la gestión de la identidad digital y protección de la salud y positivamente con la competencia total. Compartir información y contenidos digitales está positivamente asociada con la netiqueta, la gestión de la identidad digital, la protección de datos personales, la protección de la salud, el acoso en redes sociales, Internet y móviles y la competencia total. La netiqueta se asocia positivamente con: la gestión de la identidad digital, la protección de datos personales, la protección de la salud, el acoso en redes sociales, Internet y móviles y competencia total. La gestión de la identidad digital se relaciona positivamente con: la protección de datos personales, la protección de la salud, el acoso en redes sociales, Internet y móviles y la competencia total. Protección de datos personales está además positivamente asociada a la protección de la salud y

la competencia total. La protección de la salud se asocia directamente con el acoso en redes sociales, Internet y teléfonos móviles, así como con la competencia total. Estas dos últimas variables están también relacionadas entre sí.

En el análisis de la relación del sexo con la edad, edad de inicio en redes sociales y competencia en redes sociales se observa que los hombres se inician antes que las mujeres en las redes sociales (13,46 años Vs 13,76 años). La competencia de compartir información y contenidos digitales es mayor en mujeres (7,10) que en hombres (6,59). La competencia en gestión de la identidad digital es superior en hombres (5,72) que en mujeres (5,21). Por último, la competencia en protección de la salud es mayor también en hombres (6,27) que en mujeres (5,45).

La edad de los participantes únicamente está relacionada con la edad de inicio en redes sociales. Las pruebas no paramétricas de Mann-Whitney indican que la edad de inicio es menor en el grupo de menos de 20 años, seguido de los de 20-24 años, y por último los que tienen más de 24 años. La edad de inicio en redes sociales está significativamente relacionada con la interacción mediante tecnologías. Los participantes que se han iniciado antes de 12 años tienen menos competencia en esta dimensión que los que se han iniciado entre 12 y 14 y posteriormente.

4. Discusión y conclusiones

Con este estudio se trata de identificar los niveles y perfiles de futuros docentes en el área de seguridad digital, para detectar necesidades formativas que permitan plantear acciones en la formación inicial universitaria. Para ello se diseña un instrumento que muestra evidencias de validez de contenido y de fiabilidad, con una estimación alta del Alfa de Cronbach (Panayides, 2013).

Objetivo 1: Para identificar el nivel de competencia digital en el área de seguridad de los futuros docentes se realiza un análisis de clústers, que permite identificar tres niveles competenciales teniendo en cuenta las categorías de la seguridad digital del cuestionario. Al evaluar el nivel de competencia digital, el 36,85% de los futuros docentes obtienen un nivel medio, resultado similar al obtenido por Fernández-Cruz y Fernández-Díaz (2016) con futuros docentes de la denominada «Generación Z» y Napal, Peñalva-Vélez y Mendióroz (2018) con profesorado en formación de secundaria.

Objetivo 2: Se describe el perfil competencial que tienen los futuros docentes según la diferenciación entre «docentes digitalmente seguros» (nivel alto), «docentes en riesgo medio» (nivel medio) y «docentes en riesgo digital» (nivel bajo). En general predominan las mujeres de 20-24 años, que comparten como característica común que un 93% no se ha formado en esta área, aun cuando intentan realizar prácticas seguras. El aprendizaje autodidacta sobre la seguridad se ha adquirido fuera de la educación formal, pero se evidencia la necesidad de formación (Engen, Giæver, & Mifsud, 2015). En cuanto al género en relación con las categorías del cuestionario existe escasa diferencia (6,49 en hombres y 6,42 en mujeres), si bien los primeros tienen un promedio ligeramente superior en CICD, N, PDP y ARSITM. En cuanto a la edad, los menores de 20 años se muestran más competentes en CICD y PDP. El perfil con un comportamiento de alto riesgo para la seguridad se observa asociado al uso de Internet permanentemente (Yan, 2009; Fernández-Montalvo, Peñalva, & Irazabal, 2015). Los resultados según las dimensiones conocimientos (6,7), actitudes (8,7) y habilidades y prácticas (6,03) muestran que tienen mejor disposición hacia la seguridad, pero menos conocimientos y prácticas relacionadas con el uso seguro y responsable de Internet.

Objetivo 3: La exploración de diferencias permite apreciar la necesidad de mejorar la competencia digital en el área de seguridad, en forma de acciones formativas, programas de prevención y educativos para el uso seguro y responsable de Internet (Chou & Peng, 2011; Fernández-Montalvo, Peñalva, & Irazabal, 2015), que permitan establecer pautas para mejorar las habilidades y comportamientos seguros y saludables a través de la red (Chou & Chou, 2016), dado que es una de las dimensiones que, cuando se evalúa la competencia digital, aún muestra notables dificultades (Napal, Peñalva-Vélez, & Mendióroz, 2018).

¿Por qué formar en seguridad? Un importante cuerpo de estudios sobre competencia digital centra sus objetivos en evaluar el área de alfabetización tecnológica o informacional, pero apenas existen estudios que aborden específicamente el área de seguridad en el ámbito universitario o en futuros docentes. En ese sentido, coincidimos con Yan (2009) y Shin (2015) en que los futuros docentes no reciben suficiente

formación en esta área y en este estudio hay resultados que muestran una mínima formación sobre cuestiones de seguridad en Internet.

Objetivo 4: Este estudio plantea que la seguridad constituye un factor determinante en la adquisición de la competencia digital. Garantizar un uso responsable y apropiado de la tecnología es compromiso de las asignaturas del área de Tecnología Educativa en la formación inicial. Aunque la seguridad digital en todos sus ámbitos se considera un desafío difícil por instituciones como la UNESCO, UNICEF u OCDE y por DigCompEdu en Europa, INTEF en España o INCoDe.2030 en Portugal, entendemos la importancia que tiene en la profesionalización de los educadores para ser digitalmente competentes, seguros y responsables (Tejada & Pozos, 2018) así como el valor de la información sobre el impacto diario de la tecnología en el consumo y el medio ambiente para la ciudadanía digital.

En esta investigación se reconocen limitaciones metodológicas, como que los futuros docentes se circunscriben a Educación Infantil y Primaria y también el carácter voluntario para cumplimentar online el cuestionario. La primera no posibilita la generalización a otros niveles educativos. En cuanto a la segunda, ese carácter influye en el propio tamaño de la muestra.

¿Qué temáticas son fundamentales para la formación del futuro profesional? Los resultados de este estudio permiten plantear las siguientes temáticas: reglas de comunicación y comportamiento en la Red (netiqueta), medidas y protocolos para prevenir riesgos en Internet y para cuidar la salud física y psicológica, conceptos relacionados con la seguridad digital (reputación, identidad, brecha, huella digital), protección de datos personales en el ámbito educativo, y protección de la seguridad en dispositivos y en creación de contraseñas. A pesar de la limitación que supone la escasez de referentes que tratan específicamente la seguridad digital, se ofrecen evidencias empíricas de la importancia que puede llegar a tener en la formación inicial. De este trabajo surge la necesidad de profundizar en la investigación sobre seguridad digital docente, así como promover e incluir en los currículos universitarios contenidos sobre seguridad como ya se hace en otras etapas educativas, en la línea del modelo PIES (Šimandl & Vanícek, 2017), del programa CIPA (Yan, 2009) o del proyecto TAIS (Chou & Peng, 2011).

Se plantean como futuras líneas de investigación: profundizar en las desigualdades curriculares existentes en planes de estudio universitarios diferentes y no solo en aquellos que forman profesorado, indagar sobre el impacto que puede tener la formación en materia de seguridad para las prácticas externas, en la formación inicial y en el ejercicio profesional, y cómo se puede enseñar y evaluar esta área competencial más allá de la mera autopercepción del futuro maestro mediante estudios interdisciplinares de educación, psicología, medicina, economía, derecho e ingeniería (áreas con una estrecha relación en subcompetencias relacionadas con el área de seguridad).

Apoyos

Estudio realizado en el Programa Estatal de Ayudas de Formación del Profesorado Universitario (FPU17/05164) del Ministerio de Educación español, y parcialmente financiado por la Universidad de Granada (Unidad Científica de Excelencia «Formación y Desarrollo Profesional del Profesorado» - Plan Propio de Investigación y Transferencia 2017) y por la Universidade de Coimbra (Faculdade de Psicologia e Ciências da Educação).

Referencias

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). E-safety: The experience of English educational establishments: Summary and recommendations. 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. UNICEF. https://uni.cf/2FUq60R
Instituto Nacional de Tecnologías Educativas y Formación del Profesorado (Ed.) (2017). Common digital competence framework for teachers. 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, 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). 18 de diciembre de 2006, sobre las competencias clave para el aprendizaje permanente. Diario Oficial L 394 de 30 de diciembre de. 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*Luxembourg: . Joint Research Centre. 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