

Intervención y evaluación con tecnologías de la competencia en seguridad digital

Norma Torres-Hernández

normath@ugr.es

Universidad de Granada, España

Teresa Pessoa

tpessoa@fpce.uc.pt

Universidad de Coimbra, Portugal

María-Jesús Gallego-Arrufat

mgallego@ugr.es

Universidad de Granada, España

Resumen

La atención a los problemas y riesgos relacionados con la seguridad digital requiere acciones educativas para reducir la incertidumbre que genera la convivencia en la sociedad digital. Este estudio tiene como propósito conocer el nivel competencial de estudiantes universitarios en el área de seguridad digital y el alcance de una intervención implementada y evaluada en entornos enriquecidos con tecnología. Participan 154 estudiantes de dos universidades de España y Portugal. La evaluación del nivel competencial en seguridad digital es una actividad previa a la intervención en la que los participantes utilizando diversas herramientas tecnológicas realizan en total 1012 actividades. Los resultados muestran que el 93.5% de participantes tienen un nivel competencial intermedio. Como parte de la intervención se analizan 148 narrativas digitales y 141 reflexiones sobre netiqueta y redes sociales. El análisis descriptivo de la evaluación de la intervención, da como resultado una valoración media del grupo de 82.13. Los futuros educadores deben ser competentes en ésta área y ser conscientes de la importancia que ésta tiene para la educación y en la sociedad. Es importante su formación para la conformación de una ciudadanía digital más segura y responsable en el uso de la tecnología y de Internet.

Palabras clave

Seguridad digital; evaluación con tecnologías; aprendizaje potenciado por tecnologías; estudiantes universitarios

Intervention and e-assessment with technologies of the competence in digital security

Norma Torres-Hernández

normath@ugr.es

University of Granada, Spain

Teresa Pessoa

tpessoa@fpce.uc.pt

University of Coimbra, Portugal

María-Jesús Gallego-Arrufat

mgallego@ugr.es

University of Granada, Spain

Abstract

Attention to Digital Security Issues and risks requires action to reduce the uncertainty generated by coexistence in the digital society. This study has as main purpose to become acquainted with the competence level of university students in digital security and the scope of an intervention implemented and evaluated in environments that are enriched with technology. 154 students from two universities in Spain and Portugal participate. The evaluation for the level of competence in digital security is an activity previous to the intervention in which the participants perform a total of 1012 activities using various technological tools. Results show that 93.5% of participants have an intermediate level of competence. As part of the intervention, 148 digital narratives and 141 afterthoughts about netiquette and social media are analyzed. The descriptive analysis of the evaluation shows the result of an average assessment of 82.13. The future educators must be competent and aware of the importance that this area has in education and in society. Training to create a safer and more responsible digital citizenship in the use of technology and the internet is fundamental.

Keywords

Digital Security; E-assessment; Technology Enhanced Learning; Higher Education

I. Introducción

El cambio cultural propiciado por el uso de las Tecnologías de Información y Comunicación y de Internet en las aulas supone transformaciones y favorece la innovación en la educación superior. También ha abierto grandes debates y nuevas expectativas en torno a la incorporación de nuevas temáticas que surgen en el marco de la Sociedad del Conocimiento.

La seguridad digital y la evaluación con tecnologías son dos temas que en los últimos años han despertado el interés de investigadores, instituciones y profesionales de la educación, por lo que su presencia en la literatura científica ha crecido notablemente.

Las Tecnologías de la Información y Comunicación (TIC) y el uso de Internet han traído importantes avances y beneficios a la sociedad, pero también es evidente que su uso implica la aparición de múltiples riesgos y problemas. Entre otros muchos, se encuentran: la exposición a contenido no deseado, el ciberbullying, el robo de contraseñas, la publicidad ofensiva o las manifestaciones de odio o racistas. En este marco, surgen diversas preocupaciones relacionadas con la privacidad y la responsabilidad en el uso de Internet y de dispositivos tecnológicos (Chou & Peng, 2011).

Resolver, atender y prevenir las situaciones problemáticas que aparecen exige formar y educar para la conformación de la ciudadanía del siglo XXI donde la competencia digital es un concepto clave. Esto la convierte también en un objetivo central para la Educación.

En materia de ciudadanía digital, los conocimientos, habilidades y actitudes críticas y responsables acerca de la seguridad electrónica o e-seguridad en el Marco para el Desarrollo y Comprensión de las Competencias Digitales en Europa (DIGCOMP) son fundamentales, por lo que todos los ciudadanos europeos deben adquirir o mejorar esta competencia. Hutson, Kelly, & Militello (2018) definen la ciudadanía digital como el uso de la tecnología de manera responsable o ser un buen ciudadano en línea. A través de ella se puede adquirir una conciencia personal acerca de las vulnerabilidades y riesgos, tanto en usuarios menos aventajados, como en aquellos más competentes.

La competencia digital es clave para el fomento del uso responsable, eficiente y democrático de las TIC para todas las personas (García-Ruiz, González, & Aguaded, 2014) y es una capacidad que los ciudadanos necesitan para su desarrollo en los ámbitos personal, académico, laboral y social que implica entre otros aspectos el uso crítico y seguro de las Tecnologías de la Sociedad de la Información para el trabajo, el tiempo libre y la comunicación (Parlamento y Consejo de la Unión Europea, 2006).

La competencia digital docente es una de las competencias instrumentales relacionada con la labor docente (Fernández, Rodríguez, & Fernández, 2016) y es indispensable para el profesorado de la llamada era digital. Se puede definir como el conjunto integrado de características personales, conocimientos, habilidades y actitudes necesarios para la actuación eficaz en diversos contextos docentes (Tigelaar, Dolmas, Wolhagen, & Dan der Vleuten (2004) que incluye diversas áreas, entre las que se encuentra la vinculada con la protección de datos personales, protección de la identidad digital, medidas de seguridad en dispositivos, y el uso seguro, responsable y sostenible de la tecnología.

Los docentes en el campo de la educación son un elemento clave en la enseñanza de la ciudadanía digital y quienes, ante la vorágine del uso del uso de las tecnologías en la enseñanza, demandan una formación para mejorar sus competencias digitales. Por ello es importante que quienes hoy se preparan para enseñar, como futuros educadores, adquieran un buen nivel de competencia digital (Cabezas & Casillas, 2017; Castellanos, Sánchez, & Calderero, 2017) ya que como señalan Chou & Peng (2011), el profesorado en activo y en formación no tiene los conocimientos suficientes sobre cómo enseñar acerca de la seguridad online. Esta carencia ha llevado a plantear la urgencia del

diseño de aprendizajes centrados en el alumnado con contenidos y criterios de evaluación en torno a este tema (Yan, 2009, Chou & Peng, 2011; Simandl & Vaníček, 2017).

Los sistemas educativos reconocen la importancia de la formación del profesorado para el dominio de las TIC y en particular sobre la seguridad, pero como afirman Cózar & Roblizo (2014), aún hay vacíos acerca de las directrices específicas sobre las capacidades básicas que se exigirán como parte de la formación inicial. Para responder a las exigencias del mundo laboral, se espera que el futuro profesorado, además de tener un buen nivel de alfabetización en el manejo instrumental de las tecnologías, sea un modelo y un guía responsable en cuanto a la navegación, uso, comunicación y colaboración a través de Internet y de las tecnologías.

Los programas de formación para la mejora de las competencias digitales del profesorado no solo deberían considerar ventajas y beneficios de las redes sociales e Internet en el aula. Deberían incidir en los riesgos y peligros potenciales a los que se pueden enfrentar sus usuarios (Keith, 2013). Permitir reflexionar y analizar sus propios hábitos de consumo en los medios para ayudarlos a utilizar Internet de manera responsable y hacerlos conscientes de las oportunidades, retos y riesgos que este recurso tecnológico tiene. Ser competente en el uso de las tecnologías y mostrar comportamientos y actitudes ante los riesgos en el mundo virtual, ayudan en la puesta en marcha de acciones preventivas y educativas para que, desde el aula, puedan garantizar la seguridad digital y ayuden a disminuir sus problemas asociados.

La necesidad de orientar la formación del profesorado hacia la parte práctica y reflexiva y utilizar diferentes métodos de formación sobre uso de las TIC, con modalidades de enseñanza enriquecidas con tecnologías y aprendizajes basados en situaciones reales del aula (Wastiau, et. al 2013) y a partir de su propia experiencia (Šimandl, Dobiáš, & Šerý, 2017; Vaclav, 2017), ayudarán a mejorar las competencias digitales a través de modelos de formación para un eficiente desarrollo profesional en el ámbito educativo (Henriquez, Moreira, Goulão, & Vieira, 2017) que en el modelo por competencias no puede prescindir de estrategias de evaluación y el uso de recursos tecnológicos para evaluar.

Para evaluar competencias, según Fernández, Rodríguez, & Fernández (2016), resulta imprescindible valorar evidencias pues es en ellas donde se encuentran los argumentos para la emisión de juicios valorativos. Es por ello que la evaluación, como elemento determinante en todo proceso formativo, se plantea como una estrategia que a partir de evidencias facilita conocer aquello que sabemos y cómo mejorarlo.

Los cambios sociales y tecnológicos actuales han enriquecido la evaluación desde el punto de vista técnico, la transformación de las formas, los escenarios, la adaptación y uso de instrumentos y técnicas acordes con el desarrollo tecnológico. Desde la pedagogía, usar las tecnologías para evaluar, además de la función formativa, propicia la autorreflexión y la participación de todos los agentes, así como la renovación de las prácticas educativas. Además garantiza la adecuación y actualización de los profesionales (Flores, Flores, & Ramos, 2017; Nogueira, Pessoa, & Gallego, 2015) ante las exigencias de una sociedad en red. Evaluar con tecnologías puede convertirse en una estrategia cultural para abrir la participación y el empoderamiento a los ciudadanos digitales.

En la evaluación de la competencia digital, herramientas como la rúbrica electrónica (Cebrián-de-la-Serna & Cebrián-Robles, 2018; Raposo-Rivas & Gallego-Arrufat, 2016), las narrativas digitales (Herreros, 2016), la participación en foros, los cuestionarios online, así como la realización de actividades, las video anotaciones y el uso de diferentes técnicas o herramientas tecnológicas (Cebrián-de-la-Serna & Cebrián-Robles, 2018) hacen posible mejorar las competencias digitales tanto del profesorado como del alumnado.

La revisión de la literatura sobre la seguridad digital (Tabla 1) plantea un interesante campo de estudio, intervención y evaluación en diferentes etapas educativas que se puede abordar interdisciplinariamente desde la psicología, el derecho o la educación.

Tópicos	Autores
Usurpación de identidad y fraude electrónico	Gabaldón & Pereira (2008)
Hábitos y comportamientos en Internet en adolescentes	Fernández, Peñalva, & Irazabal (2015)
La seguridad en competencias digitales de los <i>millennials</i>	Castillejos, Torres, & Lagunes (2016)
Comportamientos adoptados para la seguridad en línea	Dodel & Mesch, (2018)
Rutinas, conocimiento técnico y conciencias de profesores en servicio sobre la seguridad digital	Simandl & Vaníček (2017); Chou & Peng (2011)
Percepciones sobre la seguridad en Internet en estudiantes de educación secundaria y estudiantes universitarios	Zheng (2009)
Seguridad digital, daños y riesgos en niños y jóvenes	Cohen (2017)
Seguridad digital y atención parental	Tomczyk, & Wasinski (2017)
Revisión de literatura sobre seguridad y privacidad	Silva, Souza, & Rainha (s.f)

Tabla 1. Estudios sobre seguridad digital
Fuente: Elaboración propia

Por otra parte, la revisión sobre la competencia digital docente muestra que los estudios se han centrado especialmente en la alfabetización digital y en su evaluación (Tabla 2) y son escasas las investigaciones que informan sobre intervenciones llevadas a cabo para la mejora de esta competencia.

Tópicos	Autores
Evaluación de la competencia digital con instrumentos diseñados y validados ex profeso	Cózar & Roblizo (2014); Cabezas, Casillas, Ferreira, & Teixeira (2017); Castellanos, Sánchez, & Calderero (2017); Gutiérrez-Castillo, Cabero-Almenara, & Estrada-Vidal (2017); Miranda, Gisbert, Morales, & Onneto (2016); Roig & Pascual (2012); San Nicolás, Fariña, & Área (2012); Silva (2017); Silva, Cabezas, & Casillas (2017)
Evaluación de la competencia digital con instrumentos validados en otros estudios	Esteve-Mon, Gisbert-Cervera, & Lázaro-Cantabrana (2016)
Evaluación de la competencia digital utilizando el modelo TPACK	Coffman (2013); García Valcárcel & Martín (2016); Nogueira, Pessoa, & Gallego, (2015)
Evaluación de la competencia digital utilizando el modelo de alternancia académico-profesional	Lázaro & Gisbert (2015)
Estudio de la competencia digital y su relación con estrategias de aprendizaje	Díaz-García, Cebrián-Cifuentes, & Fustes-Palacios (2016); Cózar-Gutiérrez, Moya-Martínez, & Hernández-Bravo (2016)

Percepciones y niveles de apropiación de la competencia digital	Flores-Lueng & Roig (2016)
---	----------------------------

Tabla 2. Estudios sobre competencia digital de estudiantes de Educación
Fuente: Elaboración propia

II. Objetivos

Los objetivos del estudio son los siguientes: identificar el nivel de la competencia digital en el área de seguridad de estudiantes universitarios, e implementar y evaluar una intervención para la mejora de la e-seguridad.

III. Metodología

Se trata de un estudio de carácter exploratorio y descriptivo, empleando una metodología mixta para la recogida y análisis de la información.

a. Participantes

Se realiza un muestreo por conveniencia en dos universidades (en España y Portugal). Los participantes son estudiantes universitarios de titulaciones de Grado en Educación (N=154 estudiantes). Son 40 hombres y 114 mujeres, de edades comprendidas entre 18 y 29 años, con una desviación de 1.906.

En la figura 1 se muestra la distribución de los participantes en el estudio en función de su género.

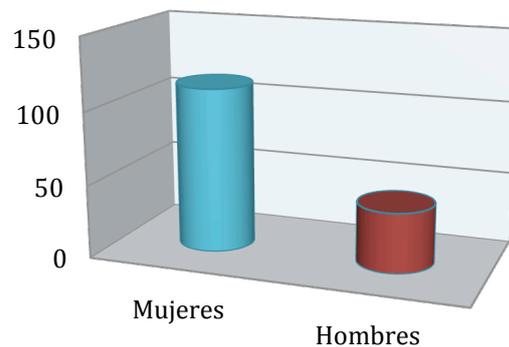


Figura 1. Participantes según género
Fuente: Elaboración propia

b. Instrumentos

Para el logro del objetivo 1, se utilizó un cuestionario online (Torres-Hernández & Pérez-Torregrosa, 2018; Gallego-Arrufat, Torres-Hernández, & Pessoa, 2019) de 59 ítems, diseñado a partir del Marco Europeo común para la Competencia Digital de los Educadores (DigCompEdu) (2017) y suministrado online a los participantes a través de la herramienta Limesurvey. Contiene las siguientes secciones: información personal, protección de datos personales, protección de la salud, compartir información y contenidos digitales, interacción mediante tecnologías, netiqueta, gestión de la identidad digital y experiencias y percepciones sobre ciberacoso.

Para el objetivo 2 se diseñó una intervención educativa bajo la modalidad de taller semipresencial "Seguridad digital y privacidad en Internet". Se planteó como una intervención diversa y enriquecida con tecnologías en cuanto a los temas, las actividades, el uso herramientas tecnológicas, el contexto, el idioma y los tiempos de realización.

c. Procedimiento

El procedimiento seguido en el estudio se muestra en la Figura 2.

La primera actividad del estudio consistió en la aplicación de un cuestionario suministrado online, diseñado ex profeso para evaluar el nivel en este área competencial. Los participantes autoevaluaron su nivel competencial en el área de seguridad digital a partir de sus opiniones, experiencias y conocimientos.



Figura 2. Proceso seguido en el estudio
Fuente: Elaboración propia

Posteriormente, de manera individual y bajo la tutoría del profesorado, los participantes realizaron el taller “Seguridad Digital y privacidad en Internet”, que bajo la modalidad de formación blended learning se alojó en las plataformas LMS de las Universidades de Granada y Coimbra, respectivamente.

Intervención educativa

La intervención educativa se llevó a cabo en un período de tiempo de tres-cinco sesiones de trabajo. Sus propósitos fueron: profundizar en conceptos relacionados con la seguridad digital en el marco de la competencia digital de la ciudadanía del siglo XXI, propiciar la mejora del nivel competencial en el área de seguridad digital mediante la realización de diversas actividades y facilitar contenidos y estrategias para la enseñanza y práctica de la enseñanza de la seguridad digital en el aula.

Los contenidos tratados fueron los siguientes:

1. La seguridad digital en el marco de la competencia digital docente
2. Problemas y tipos de riesgos vinculados a la seguridad digital
3. Netiqueta y conductas que afectan a la seguridad digital en Internet y en dispositivos tecnológicos
4. Acciones educativas y preventivas para la seguridad digital

En la intervención se realizaron actividades relacionadas con los cuatro temas estudiados (Figura 3). En ella los participantes utilizaron diferentes herramientas tecnológicas que se relacionan en la Figura 5, indicando la función para la que se emplea cada una, p.ej. herramientas de Google para trabajo colaborativo o Coannotation como soporte para las video anotaciones, entre otras.

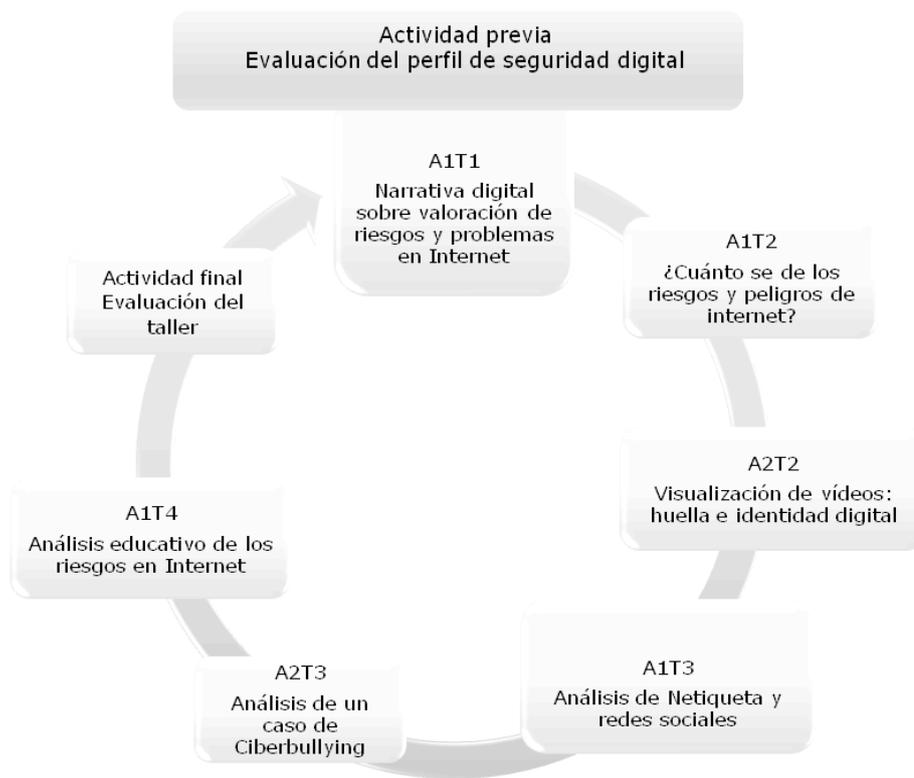


Figura 3. Conjunto de actividades realizadas durante la intervención

Fuente: Elaboración propia

Para la evaluación del taller se utilizó una e-rúbrica de evaluación (Figura 4) y un cuestionario para valorar los posibles efectos del taller en la mejora de su nivel competencial.



Figura 4. Diseño de una e-Rúbrica para la evaluación de la intervención

Fuente: sl.ugr.es/0arM



Figura 5. Uso de herramientas tecnológicas en la intervención en seguridad digital
Fuente: Elaboración propia

La evaluación mediante el cuestionario se planteó en torno a tres aspectos: valoración sobre los contenidos del taller, valoración sobre las competencias digitales docentes adquiridas en el área de seguridad digital y valoración de los futuros efectos del taller en la práctica educativa.

d. Análisis

Para el análisis de los cuestionarios iniciales (Objetivo 1), las dos actividades realizadas por los participantes (A1T1 y A1T3) y los cuestionarios de evaluación de la intervención (Objetivo 2), se utilizan los programas Excel, SPSS (Versión 23) y MAXQDA.

Se estudian las variables género, actividades y resultados (Cuestionario inicial y final).

IV. Resultados

En este estudio se presentan los resultados de 154 cuestionarios de evaluación de la competencia digital "Seguridad, privacidad e identidad digital", el análisis descriptivo de dos actividades realizadas por los participantes (148 narrativas sobre experiencias en seguridad digital y 141 reflexiones sobre netiqueta y riesgos en redes sociales) y 130 cuestionarios de evaluación cumplimentados por los participantes al finalizar la intervención.

a. Resultados del cuestionario de evaluación de la competencia digital

Para la definición de los niveles competenciales de los participantes en este estudio, era necesario tratar de conocer, a través del cuestionario aplicado, algunos conocimientos básicos, prácticas y opiniones relacionadas con el uso seguro y responsable de Internet que los participantes manifestaron antes de la intervención educativa.

Con relación a la edad en que comenzaron a ser miembros de una red social, el 48% de los participantes dijeron haber iniciado su actividad en redes sociales entre los 12 y 13 años, el 28% entre los 14 y 15 años, el 21% entre los 10 y 11 años y solo un 3% se iniciaron como miembro de una red social entre los 16 y 17 años.

Sobre el uso de herramientas tecnológicas con acceso a Internet, un 49% de los participantes dijeron utilizar entre cuatro y cinco dispositivos (teléfono, tablet, portátil, ordenador de escritorio, reloj inteligente), el 32% utiliza al menos un dispositivo, el 13% utiliza hasta seis diferentes herramientas en su vida diaria y un 6% solo usan dos o tres herramientas.

Con relación al uso de cuentas de correo electrónico (universidad donde estudian, Hotmail, Gmail y Yahoo, el 41% de participantes dijo que solo usan un correo electrónico, el 31% utiliza dos correos y el 25% de participantes usa más de tres servicios de correo electrónico para enviar y recibir información o comunicarse con otras personas.

Como usuarios de las redes sociales (Facebook, Line, Twitter, WhatsApp, Instagram, Viver, Telegram, Snapchat, Skype, Myspace), el 58% de los participantes utilizan entre tres y cinco redes sociales, siendo las más utilizadas Facebook y WhatsApp. Un 19% usan entre una y dos, un 18% es usuario de seis redes sociales y un 5% dijo participar activamente en más de 7 redes sociales.

Acerca de las personas con las que interactúan a través de redes sociales, el 83% de los participantes manifestaron conocer personalmente a la mayoría de las personas agregadas a sus redes sociales, un 12% dijeron que conocen personalmente a muy pocos amigos o contactos, mientras que el 5% conoce personalmente a todas las personas agregadas como amigos o contactos en sus redes sociales.

De acuerdo a las respuestas emitidas y los resultados obtenidos en el cuestionario en seis de las siete áreas para evaluar el nivel competencial en materia de seguridad digital, 93.5% del total de participantes poseen un nivel intermedio, 5.8% un nivel básico y 0.6% de participantes nivel alto.

Según muestra la figura 6, la distribución según género de los participantes es la siguiente: de quienes tienen un nivel intermedio, el 70.7% son mujeres y 22.7% son hombres; en el nivel básico

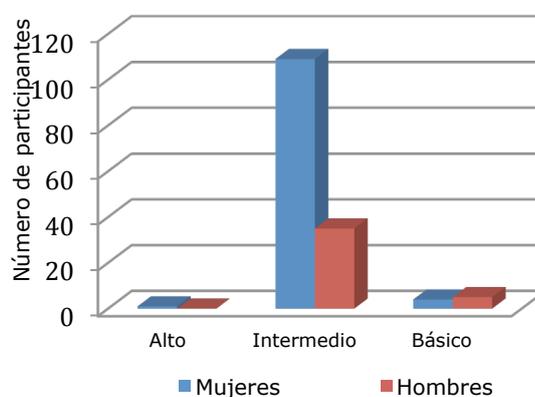


Figura 6. Nivel de competencia según género
Fuente: Elaboración propia

2.59% son mujeres y 3.2% hombres y el 0.6 corresponde a una mujer que se ubica en el nivel alto.

b. Resultados de la intervención

Se realizaron 1012 actividades individuales durante el taller (Tabla 3), lo que equivale a una media de 7 actividades por participante.

Tipo_actividad	Total de actividades	Porcentaje total de participantes
AO_Evaluación del perfil de seguridad digital	154	100%
AT1_Narrativa digital sobre valoración de riesgos en Internet	148	96%
A1T2_¿Cuánto sé de los riesgos y peligros de Internet?	135	87%
AST2_Visualización de vídeos: huella e identidad digital	154	100%
A1T3_Análisis de netiqueta y redes sociales	141	91%
A2T3_Análisis de un caso de Cyberbullying	68	44%
A1T4_Análisis educativo de riesgos en Internet	88	57%
AF_Cuestionario de evaluación	130	85%

Tabla 3. Actividades realizadas en cada uno de los temas
Fuente: Elaboración propia

c. Resultados A1T1_Narrativa digital sobre valoración de riesgos en Internet

En esta actividad los alumnos elaboraron una narrativa digital sobre alguna experiencia personal o conocida en torno a algún problema relacionado con el uso inapropiado de las redes sociales o de Internet. Fue realizada por el 96% de los participantes. Las 148 producciones digitales proyectan su vivencia personal con relación al tema de estudio.

Del análisis de contenido de las narraciones digitales se obtuvieron 997 registros agrupados en 21 categorías de análisis (Figura 7). El número de registros para cada categoría se distribuye así: IRP_identificación de riesgos y problemas (191), SC_soluciones al caso (129), PA_personas afectadas (122), UT_uso de tecnologías (106), AA_aprendizajes adquiridos (78), R_reflexiones (76), MPA_medidas preventivas adoptadas (53), PME_propuesta de medidas educativas (32), PCI_práctica de conductas inadecuadas (31), C_consecuencias (28), MC_mejora de competencias (28), OP_opiniones personales (20), SE_sentimientos experimentados (19), EE_etapa educativa (19), IPI_instituciones y personas involucradas (15), MC_modificación de conducta (12), ISTP_información sobre el caso a terceras personas (10), CM_causas o motivos que originan el riesgo o problema (10), acción pedagógica (10) EFPE_efectos futuros en la práctica educativa (7) y CN_casos de negligencia (1).

Por su importancia y su estrecha relación con la mejora de competencias digitales docentes para la prevención y educación de problemas y riesgos sobre seguridad digital, se presentan en este

estudio resultados de las categorías IRP, SC, UT, AA, PME, MC y EFPE.

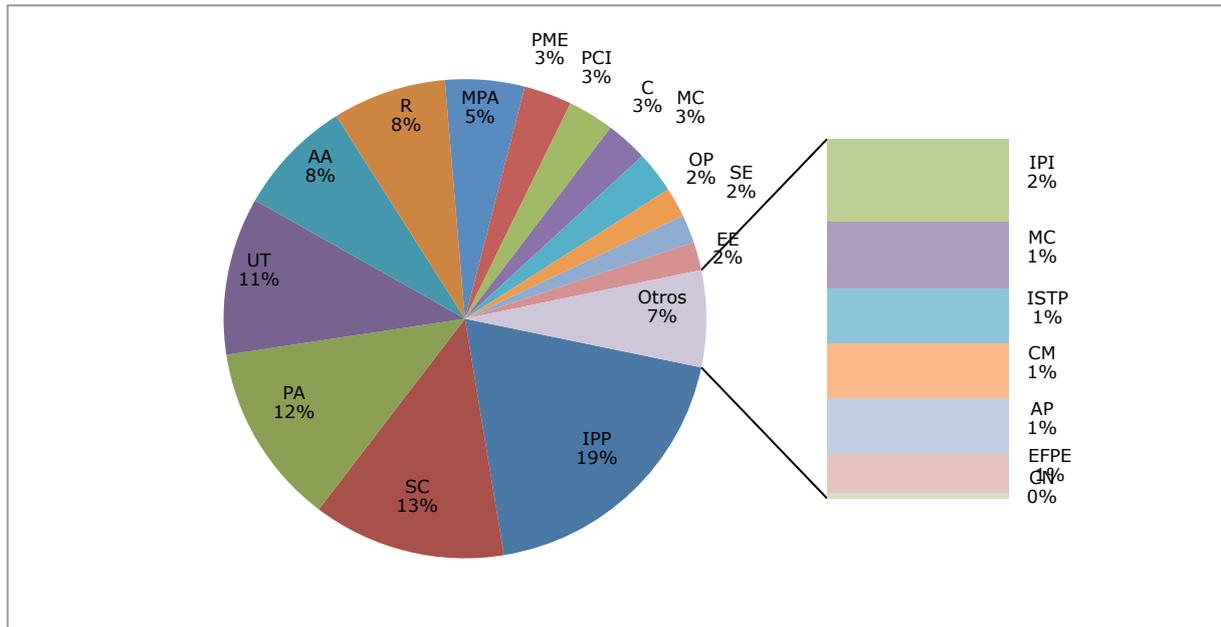


Figura 7. Distribución de registros en la narrativa digital
Fuente: Elaboración propia

En el caso de la identificación de riesgos y problemas (IRP), las situaciones más comunes que aparecen en las narraciones son: suplantación de la identidad (envío de mensajes maliciosos haciéndose pasar por la víctima), invasión a la privacidad, persecución (envío de mensajes amenazantes), denigración (difusión de rumores sobre la víctima), violación de la intimidad (difusión de secretos o imágenes de la víctima), estafas y ciberbullying.

De acuerdo con las narraciones, un 90% de los casos fueron solucionados a través de denuncias ante las autoridades civiles y educativas correspondientes, la comunicación a padres de familia o amigos, o con la intervención de los gestores de las redes sociales involucradas.

Facebook, Instagram y WhatsApp son las redes sociales en las que se presentaron la mayor parte de los problemas o riesgos narrados (UT).

Con relación a los aprendizajes adquiridos (AA) en la intervención, los participantes expresan, entre otros, los siguientes argumentos:

Esta experiencia me puede ayudar a intervenir en situaciones de riesgo o problemas relacionados con el uso inadecuado de las TIC o Internet ya que tengo más conocimientos sobre ello debido a las asignaturas que estoy dando y a los contenidos que estoy dando en ellas (15M)

Esta experiencia me ha ayudado a realizar compras por Internet de forma más segura (21M)

(..) lo que nos enseñó a todos fue, lo primero, a tener la información privada, segundo, a dejar claro que nos tenían que mencionar y pedir permiso si querían utilizar algo nuestro, y tercero, que podemos hacer mucho daño sin darnos cuenta (33M)

(..) me vino bien esa experiencia para tener más cuidado con las tecnologías, concretamente con la privacidad del usuario y de la contraseña (45H)

Creo que esta situación me sirvió para darme cuenta de la importancia que tiene proteger tus datos, y que si por casualidad pasara algo como esto es importante acudir a hablar con los profesionales (maestros, policía...) (54H)

Desde entonces cada vez que cojo una foto de Internet miro que no tenga derechos de autor y si los tiene pregunto si la puedo utilizar (70H).

Creo que con esta experiencia estoy capacitada para ayudar a la gente en el mismo caso o similar, recordando que cierren sesión en los dispositivos ajenos o directamente utilizando los suyos propios (88M)

Na minha opinião, esta experiência ajudou me a ser mais consciente e a ser mais responsável no mundo virtual e que me vai ajudar a intervir em alguma situação de risco (89M)

Com esta situação, aprendemos que não devemos deixar as nossas contas abertas em meios tecnológicos que não sejam nossos, e mesmo nestes, devemos ter o especial cuidado de terminar sempre sessão (99M)

(...) esta experiência ajudou-me bastante a intervir nestas situações e a alertar os meus colegas/amigos quando falam com desconhecidos (102M)

Seguindo este exemplo, passei a compreender que antes de começar a fazer uma encomenda online devo ter a certeza que o site é minimamente fidedigno e que a minha segurança digital está intacta (112H)

Entre las medidas educativas (PME) que los participantes consideran que se podrían plantear en la práctica educativa en casos similares a su experiencia narrada, se encuentran:

Integraría el tratamiento del tema en el aprendizaje dentro de las aulas, a través de actividades o talleres (5M)

Se debería enseñar desde que el niño utiliza Internet y dispositivos digitales para que conozca realmente todos los riesgos y problemas que tiene el uso de Internet...(9M)

Considero que (...) es fundamental intervenir de manera educativa en seguridad digital, ya que nos encontramos en una etapa donde hasta los niños chicos tienen teléfono móvil, tablet... y debemos fomentar el buen uso de las TIC para que no se vean involucrados en problemas de Internet como el grooming, suplantación de identidad, abusos...(13H)

pienso que es imprescindible educar sobre materia TIC (...). Así ellos mismos podrán evitar el quebranto de su seguridad digital y tener un perfil digital indeseado (20M)

Sobre los efectos que la experiencia puede tener en su futura práctica como educadores (EFPE), los participantes señalan entre otras cosas que:

Transmitir a mis alumnos educación en seguridad digital es de gran importancia, ya que un mal uso de los medios digitales e internet puede llevar a grandes problemas tanto para los usuarios como para terceras personas (12M)

Me puede ayudar a evitar situaciones de riesgo o a intervenir ya que al ser un problema que me ha afectado, puedo ayudar a la persona en cuanto a conocimientos sobre un uso inadecuado de Internet (25M)

Creo que sí me ayudaría a intervenir en situaciones de riesgo o problemas relacionados con el uso de las TIC o Internet (35M)

(...) Podría aconsejar y, sobre todo, poner al alcance de todos la información que yo estoy recibiendo sobre estos temas para crear una concienciación de los problemas que puede acarrear este mal uso y que no vuelvan a pasar... (38M)

Si en un futuro me tuviese que enfrentar a este tipo de problema, lo primero que haría sería explicarles a mis alumnos sobre el manejo de las redes sociales y los posibles problemas que esta red puede presentar y las consecuencias...(64H)

(..) ajudar a intervir em situações parecidas ou que tenham haver com a privacidade e proteção de dados nas tic, uma vez que a partir desse momento tornei-me muito mais atenta a essas questões, tornando-me capaz de informar outras pessoas acerca dos riscos que corremos quando não nos preocupamos o suficiente com essas definições de privacidade e proteção de dados que parecem mínimas e irrelevantes, porém se não tivermos cuidado algo de muito perigoso pode nos vir a acontecer (9M)

d. Resultados A1T3_Análisis de netiqueta y redes sociales

El propósito de esta actividad fue que los participantes reflexionaran acerca de sus comportamientos cuando utilizan las redes sociales e Internet y crear conciencia de la importancia que tiene respetar las normas de netiqueta tanto en la comunicación con una sola persona como con su grupo de amigos. Con las respuestas a una serie de preguntas definieron su perfil en este aspecto relacionado con el uso responsable de las redes sociales.

(P1): Cuándo te comunicas a través de correo o de las redes sociales, ¿respetas las reglas de comunicación? El 88% del total de participantes, respondió afirmativamente, mientras que el 12 % reconoció no respetar las reglas de netiqueta.

(P2): ¿Tus amigos o contactos respetan reglas de comunicación y comportamiento? El 82% manifestó que los amigos y contactos sí respetan las reglas de netiqueta, el 11% algunas veces y 8%. Fue respondida por 65 participantes.

(P3): A la cuestión: tus contactos o miembros de grupos en redes sociales ¿han propuesto alguna norma para su uso? El 53% respondió que no mientras que el 47% señaló que sí se han establecido algunas normas de comportamiento.

(P4): Escribe 5 situaciones en las que consideres que no se ha respetado la netiqueta en la comunicación establecida. Para ello, los participantes revisaron los mensajes de la última hora de una red social en la que son miembros activos. Los casos más comunes descritos son los siguientes:

- *Colapso de mensajes (1H)*
- *Enviar mensajes en cadenas (5M,9M, 28H, 36M, 42H, 56M,59M, 64M, 69H, 75M)*
- *Escribir enfadado con alguien (2H)*
- *Envío de mensajes en horas no apropiadas (madrugada, vacaciones, etc.) (6M, 8M, 9M)*
- *Hacer comentarios de personas que no son miembros del grupo (4M, 9H, 13H, 26H, 35H)*
- *Pasar fotografías, imágenes o vídeos sin consentimiento de quienes allí aparecen (7M, 8M, 9H, 12M, 16M, 20M, 26H, 44M, 50M, 57M, 58M, 60H, 107M, 117M)*
- *Reenviar fake news (17H, 24H, 39M, 50M, 53M)*
- *Dejar en evidencia a algún miembro del grupo (20M)*
- *Leer mensajes en móvil de otra persona sin su consentimiento (16M)*
- *Escribir con mayúsculas (1H, 3H, 5M,10M, 13M, 14M, 15M, 21M, 23M, 28H,36M, 39M, 47M, 48M, 54M, 64M, 66H, 77H, 88M)*
- *Faltas de ortografía (13H, 20M, 21M, 32M, 44M, 47M, 52H, 57M, 58M, 59M, 60H, 63M, 67H, 68H, 70H, 75M, 77H)*
- *Compartir ideales políticos (21M, 53M)*
- *Enviar contenidos inapropiados (17H, 20M, 22M)*
- *Poner nuestros perfiles de forma pública sin tener en cuenta que cualquier persona puede tener información sobre nosotros, y multitud de ejemplos parecidos (12M)*
- *Se creó un grupo de trabajo sin acuerdo previo con los demás integrantes de dicho grupo (15M, 31M, 33M, 35H)*
- *Faltar al respeto (32M, 38M, 46H, 50M, 55M, 57M)*
- *No respetar el tiempo de los demás (49H)*
- *El último mensaje recibido en uno de los grupos de mi Whatsapp: una amiga expone el lugar donde se encuentra y otra manda una imagen de que ha sacado un billete de bus para visitarnos en unas semanas. En ella se pueden observar distintos datos personales (nombre completo, DNI, número de teléfono, correo electrónico, código de billete). Ambos casos, aunque no lo percibamos, corren mucho riesgo (18M)*
- *Se han utilizado acrónimos y abreviación de palabras (6M,10M, 13M, 18M, 19M,28M, 36M,*
- *Utilizan el sarcasmo y humor (19M, 23M, 24M, 36M, 54M)*
- *Insultar a alguien en el grupo (8M, 25H,35H,36M, 44M, 53M, 54M)*

e. Resultados de la evaluación de la intervención por los participantes

e.1. Valoración general

La intervención es valorada por el 84 % del total de participantes. De ellos, 75% son mujeres y 25% hombres.

De acuerdo a los datos del análisis descriptivo, los resultados muestran una valoración media de 82.13 por parte del conjunto de participantes.

Al analizar los valores medios considerando la variable género, las mujeres otorgan una valoración media de la intervención de 82.24 mientras que la valoración media de los hombres es de 84.34.

e.2. Aspectos evaluados en el cuestionario final

La evaluación realizada en cada uno de los tres apartados muestra que el apartado de valoración sobre los contenidos del taller obtiene una valoración media de 85.69, sobre los otros aspectos evaluados. La valoración sobre la mejora de competencias digitales docentes en el área de seguridad digital y la valoración de futuros efectos del taller en la práctica educativa obtienen una media de 81.69 y 79 respectivamente.

El análisis de cada uno de los tres aspectos evaluados considerando el género de los participantes muestra, de acuerdo a la tabla 4, que las mujeres perciben una mejora de su competencia digital en el área de seguridad, otorgando una mejor valoración en este apartado (81.64) que el de los hombres, que fue de 78.13. Asimismo, valoran con 80.81 la experiencia de la intervención como una acción con posibles efectos positivos en su práctica educativa. En el caso de los hombres a este apartado le otorgan un 71.05.

Los contenidos del taller		Mejora de competencias digitales docentes en área de seguridad digital		Futuros efectos del taller en práctica educativa	
M	H	M	H	M	H
85.27	86.96	78.13	81.64	80.81	71.05

Tabla 4. Valoraciones medias de los tres aspectos evaluados
Fuente: Elaboración propia

La valoración media sobre los contenidos del taller es similar independientemente del género de los participantes (86.96 hombres y 85.27 mujeres). Incluyen afirmaciones como:

- He aprendido mucho sobre temas que no sabía, de conceptos que es necesario conocer*
- Me resulta muy interesante para nuestro futuro trabajo (AM46)*
- Me resulta muy interesante saber sobre los riesgos que existen, ya que en muchos casos no somos conscientes (AH99)*
- Me parece que el conocimiento de todos los contenidos que tienen que ver con la seguridad tecnológica es muy importante y necesario ya que son una herramienta que todos utilizamos y no todos tenemos los suficientes conocimientos (AM135)*
- El haber experimentado estos contenidos de forma dinámica creando herramientas y reflexionando sobre ellas ha hecho que esto no sea una información memorística sino que la he integrado, y solo así seré capaz de transmitirla (AM27)*
- El tema de riesgos y problemas de Internet es bastante relevante (AH127)*
- (...) están presentes en nuestro día a día por lo que las normas no escritas también debemos de conocerlas y respetarlas para evitar riesgos, porque la seguridad es muy importante (AM4)*

e.3. Valoración de los contenidos

Con relación a los contenidos tratados en la intervención, la valoración que se hace por parte de todos los participantes (Tabla 5) indica que el tema 2 obtuvo una mejor valoración con respecto a los temas 1, 3 y 4.

Nº tema	Temas	Valoración de los participantes
T1	La seguridad digital en el marco de la Competencia Digital Docente	84
T2	Problemas y tipos de riesgos vinculados a la seguridad digital	86.5
T3	Netiqueta y conductas que afectan a la seguridad digital en Internet y en dispositivos tecnológicos	83
T4	Acciones educativas y preventivas para la seguridad digital	83

Tabla 5. Media de las valoraciones según temas
Fuente: Elaboración propia

Los resultados de la evaluación sobre la mejora de las competencias digitales en el área de seguridad se complementan con afirmaciones como las siguientes:

Si yo no adquiero pautas y hábitos para tener una navegación segura de forma personal, no podré transmitirlos a aquellos sobre los que ejerza función de pedagogo (AM76)

No somos conscientes de los riesgos a los que nos presentamos y hemos de serlo para poder navegar de forma segura (AM18)

Es muy importante tener los suficientes conocimientos sobre el tema para poder aplicarlos y enseñarlos (AH151)

Sobre los futuros efectos de la intervención en la práctica educativa afirman:

He conocido muchos recursos y estrategias a lo largo de la realización de estas tareas (AM25)

Contamos con una serie de recursos que podremos utilizar en nuestra trayectoria como pedagogos, pero también en nuestros proyectos personales (AM79)

He identificado necesidades para prevenir en un futuro como profesional y para mejorar los problemas que observe (AM65)

Las personas ignoran el riesgo que supone navegar por Internet o tener la misma contraseña en todas las cuentas de usuario. Se requiere una educación en conciencia con respecto al tema (AM54)

V. Discusión y conclusiones

Promover las competencias digitales, y en particular la seguridad digital con fines formativos, se plantea como una necesidad actual de la educación del profesorado (Šimandl & Vaníček, 2017). Ofrecer experiencias alternativas de aprendizaje, aprovechar la potencialidad de las tecnologías de la información y la comunicación y diseñar actividades en las que los estudiantes aprendan a partir de su propia experiencia personal (Šimandl, Dobiáš, & Šerý, 2017), es facilitar el desarrollo académico para consolidar las competencias de los futuros educadores y contribuir así a la conformación de una ciudadanía digital más competente, crítica y responsable en el uso de Internet y de las tecnologías.

En este aspecto, coincidimos con Yan (2009) y Chou & Peng (2011) en que proporcionar programas de seguridad digital podría mejorar el nivel de conciencia de los estudiantes universitarios, mejorar actitudes, comportamientos, conocimientos y emociones y en la necesidad de la integración curricular o acciones formativas que integren la e-seguridad como contenido en el aprendizaje. Para mejorar la seguridad digital en las etapas educativas de primaria y secundaria, es fundamental mejorar también la formación inicial (Woollard et al, 2009)

En este estudio hemos presentado una intervención educativa sobre la seguridad digital en la que se ha utilizado la evaluación con tecnologías como una estrategia para conocer el perfil competencial de los participantes -futuros educadores- y sus valoraciones sobre dicha acción formativa cuyo diseño y desarrollo se presenta también en este trabajo.

Respecto al objetivo 1, podemos concluir que el cuestionario aplicado ha permitido, a través de la evaluación con tecnologías, conocer los niveles competenciales de los futuros educadores de España y Portugal en un área que, hasta hace poco, escasos estudios han analizado y evaluado, pero, además, ha propiciado la sensibilización de los participantes acerca de sus propias prácticas y conocimientos en torno a la seguridad digital. La ubicación del 93.5% de los participantes en un nivel intermedio puede suponer para la educación la garantía de contar en un futuro con docentes que han adquirido conocimientos, actitudes y habilidades necesarias para atender y resolver situaciones en el aula relacionadas con la seguridad digital.

Con relación al objetivo 2, la intervención ha sido implementada y evaluada. La intervención sobre seguridad digital y riesgos en Internet tuvo como propósito acercar a los participantes al conocimiento de un tema no integrado curricularmente en la formación universitaria pero que no es ajeno a las experiencias de los estudiantes universitarios y en el que como educadores del mañana necesitan formación.

En ese sentido se ha diseñado, coherente desde nuestro punto de vista, con las necesidades planteadas sobre la formación inicial sobre seguridad digital. Es una propuesta de formación inicial emergente de la práctica educativa y de una necesidad social en la que se realizan las actividades propuestas y se emplean diversidad de recursos tecnológicos (Cebrián-de-la-Serna & Cebrián-Robles, 2018). Ha buscado movilizar conocimientos, experiencias y reflexiones de los propios participantes (Flores, Flores, & Ramos, 2017) ya que estamos de acuerdo en que las experiencias narradas que el profesor tiene pueden ayudarle a mejorar su comportamiento y su aprendizaje (Šimandl & Vaníček, 2017). Hemos incorporado una diversidad de herramientas tecnológicas durante la intervención pues creemos, como señalan Nogueira, Pessoa, & Gallego (2015) y Flores, Flores, & Ramos (2017), entre otros, que estas son una oportunidad para la transformación de la práctica pedagógica y de la educación, tanto para quien enseña como para quien aprende.

En la evaluación de la intervención, hemos comprobado que la experiencia educativa -aún con sus propias limitaciones- ha sido bien valorada por parte de los participantes, con relación a los temas tratados y a las actividades así como a los efectos que la acción formativa traerá consigo para la práctica educativa en el futuro.

Con este estudio hemos querido contribuir a enriquecer el campo de investigación en seguridad digital, iniciado en diferentes contextos educativos y en los que se trata sobre la formación, el consumo mediático y las competencias digitales y su relación con la e-seguridad (Castillejos, Torres, & Lagunes, 2016; Chou & Peng, 2011; Šimandl Dobiáš, & Šerý, 2017; Simandl & Vaníček, 2017; Yan, 2009; Vaclav, 2017; Woollard, Powell, & Russell, 2009).

Futuros estudios

Toda investigación plantea expectativas y nuevos retos. En ese sentido, creemos que se hace necesario enriquecer la investigación sobre el uso de la tecnología para mejorar las competencias digitales en educación inicial en el área de seguridad, indagar cuáles son los mejores métodos de

aprendizaje y enseñanza de contenidos relacionados con la seguridad digital y cómo éstos pueden mejorar las habilidades y actitudes de las nuevas generaciones. Se plantea además la importancia de construir instrumentos para evaluar la seguridad digital en diferentes niveles educativos.

Agradecimiento

Este estudio se ha realizado gracias a la financiación del Ministerio de Educación y Formación profesional a través del Programa Estatal de ayudas Contratos predoctorales de Formación del Profesorado Universitario (FPU17/05164).

Referencias

- Cabezas, M., Casillas, S., Ferreira, M., & Teixeira, F. (2017). Validación de un instrumento para medir la competencia digital de estudiantes universitarios (CODIEU). *Revista de estudios e investigación en Psicología y Educación*, 13. doi: 10.17979/reipe.2017.0.13.2180
- Castellanos, A., Sánchez, M., & Calderero, J. (2017). Nuevos modelos tecnopedagógicos. Competencia Digital de los alumnos universitarios. *Revista Electrónica de Investigación Educativa*, 19 (1), 1-9. doi: 10.24320/redie.2017.19.1.1148
- Castillejos, B., Torres, C., & Lagunes, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura*, 8 (2), 54-69.
- Cebrián-de-la-Serna, M., & Cebrián-Robles, D. (2018). Evaluación de los e-aprendizajes con el PLE-portafolios: Anotaciones multimedia y las rúbricas. Colección Gtea: Universidad de Málaga. ISBN 978-84-697-9425-8.
- Chou, Ch., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *Internet and Higher Education*, 14, 44-53. doi: 0.1016/j.iheduc.2010.03.006
- Cózar, R., & Roblizo, M. (2014). La competencia digital en la formación de futuros maestros: percepciones de los alumnos de los Grados de Maestro de la Facultad de Educación de Albacete. *Revista Latinoamericana de Tecnología Educativa*, 13 (2), 119-133. doi: 10.17398/1695288X.13.2.119
- Fernández, M., Rodríguez, J. & Fernández, F. (2016) Evaluación de competencias docentes del profesorado para la detección de necesidades formativas. *Bordón* 68, (2), 85-99.
- Flores, P. Q., Flores, A., & Ramos, A. (2017). *What teachers do, observe, and feel in pedagogical practice through the use of digital resources*. Proceedings of EDULEARN17 Conference 3rd-5th July 2017, Barcelona, Spain. Retrieved from <https://core.ac.uk/download/pdf/154272993.pdf>
- Ferrari, A. (2013). *DIGCOMP a framework for developing and understanding digital competence in Europe*. Luxembourg: Publications Office. Recuperado de: <http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=6359>
- Gallego-Arrufat, M.J.; Torres-Hernández, N.; & Pessoa, T. (2019). Competencia de futuros docentes en el área de seguridad digital. *Comunicar*, 61(4). doi:10.3916/C61-2019-xx
- García-Ruiz, R, González, V. & Aguaded, J. (2014). La competencia mediática como reto para la educomunicación; Instrumentos de evaluación. *Cuadernos.info*, 35, 15-27, doi: 10.7764/cdi.35.623
- Henriques, S., Moreira, J.A., Barros, D., & Goulão, M.F. (2017). Respondendo aos desafios formativos da era digital: o curso de formação para a docência no ensino superior online. Em Paulo Dias, Darlinda Moreira e António Quintas-Mendes (Coord.). *Novos olhares para os cenários e práticas da educação digital*. Educação a Distância e eLearning, N.º 2. UAb. pp. 148-178.
- Herreros, M. (2016). El uso educativo de los relatos digitales personales como herramienta para pensar en el yo (Self). *Digital Educational Review*, 22, 68-79.
- Hutson, E., Kelly, S., & Militello, L. (2018). Systematic Review of Cyberbullying Interventions for youth and Parents With Implications for Evidence-Based Practice. *Worldviews on Evidence Based Nursing*, 15, (1), 72-79.
- INTEF (2017). *Common Digital Competence Framework for Teachers*. Recuperado de: <http://educalab.es/documents/10180/12809/MarcoComunCompeDigiDoceV2.pdf>

- JRC (2017). *Digital Competence Framework for Educators (DigCompEdu)*. Recuperado de: <https://ec.europa.eu/jrc/en/digcompedu>
- Keith, H. (2013). Using Facebook and other SNSn in K12 classrooms: ethical considerations for safe social networking. *Issues in Teacher Education*, 22 (2), 39-54.
- Nogueira, F., Pessoa, T., & Gallego, M.J. (2015). Desafios e oportunidades do uso da tecnologia para a formação continua de professores: uma revisão em torno do tpack em Portugal, Brasil e Espanha. *TEAR: Revista de Educação, Ciência e Tecnologia*, 4 (2), 1-20. Recuperado de <https://periodicos.ifrs.edu.br/index.php/tear/article/view/1950>
- Raposo-Rivas, M., & Gallego_Arrufat, M. J. (2016). University Students' Perception of Electronic Rubric-Based Assessment. *Digital Educational Review*, 30, 220-233.
- Recomendación 2006/962/CE del Parlamento Europeo y del Consejo, de 18 de diciembre de 2006, sobre las competencias clave para el aprendizaje permanente, Diario Oficial L 394 de 30 de diciembre de 2006
- Šimandl, V., Dobiáš, V., & Šerý, M. (2017). The Influence of Teaching Methods on Learners' Perception of E-safety. *Journal of Information Technology Education: Innovations in Practice*, 16 (1), 253-275. Retrieved from <http://www.informingscience.org/Publications/387>.
- Šimandl, V., & Vanicek, J. (2017). Influences on ICT teachers knowledge and routines in a technical e-safety context. *Telematics and Informatics*, 34, 1488-1502. doi:10.1016/j.tele.2017.06.012
- Tigelaar, D., Dolmas, D., Wolhagen, I., & Dan der Vleuten, N. (2004). The development and validation of a framework for teaching competencies in higher education. *Higher Education*, 48, 253-268.
- Torres-Hernández, N., & Pérez-Torregrosa, A. (2018). *Comunicación y seguridad digital de los futuros docentes: Desarrollo de instrumentos de análisis*. XXI Congreso Internacional EDUTEC. Educación con tecnología: un compromiso social. Lleida, 24 y 25 de Octubre.
- UNESCO (2016). *Competencias y estándares TIC desde la dimensión pedagógica: Una perspectiva desde los niveles de la apropiación de las TIC en la práctica educativa docente*. Cali: Pontificia Universidad Javeriana.
- Vaclav Dobias, M. (2017). The Influence of Teaching Methods on Learners' Perception of E-safety. *Journal of Information Technology Education: Innovations in Practice*, 16 (1), 253-275.
- Wastiau, P., Blamire, R., Kearney, C., Quittre, V., Van de Gaer, E., & Monseur, C. (2013). The use of ICT in Education: a survey of schools in Europe. *European Journal of Education*, 48 (1), 11-27. doi: 10.1111/ejed.12020
- 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. doi: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, 209-217.