Formación Universitaria
Vol. 14(1), 33-44 (2021)
http://dx.doi.org/10.4067/S0718-50062021000100033

Uso crítico y seguro de tecnologías digitales de profesores universitarios

Erika P. Alvarez-Flores
Unidad Académica Hermosillo, Universidad Estatal de Sonora, Ley Federal del Trabajo S/N, México.
(correo-e: ericka.alvarez@ues.mx)

Recibido Abr. 29, 2020; Aceptado Jun. 24, 2020; Versión final Jul. 29, 2020, Publicado Feb. 2021

Resumen

El objetivo de esta investigación es detectar requerimientos de formación para prácticas de navegación segura en Internet de profesores universitarios. Se aporta una visión sobre patrones de comportamiento, capacitación y nivel de competencia enfocados en el uso crítico y seguro del Internet. La investigación es exploratoria y utiliza un instrumento basado en el marco digital DigComp. La muestra está compuesta por 338 docentes de 39 universidades de nueve países hispanos. Se realizó un análisis estadístico descriptivo e inferencial. Los resultados revelan que las universidades están capacitando a los profesores en competencias digitales, pero con escasa formación en seguridad. Hay una tendencia en los profesores a involucrarse en experiencias con consecuencias negativas, pero existen mejoras significativas del nivel de competencia y hábitos seguros en función de la capacitación. Se concluye que hay evidencia de la necesidad de una formación que refuerce el uso responsable de las tecnologías impidiendo riesgos y peligros.

*Palabras clave***:** *competencia digital docente; conductas de riesgo; tecnología digital*

Critical and safe use of digital technologies by university professors

Abstract

The main objective of this research study is to identify training measures needed to achieve safe online navigation practices by university professors. The present study provides a view of Internet behavior profiles, training, and proficiency levels focused on Internet safe use. The research is exploratory and uses an instrument developed using the DigComp digital framework. The sample consists of 338 professors at 39 universities from nine Hispanic countries. A descriptive and inferential statistical analysis was performed. The results show that university institutions train professors on digital skills, but there is a lack of training on Internet security. There is a tendency for professors to have negative online experiences. However, there is a significant improvement in the level of proficiency and safe habits in terms of training. It is concluded that there is a need for digital training of university professors that reinforces responsible use of technologies to prevent risky behaviors.

Keywords: digital teacher competence; risk behavior; digital technology

INTRODUCCIÓN

La incorporación de las tecnologías en todos los ámbitos ha hecho necesario que los usuarios adquieran competencias para su tratamiento, puesto que de forma paralela a los beneficios que aportan los avances tecnológicos se presentan prácticas de riesgo, peligro, moralidad, identidad y más (Gamito et al., 2017). Autores como Shillair et al. (2015) argumentan que muchas personas aún no siguen precauciones básicas de seguridad a pesar de frecuentes informes de pérdidas causadas por problemas de seguridad informática y enfrentan amenazas graves y generalizadas. Las ventajas que proporciona internet ante su naturaleza interactiva, su facilidad de acceso, comodidad de uso e inmediatez pueden transformarse en desventajas al plantear a los individuos posibles efectos negativos al entrañar diversas amenazas consecuencia del uso inadecuado o sin control. Las redes pueden ser vía para robo de identidad, desinformación, fraude y estafas por admitir material inapropiado, acoso cibernético, explotación, invasión de la privacidad personal, entrar en contacto con lenguaje dañino y crear hábitos de adicción a su uso. Así mismo, involucrar al individuo en cuestiones de infracción de derechos de autor, plagio y violaciones de seguridad.

Ante el despliegue digital, la Comisión Europea precisó competencias clave que toda persona debe tener para realización y desarrollo personal, para la ciudadanía activa, la inclusión social y el empleo (Ferrari, 2013) entre las que se encuentra la Competencia Digital que entraña como imperante la gestión de identidad digital, el uso seguro y crítico de las tecnologías de la información y protección de datos personales. Los procesos de enseñanza y aprendizaje han evolucionado estrechamente ligados al desarrollo de las tecnologías. Por lo que la competencia digital toma relevancia para el quehacer académico, no solo para el ámbito personal, al asumir muchos de los docentes el papel de diseñador de experiencias de aprendizaje digital, y donde el alumno controla por sí mismo su acceso a la información en la web.

Los peligros en la web como el ciberacoso o ciberagresión son fenómenos cada vez más preocupantes que afectan y desafían a todos los grupos demográficos (Chatzakou et al., 2019). Puede pensarse que el adulto no requiere pautas de protección, pero se ha observado que ocurre más acoso cibernético en adultos que en niños (Kowalski et al., 2018). Otras investigaciones (Baruh et al., 2017) indican que los adultos son susceptibles al fraude cibernético al ceder a la solicitud ilegal de claves mediante sitios web o correos electrónicos. Para aminorar los peligros en la red, se han explorado y analizado aspectos como estrategias de gestión de privacidad individual y grupal en redes sociales (De Wolf et al., 2014; Dourish y Anderson, 2006), seguridad en banca en línea (Jansen y van Schaik, 2018), características del comportamiento abusivo en internet (Chatzakou et al., 2019), elementos que guíen a los educadores a identificar, gestionar y prevenir el ciberacoso (Redmond et al., 2018), efectos psicológicos del uso excesivo de herramientas de redes (Mingming y Xiaotian, 2019), entre otros, que proporcionen conciencia y confianza en el intento de promover una vida segura y saludable en línea.

Para educar a las generaciones del siglo XXI no basta que el profesorado universitario emplee las tecnologías para el ejercicio de su profesión en el aula, la habilidad tecnológica juega un papel relevante en la garantía de una educación de calidad (Amor y Serrano, 2019). Como agente de cambio y como profesional debe asumir el papel de líder que favorezca su incorporación y abarcar otras posibilidades de interacción con y para otros (estudiantes, compañeros, instituciones, comunidad) para su acción en la docencia, la investigación y la gestión. Sin embargo, muchos profesores no están adecuadamente preparados para alcanzar altos niveles de presencia social, cognitiva y docente en entornos de aprendizaje en línea (Blayone et al., 2018). Si desea liderar procesos de innovación le conlleva una formación, dedicación y uso eficaz de las tecnologías digitales (Prendes et al., 2018), acorde con sus responsabilidades del ejercicio profesional y las relaciones socioculturales, responsabilidades que están interrelacionadas entre sí. El docente competente en un mundo mediado por la tecnología requiere estar consciente de la vulnerabilidad digital, del empoderamiento crítico y de desarrollar su capacidad técnica guiada por el buen juicio para mitigar el impacto negativo (Redmond et al., 2018) y ser responsable de sus interacciones en Internet que podrían ser perjudiciales para su seguridad o bienestar físico, psicológico y social.

El presente trabajo surge con el propósito de aportar una visión sobre las prácticas del uso de Internet, capacitación y el estado de competencias que detecten un riesgo para el profesorado; indicadores que ubiquen si es necesario abordar acciones y sirvan de base para aplicar medidas específicas de formación consecuente por parte de las administraciones educativas y por los docentes mismos. La investigación se focaliza en explorar y medir concepciones, percepciones, prácticas y sentimientos docentes basada en marcos digitales internacionales; información que facilite percibir y clarificar qué tipo de aprendizajes tecnológicos no se ha adquirido (Escudero et al., 2018). Se pretende contribuir, a través del análisis específico del uso crítico y seguro de tecnologías digitales y de la competencia digital asociada a este ámbito, a orientar hacia un itinerario de diseño de capacitación coherente que refuerce y redunde de forma eficaz en una de las áreas de la profesionalización docente. Esto de cara a procesos de mejora de la calidad de la docencia y que, a la vez, se facilite a través de los docentes esta competencia digital en los estudiantes.

Al ser el profesorado un factor clave en la calidad educativa, el estudio de la competencia digital docente alcanza un impacto creciente en la investigación científica abarcando aspectos relacionados con su compromiso como profesor y como ciudadano en un entorno profesional digital, proponiéndose modelos y marcos institucionales internacionales que consideran una dimensión social, ética y/o ciudadana, entre ellos: el Marco Europeo para la Competencia Digital Docente DigCompEdu (European Commission, 2017), el National Educational Technology Standards for Teachers NETS-T (ISTE, 2018), el Marco Común de Competencia Digital Docente del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF, 2017), el DigiLit (Fraser et al., 2013) y el Marco de competencias TIC para docentes ENLACES (Ministerio de Educación de Chile, 2010). Otro punto de referencia que comprende el uso de tecnologías en el desempeño profesional docente universitario es el Technological Pedagogical Content Knowledge (Mishra y Koehler, 2006) que instaura imprescindible domine competencias tecnológicas junto al conocimiento disciplinar y pedagógico.

Modelos reformulados recientemente como el de Tejada y Pozos (2018) hacen énfasis en que se deben poseer competencias profesionales conectadas con la dimensión social, ética y ecológica para asumir los retos de la sociedad del conocimiento. Por otra parte, Instefjord y Munthe (2017) destacan que la eficacia del docente en las aulas digitales se correlaciona positivamente con su formación digital. Propuestas que nos hacen reflexionar que el docente podrá formar ciudadanos digitales críticos, reflexivos y comprometidos si está capacitado para ofrecer al estudiante experiencias positivas de relación humana y social. Debemos por lo tanto concebir el perfil docente en un proceso de aprendizaje recurrente y continuo (Tejada y Pozos, 2018) que fortalezca las competencias profesionales necesarias para hacer frente a los retos del entorno.

La Comisión Europea ha considerado esencial la formación de los docentes (2017) y remarca que al igual que los estudiantes, los profesores deben participar en la alfabetización digital como parte de su desarrollo profesional continuo para enfrentar las necesidades de la sociedad. Las instituciones educativas han contribuido para configurar programas de formación docente en pro de la adquisición de competencias digitales, pero dotar a los profesionales académicos con elementos para desarrollar la competencia digital en todas las dimensiones en un reto que representa atender diversos puntos (Gisbert et al., 2016). Con frecuencia, en este tipo de formación se tiende a dar énfasis a las competencias instrumentales y/o metodológicas para usar e integrar recursos tecnológicos en el desarrollo de experiencias de aprendizaje. Sin embargo, es fundamental para impulsar la labor docente no ignorar otras dimensiones transversales como las relativas a actitudes y valores ante el uso responsable de tecnologías si se desea coincidir con la realidad del entorno del profesorado. Prendes et al. (2018) indican que las acciones formativas de competencia digital casi siempre se quedan en la capacitación técnica; en ocasiones trabajan el uso de herramientas para gestión de información y comunicación; menos veces capacitan en el uso educativo y metodologías docentes y denotan que casi nunca se abordan niveles analíticos y éticos. Desplegándose una brecha de formación docente en el uso responsable y ético de tecnologías.

Determinar acciones pertinentes para una formación docente digital, supone contextualizar, verificar y reflexionar dentro de un proceso de investigación en todas sus dimensiones para determinar exactamente qué debe abordarse y con ello mejorarla. En este caso en particular, nos enfocamos en un elemento digital poco abordado en las capacitaciones de las instituciones educativas, el uso crítico y seguro de Internet de cara a que comprendan sus responsabilidades y riesgos como ciudadanos digitales pese a encontrase en un entorno tecnológico social y académico seguro. Y con ello, tomen medidas que aseguren su bienestar físico, psicológico y social cuando utilicen tecnologías digitales.

METODOLOGÍA

El enfoque de investigación se enmarcó en un análisis exploratorio de carácter fundamentalmente cuantitativo y alcance descriptivo e inferencial basado en el diseño y aplicación de un instrumento ad hoc para abordar el diagnóstico del uso crítico y seguro en Internet que realizan profesores universitarios, así como capacitación y nivel competencial que tienen en ello. Por su carácter exploratorio pretende revelar información útil que facilite diseñar capacitación coherente que fortalezca el conocimiento sobre este punto de actuación.

Muestra

La población objeto de estudio fue compuesta por profesores universitarios de instituciones hispanas. Ante la imposibilidad de contar con acceso a todos ellos, se trabajó con una muestra no probabilística de oportunidad, sujetos accesibles a participar en la investigación tras cuatro semanas en las que estuvo abierto el instrumento en la red durante junio y julio del 2018. La muestra la componen 338 docentes de 9 países: Argentina, Chile, Colombia, Ecuador, El Salvador, España, México, Perú y Venezuela. Todos ellos participaron de manera anónima y espontánea. Para reflexionar bajo contextos diversos y evitar sesgos institucionales de formación,

la invitación a participar se realizó por medio de correos electrónicos de contacto con docentes pertenecientes a una red de colaboración de investigación. Se envió a los investigadores el enlace al instrumento para su realización en línea, quienes a su vez contactaron con profesores de sus respectivas universidades de manera aleatoria. De forma que quienes respondieron lo hicieron voluntariamente. La Tabla 1 proporciona información en función al país y representada bajo tres áreas de conocimiento. Presentándose una mayor proporción de universidades públicas y del área de Ciencias Sociales y Jurídicas. En el caso de las universidades privadas fueron: 3 universidades de México, 2 de España y 1 de Argentina.

Tabla 1: Participantes en función al país de la universidad de adscripción y por área de conocimiento

País	*Universidades de adscripción*	*Área de conocimiento*			*Total Profesores*
		Arte y Humanidades	*Ciencias Sociales y Jurídicas*	*Ciencias Exactas, Salud e Ingenierías*	
Argentina	7	21	15	8	44
Chile	6	0	6	19	25
Colombia	2	7	13	0	20
Ecuador	1	4	7	1	12
El Salvador	1	6	15	0	21
España	6	16	33	15	64
México	14	39	36	56	131
Perú	1	0	6	7	13
Venezuela	1	0	5	3	8
Total	39	93	136	109	338

La muestra cuenta con un 42% de hombres y un 58% de mujeres con edades comprendidas entre los 25 y los 61 años. El intervalo de 36 a 45 años tiene mayor representación (35.2%), mientras que el rango de más de 56 años es el de menor presencia (14.8%). El 34.9% son de 46 a 55 años y el 15.1% son del intervalo de edad de 25 a 35. Casi la mitad de participantes, 47.9%, tiene doctorado o posdoctorado, el 40.8% Maestría y un 11.3% Licenciatura/ Especialidad. El 93% ha llevado formación en temas digitales (uso de TIC en la educación, de Internet, aplicaciones generales o herramientas multimedia para el diseño de cursos en plataformas educativas) y el 27% específicamente en temas de seguridad digital. De este 27%, 25% orientado a limitar uso de dispositivos, todos estos docentes (el 27%) en temas para el establecimiento de contraseñas seguras y diferentes según tipo de servicios, 12% cómo detectar o proteger del acoso cibernético, 25% a impedir entrada de programas malignos y solo el 4% sobre certificados digitales, cifrado de información). Todos los cursos sobre temas de seguridad fueron de corta duración y como complemento a los de implementación de recursos tecnológicos.

Dado que la distribución entre universidades y por país se presenta muy dispar, no resulta viable una comparación entre estas variables. Es relevante denotar que no se trata de muestras representativas, pero al ser de carácter exploratorio consideramos que los datos facilitan vislumbrar predisposición en torno al problema de investigación y determinar si hay un perfil diferencial en función de variables como formación en competencias digitales, área de conocimiento de docencia, edad o grado académico del docente.

Instrumento

Para la construcción ex profeso del instrumento se hizo una revisión de marcos institucionales internacionales que delimitan la competencia en cuestión. De allí, se tomaron como referentes para fundamentar la operacionalización de algunas cuestiones el Marco de Competencia Digital Docente DigCompEdu (European Commission, 2017) y el Marco de competencias Digitales de la Ciudanía en sus versiones DigComp 2.0 (Vuorikari et al., 2016) y DigComp2.1 (Carretero et al., 2017). Ambos son de interés y de gran impacto en el ámbito de la educación digital ya que parten de un enfoque holístico e integran la visión de expertos e investigadores internacionales. En estos marcos se determinan factores, proponen descriptores de niveles y ejemplos de uso en el ambiente de aprendizaje que facilitan la exploración de competencias. Tras revisión de literatura referente al tema y de Marcos de Competencias Digitales quedaron en el instrumento 44 ítems distribuidos en cuatro dimensiones, de los cuales 37 ítems que permiten caracterizar el uso crítico y seguro en Internet cuando se lleva a cabo comunicación, colaboración y otras interacciones en la red.

La primera dimensión contiene instrucciones para responderlo y además abarca aspectos generales del participante al involucrar indagaciones sobre el contexto y formación permanente tecnológica recibida. La segunda y tercera constan de 29 ítems que se centran en explorar concepciones, experiencias vividas en red, prácticas y sentimientos docentes sobre uso crítico y seguro en internet como el uso de protección personal y de datos al participar en procesos colaborativos y de gestión de información, que den posibles indicios de sus acciones de ciberseguridad; por lo que incluían preguntas cerradas dicotómicas, preguntas abiertas y 23 preguntas con escala de respuesta tipo Likert que fueron transformadas a valores: nunca (valor=1),

ocasionalmente (valor=2), con frecuencia (valor=3), mucho o siempre (valor=4). La cuarta dimensión fue construida para medir el nivel de dominio de la competencia uso responsable o de bienestar cuando usen tecnologías digitales del Marco DigCompEdu (European Commission, 2017). Para ello se adaptaron 8 ítems con elementos del DigComp 2.0 y DigComp2.1 estrechamente vinculados a este aspecto; Marcos de competencias Digitales en los que se ha basado la investigación para determinar los niveles que facilitan definir un perfil competencial del docente. Cada cuestión expone un elemento de competencia con cuatro series de conductas diferentes de actuación de modo que el participante debe seleccionar de entre ellas una que caracteriza sus acciones cuando trabaja en la red, donde cada serie fue transformada posteriormente a un nivel de competencia: Nulo=1, fundamental=2, Intermedio=3 o avanzado=4.

El instrumento fue validado a través de la técnica de análisis y discriminación de contenido bajo juicio experto, por parte de 7 miembros de una red de colaboración de investigación, siguiendo criterios de formación académica y experiencia en el campo en particular; estas personas son de 7 países de los 9 que intervienen en la investigación. El trabajo de validación se hizo en tres fases y sustentadas principalmente a través de reuniones en forma virtual. En la primera fase se les dio a conocer el contexto y objetivo de la investigación, donde además se les compartió el borrador del instrumento. Se llevó a cabo un primer análisis de la pertinencia y contenido de los ítems que les fueron comunicados por los investigadores de este trabajo. En una segunda fase, a través de comunicaciones más individualizadas, se recibieron comentarios que condujeron a nuevos ajustes. Tras incorporar en el instrumento las aportaciones y atender sugerencias de mejora vertidas por el panel de expertos en la primera y segunda fase, se logró en una tercera fase un acuerdo de forma general en la redacción, pertinencia y adecuación de los ítems. Además, se llevó a cabo la validación experimental utilizando una muestra exploratoria de 35 docentes con características similares al grupo estudiado. Su fiabilidad se calculó con el coeficiente Alfa de Cronbach, obteniéndose un valor adecuado de consistencia interna entre variables de 0.824 en su conjunto.

Análisis de datos

Se utilizó el paquete Statistical Package for the Social Sciences (SPSS) v.23 para el procedimiento de análisis estadísticos que consistió en una estadística descriptiva (media, desviación típica, proporción) e inferencial (contraste de diferencia entre variables). Se aplicó la prueba de Kolmogorov-Smirnov y al no cumplir con los supuestos de normalidad se emplearon pruebas no paramétricas según muestras de medidas independientes (H de Kruskal-Wallis y U de Mann-Whitney). Se consideraron como variables dependientes las dimensiones del instrumento y como variables de agrupación el área de conocimiento, formación en seguridad, edad y grado académico del docente. La interrelación entre variables fue medida con la prueba correlación de Spearman y la prueba técnica de fiabilidad con el coeficiente Alfa de Cronbach.

RESULTADOS

Los datos de este estudio revelan que los hábitos de uso de internet del profesorado para comunicar, colaborar, publicar y bajar información; se relacionan con comportamientos de riesgo al asumir principalmente que se conectan a redes WIFI públicas e intercambiar todo tipo de archivos, una de las mayores vías de peligro de seguridad y privacidad a las que se exponen los usuarios. De acuerdo a valores en Tabla 2, más de la mitad de los profesores exponen datos, tráfico e identidad al utilizar redes públicas que no controlan para compartir, consultar y descargar videos, texto, audio, libros, revistas, utilizar Banca en línea o realizar compra de bienes y servicios. Las redes públicas son propicias para aprovechar vulnerabilidades de sistemas operativos, lo que permite que los datos transmitidos durante esa comunicación estén comprometidos. Aunado a ello, los riesgos propios de descargar archivos sin control, que éstos contengan información que resulte perjudicial o desagradable.

Otro dato de interés, que fue obtenido con las preguntas cerradas dicotómicas y preguntas abiertas, es que el 75% de participantes utilizan generalmente en sus dispositivos móviles diversas aplicaciones informáticas en las cuales se registran datos de carácter personal, incluidas imágenes y calificaciones. Estos datos quedan expuestos a muchos usuarios al participar en redes sociales, foros, blogs, páginas de noticias y en otras acciones. Siendo un inconveniente compartir información a alumnos en estos medios por el riesgo de que se divulgue a terceros no deseados información personal expuesta. En este caso, el 55% de los participantes lo hacen con frecuencia o mucho. Aunque es reducido el porcentaje (7.5%) se observan riesgos de integridad física o moral al hacer citas con personas desconocidas a través de un sitio Web.

Los comportamientos de riesgo que exponen han llevado a que un 39% de los profesores hayan sido partícipes de daños a consecuencia de las vulnerabilidades existentes en Internet. Entre las experiencias vividas en la red se encuentran el fraude cibernético, acoso cibernético, robo de datos de investigación y académicos (material evaluativo, contenido de cursos), destrucción de información, daño en hardware, virus, spam, suplantación de identidad, ingreso a redes sociales personales y envío de mensajes desde ahí.

Tabla 2: Medias (M) y desviaciones típicas (DT) para ítems de gestión, comunicación, colaboración y otras interacciones en la red con riesgos. Nunca (nun), ocasionalmente (oca), con frecuencia (fre) y mucho o siempre (sie)

Ítem	*M*	*DT*	*% en escala*			
			nun	*oca*	*fre*	*sie*
Utilizar redes WIFI públicas para leer y/o descargar libros en línea, revistas o periódico	3.13	0.901	4.6	21.0	31.5	42.9
Utilizar redes WIFI públicas para compartir y descargar videos, texto, audio, programas, etc.	3.11	0.871	3.8	21.4	34.5	40.3
Utilizar correo-e diferente a plataforma educativa para intercambio de imágenes, audio, texto, etc. con estudiantes	3.35	0.951	6.3	14.7	16.4	62.6
Utilizar herramientas de almacenamiento en nube para compartir información con alumnos	3.02	0.983	5.9	29.4	21.4	43.3
Compartir información con alumnos en redes sociales	2.68	1.215	25.2	19.3	18.1	37.4
Utilizar redes WIFI públicas para compartir contenido en Blogs	1.88	1.034	49.6	23.5	16.4	10.5
Utilizar redes WIFI públicas para uso de WhatsApp	2.64	1.123	19.7	28.2	20.6	31.5
Utilizar redes WIFI públicas para participar en cuestionarios en línea o videojuegos	1.76	0.884	48.7	31.6	14.7	5.0
Comprar bienes y servicios a través de Internet en puntos de acceso públicos	1.85	0.887	42.9	34.5	17.6	5.0
Utilizar redes WIFI públicas para el uso de servicio de Banca en línea	2.07	1.121	44.1	19.7	21.1	15.1
Hacer cita con personas desconocidas a través de un sitio Web	1.33	0.689	77.4	15.1	5.0	2.5
Establecer datos sensibles como contraseñas, datos bancarios, material de evaluación, etc. en almacenamiento en nube	1.75	1.084	58.8	22.3	3.8	15.1

Es importancia limitar el riesgo y evitar que las acciones en red tengan consecuencias mayores, por lo que otra cuestión fue observar si se involucran en acciones de protección personal y de datos. Tal y como muestra la Tabla 3, el nivel de protección es ligeramente superior en estrategias como utilización de software para detectar aplicaciones maliciosas, actuación respetuosa preservando confidencialidad y privacidad de otras personas y la propia cuando publican imágenes, configuran privacidad en perfiles, emplean contraseñas robustas o método de bloqueo de pantalla. Específicamente, porcentajes superiores al 61% las aplican con frecuencia o siempre. Mientras que más de la mitad instalan aplicaciones desde repositorios oficiales o consideran revisar la valoración y comentarios que previamente hicieron otros usuarios, que les pueda garantizar que al instalar dichas aplicaciones no haya consecuencias negativas para sus equipos e información que contienen en ellos. En relación al aspecto ético y legal, más de la mitad verifican los derechos de autor y licencias de la información y del contenido digital a utilizar en la impartición de sus asignaturas.

Tabla 3: Medias (M) y desviaciones típicas (DT) para ítems de gestión y otras interacciones en la red con acciones de protección personal y de datos. Nunca (nun), ocasionalmente (oca), con frecuencia (fre) y mucho o siempre (sie)

Ítem	*M*	*DT*	*% en escala*			
			nun	*oca*	*fre*	*sie*
Realizar copias de seguridad de información	2.60	0.907	8.0	45.0	26.0	21.0
Utilizar ventana de incógnito o eliminar historial y cookies del navegador	2.13	0.886	23.9	49.2	17.2	9.7
Utilizar Firewall, antivirus, anti-spam, etc. que detecten apps maliciosas en dispositivos	3.03	1.075	8.8	29.9	11.3	50.0
Tener cuidado al publicar imágenes y vídeos para no poner en riesgo su intimidad y la de otras personas	3.24	1.016	8.0	18.5	15.5	58.0
Configurar perfil de redes sociales para que accedan a información publicada solamente usuarios definidos	3.06	1.031	9.7	21.0	22.7	46.6
Emplear contraseñas robustas en dispositivos y aplicaciones, difíciles de adivinar por otros	3.23	0.994	3.8	29.0	7.6	59.6
Considerar un código numérico o patrón en dispositivos que bloquee acceso a personas no autorizadas	3.04	1.130	11.3	27.7	6.8	54.2
Utilizar un método de cifrado de información para que acceda únicamente la persona autorizada	1.75	0.911	50.8	29.9	13.0	6.3
Usar herramientas para localizar dispositivos, bloquearlos e incluso eliminar información almacenada en caso de robo	1.58	0.826	60.1	24.7	11.8	3.4
Descargar apps únicamente de páginas oficiales	2.95	1.056	7.6	35.7	11.3	45.4
Revisar la valoración y comentarios de usuarios de aplicaciones antes de instalarlas	2.74	1.158	17.2	31.6	11.3	39.9

El 73% de los profesores nunca utiliza la ventana de incógnito o elimina el historial y cookies, o sólo lo hace ocasionalmente, al entrar en otros ordenadores. Por lo que cabe advertir en ellos posibles riesgos de confidencialidad y privacidad de que otros visualicen las páginas visitadas o accedan con contraseñas que hayan quedado guardadas en esos dispositivos ajenos que no tienen bajo su control. Un riesgo mayor de confidencialidad y privacidad se presenta para aquellos docentes que no cifran la información y que, por ejemplo, suban archivos a la nube, o lleven a cabo una mala gestión de contraseñas y de permisos para el acceso a determinados documentos en los ordenadores que utilizan o simplemente, no bloqueen o no cierren sesiones y se alejen de los dispositivos en lugares externos; permitiendo con ello poner al alcance de otros los datos que poseen a través de sus equipos. Respecto a esto, es importante denotar que más del 50% advierte que nunca utiliza métodos de cifrado de información, localización y bloqueo total del dispositivo en caso de robo.

Ante todos estos elementos observados, se señala una falta de cultura de ciberseguridad y en muchos casos hasta de medidas básicas de prevención. Y es que independiente de las acciones en internet, se manifiestan riesgos de pérdida de datos almacenados y exposición de información en dispositivos. Menos de la mitad hacen copias de seguridad con frecuencia de la información que poseen, no hay una práctica habitual de ello en el día a día.

La necesidad de mitigar el impacto de las tecnologías ha llevado a que instituciones educativas se preocupen en preparar a los docentes en competencias digitales, el 93% afirma haber participado en los últimos años en acciones formativas sobre uso de TIC en la educación, de Internet, aplicaciones generales o herramientas multimedia. No obstante, solamente un 27% manifestó tener capacitación en seguridad tecnológica orientados en su mayoría a limitar uso de dispositivos, establecimiento de contraseñas seguras, protección y detección de ciberacoso y programas malignos; y el 4% sobre certificados digitales, cifrado de información. Aunado a ello, el 60% desconoce si su universidad dispone de normas internas y procedimientos de uso de aplicaciones digitales (restricciones de acceso o descargas, tasa de uso, derecho de autor u otros estándares de seguridad). Un dato interesante que se observó es el alto porcentaje de profesores (97%) que considera relevante la temática de la cultura en ciberseguridad y que demanda se centre también la formación en ello.

Los resultados en Tabla 4 sobre competencias relacionadas al manejo de riesgos que los docentes deben poseer para asegurar el bienestar físico, psicológico y social de los estudiantes cuando usen tecnologías digitales (European Commission, 2017), indican en su mayoría medias en el rango de 2.00 a 2.82. Esto indica que estos profesores perciben un nivel digital competente en este ámbito que oscila principalmente entre fundamental (3 ítems con porcentaje más alto en este valor) e intermedio (4 ítems con porcentaje más alto para este valor); sólo en una obtienen por encima del intermedio. Siendo la competencia sobre evaluación critica en la que se percibe al profesorado con más dominio y la relacionada a identidades digitales la que menos dominan, destacándose en ésta un alto porcentaje nulo (30.7%).

Tabla 4: Medias (M) y desviaciones típicas (DT) para ítems de competencias digitales para uso responsable en Internet. Nulo (nul), fundamental (fun), intermedio (int), avanzado (ava)

Ítem	*M*	*DT*	*% en nivel*			
			nul	*fun*	*int*	*ava*
Analizar y hacer evaluación critica de fuentes de datos, información y contenido digital	3.42	0.729	1.7	9.2	34.5	54.6
Conocer y saber cómo usar normas de comportamiento al utilizar tecnologías digitales e interactuar en ambientes digitales	2.63	0.876	10.1	33.6	39.9	16.4
Crear y administrar identidades digitales para proteger reputación y datos producidos con servicios digitales	2.00	0.900	30.7	48.3	11.3	9.7
Comprender cómo se aplican los derechos de autor y licencias a información y contenido digital	2.75	0.974	12.2	26.5	35.7	25.6
Comprender riesgos y amenazas en entornos digitales para proteger dispositivos y contenido digital	2.82	0.828	0.0	44.5	28.6	26.9
Proteger datos personales y privacidad en entornos digitales	2.45	0.897	16.0	34.9	37.4	11.8
Evitar riesgos de bienestar físico y psicológico al usar tecnologías digitales	2.53	1.070	19.7	31.9	23.5	24.8
Conocer el impacto ambiental del uso de tecnologías digitales	2.78	0.903	11.8	18.9	49.2	20.2

El análisis llevado a cabo sobre correlación entre competencias, hábitos de riesgos y de protección en Internet, estableció una relación significativa con respecto a algunas de las variables. Tras aplicar las pruebas de H de Kruskal-Wallis y U de Mann-Whitney se detectaron algunas diferencias significativas de los ítems con relación al área de conocimiento, edad, grado académico y en función de su capacitación básica de seguridad. Se aprecia en Tabla 5 solamente aquellos ítems de gestión, comunicación, colaboración y otras interacciones en

la red; tanto de riesgo como con acciones de protección personal y de datos, aunado a ellos los de competencias digitales de uso responsable, que resultaron tener relación significativa en función del área de conocimiento. Los profesores de Ciencias Sociales y Jurídicas son más propicios a compartir información en redes sociales y hacer citas con desconocidos en relación a las otras áreas. Los docentes de Artes y Humanidades son más asiduos a utilizar redes WIFI públicas para participar en cuestionarios, videojuegos y blogs; y muestran ser más críticos al evaluar el contenido digital. En cambio, a los de Ciencias Exactas, Salud e Ingenierías les preocupa más la privacidad en redes sociales.

Tabla 5: Únicos Ítems con diferencias significativas según área de conocimiento. Prueba de H de Kruskal-Wallis. Se consideran los 23 ítems de gestión e interacciones en la red y los 8 de competencias

Ítem	*Chi-cuadrado*	*gl*	*Significancia*
Compartir información con alumnos en redes sociales	12.070	2	0.002
Utilizar redes WIFI públicas para compartir contenido en Blogs	18.449	2	0.000
Utilizar redes WIFI públicas para participar en cuestionarios en línea o videojuegos	7.188	2	0.027
Hacer cita con personas desconocidas a través de un sitio Web	13.132	2	0.001
Configurar perfil de redes sociales para que accedan a información publicada solamente usuarios definidos	6.181	2	0.045
Analizar y hacer evaluación critica de fuentes de datos, información y contenido digital	10.491	2	0.005

En cuanto a la edad, se muestra en Tabla 6 solamente tres diferencias significativas; dos con relación a ítems de gestión y colaboración en la red con riesgo, y una con relación a acción de protección personal y de datos. Los más jóvenes (25 a 35 años) comparten más frecuentemente información con herramientas en nube o redes sociales. Mientras que de 36 a 45 años configuran con más frecuencia su privacidad en redes sociales.

Tabla 6: Únicos Ítems con diferencias significativas según edad. Prueba de H de Kruskal-Wallis. Se consideran los 23 ítems de gestión e interacciones en la red y los 8 de competencias

Ítem	*Chi-cuadrado*	*gl*	*Significancia*
Utilizar herramientas de almacenamiento en nube para compartir información con alumnos	12.841	3	0.005
Compartir información con alumnos en redes sociales	11.132	3	0.011
Configurar perfil de redes sociales para que accedan a información publicada solamente usuarios definidos	11.815	3	0.008

En relación al grado académico, en Tabla 7 se muestra que los de grado Doctor presentan mejores hábitos de protección y mayor nivel digital competente en seguridad. Están más acostumbrados a emplear contraseñas robustas, tienden a ser más críticos del contenido digital, administran identidades digitales, protección de datos personales y privacidad en relación con los que tienen el grado de Maestría o Licenciatura.

Tabla 7: Únicos Ítems con diferencias significativas en función del grado académico. Prueba de H de Kruskal-Wallis. Se consideran los 23 ítems de gestión e interacciones en la red y los 8 de competencias

Ítem	*Chi-cuadrado*	*gl*	*Significancia*
Emplear contraseñas robustas en dispositivos y aplicaciones. difíciles de adivinar por otros	8.050	2	0.018
Analizar y hacer evaluación critica de fuentes de datos, información y contenido digital	9.745	2	0.008
Crear y administrar identidades digitales para proteger reputación y datos producidos con servicios digitales	6.319	2	0.042
Proteger datos personales y privacidad en entornos digitales	6.462	2	0.040

Como era de esperar y de acuerdo con los descriptivos básicos reflejados en Tabla 8, los sujetos con previa capacitación en seguridad, orientados en su mayoría a limitar uso de dispositivos, en el establecimiento de contraseñas seguras y a impedir entrada de programas malignos, asumen mejores hábitos de protección y en mayor medida nivel competencial con respecto a los que no han tenido ese tipo de capacitación. Localizándose estos resultados en 6 de 11 ítems de acciones de protección personal y de datos; y en otras 6 de 8 ítems de competencias de uso responsable cuando utilizan tecnologías digitales.

Tabla 8: Medias (M), desviaciones típicas (DT) de únicos Ítems con diferencias significativas en función de capacitación básica sobre seguridad. Se consideran los 23 ítems de gestión e interacciones en la red y los 8 de competencias

Ítem	*Nunca*		*Si ha llevado*		*U de Mann-Whitney*		
	M	*DT*	*M*	*DT*	*U*	*Z*	*P*
Realizar copias de seguridad de información	2.53	0.886	2.78	0.944	4741.000	-1.984	0.047
Utilizar ventana de incógnito o eliminar historial y cookies del navegador	2.03	0.889	2.37	0.840	4308.000	-2.993	0.003
Tener cuidado al publicar imágenes y vídeos para no poner en riesgo su intimidad y la de otras personas	3.14	1.077	3.48	0.793	4783.500	-1.989	0.047
Configurar perfil de redes sociales para que accedan a información publicada solamente usuarios definidos	2.97	1.081	3.31	0.846	4719.500	-2.038	0.042
Considerar un código numérico o patrón en dispositivos que bloquee acceso a personas no autorizadas	2.93	1.159	3.32	1.002	4593.500	-2.405	0.016
Revisar valoración de aplicaciones y comentarios de usuarios antes de instalarlas	2.60	1.161	3.12	1.068	4207.000	-3.155	0.002
Conocer y usar normas de comportamiento al utilizar tecnologías digitales e interactuar en ambientes digitales	2.53	0.880	2.88	0.820	4411.000	-2.709	0.007
Crear y administrar identidades digitales para proteger reputación y datos producidos con servicios digitales	1.88	0.878	2.32	0.886	4005.000	-3.694	0.000
Comprender cómo se aplican los derechos de autor y licencias a información y contenido digital	2.62	1.008	3.09	0.785	4165.000	-3.216	0.001
Comprender riesgos y amenazas en entornos digitales para proteger dispositivos y contenido digital	2.76	0.835	3.01	0.791	4677.500	-2.142	0.032
Proteger datos personales y privacidad en entornos digitales	2.33	0.903	2.77	0.806	4090.500	-3.413	0.001
Evitar riesgos de bienestar físico y psicológico al usar tecnologías digitales	2.42	0.903	2.83	0.911	4403.500	-2.669	0.008

DISCUSIÓN

Los peligros que conllevan las tecnologías nos han impulsado a centrar la mirada en el uso crítico y seguro en Internet; y reflexionar en torno a las prácticas del docente en la red y si se apropia de esta competencia digital en la medida que esté preparado para adiestrar al alumnado a ser responsable y evitar riesgos. Los hallazgos de la investigación indican que tienen inclinación a hábitos y conductas de riesgo al exponer datos, tráfico e identidad generados con aplicaciones instaladas en sus dispositivos y trasmitidos durante comunicaciones en redes WIFI públicas.

No obstante que el hecho de administrar y proteger la privacidad en línea debe ser ya una parte esencial de la vida cotidiana (Büchi et al., 2017), hacemos alusión que una gran cantidad de ellos se vieron envueltos en experiencias poco gratas en la red, citando el fraude cibernético, acoso cibernético, robo o destrucción de datos académicos y de investigación, así como suplantación de identidad. Ante lo cual, algunos no establecieron soluciones funcionales. A la vista de los datos obtenidos, es preocupante que los profesores manifiestan una navegación no segura en red. Se observa, que hay profesores universitarios que no están adecuadamente preparados con competencias digitales para ello (Blayone et al., 2018). Reflejándose en este sentido, la necesidad de fomentar una cultura del uso responsable de las tecnologías en general, e internet en particular, de cara a que logren potenciar estas competencias en sus estudiantes (Amor y Serrano, 2019).

Los resultados infieren también que la mayoría tiende a implicarse en hábitos de protección, aunque se limitan al uso de antivirus, configuración en redes sociales, establecimiento de contraseñas robustas y se olvidan de la importancia que conlleva la gestión de la privacidad (Boerman et al., 2018) y ser consciente de la identidad digital (Chanchary et al., 2018). Por otro lado, se distingue un bajo nivel de dominio en la competencia al observarse una variación entre el nivel fundamental y el intermedio. Al tomar como base el DigCompEdu, las respuestas nulo y fundamental asemejan a niveles de iniciador o explorador, un nivel insuficiente para prevenir algunos riesgos usando tecnologías digitales. En una sociedad impregnada de tecnología en todos los ámbitos, la competencia digital se convierte en una de las competencias imprescindibles en el quehacer docente (Blayone et al., 2018).

El perfil profesional del profesor de educación superior se despliega a través de competencias para hacer frente a las actividades en el marco de su desempeño laboral. Se espera que los docentes alcancen en esta competencia un nivel de dominio más avanzado para que sean líderes en el desarrollo estratégico y crítico del uso responsable y seguro de alumnos hacia las tecnologías digitales. La circunstancia de encontrar casos de uso inapropiado, así como consecuencias negativas de su práctica hace fundamental el considerar replantear la formación para afianzar la tenencia de las competencias propias del ejercicio profesional del profesorado, particularmente porque su desempeño en línea va estrechamente ligado a la aprehensión de las competencias digitales (Instefjord y Munthe, 2017). Ante la imposibilidad de eliminar los riesgos de Internet (Gamito et al., 2017), se requiere en este caso en particular una formación que les permita desarrollar una capacidad técnica para comunicarse y construir conocimientos guiada por el buen juicio encuadrada en el uso responsable, legal y seguro de las tecnologías en los espacios académicos, coincidiendo en este sentido con los hallazgos de Villarreal-Villa et al. (2019), que requieren capacitación en ese tipo de competencias.

Al explorar qué variables podrían estar modulando los hábitos y actitudes de los docentes se encontraron escasos ítems con diferencias significativas en función del área de conocimiento (6 ítems), edad (3 ítems) y grado académico (4 ítems) de los 31 ítems tipo Likert. No obstante, los resultados advierten que los profesionales formados en cualquier tema de seguridad, se distinguen con un mejor nivel de dominio de la competencia y por utilizar más frecuentemente estrategias de protección personal y de datos. Los resultados mostraron que estos docentes no presentan relación significativa con ítems del tipo de interacciones en la red que tengan inclinación a riesgos, pero si se presenta en 12 ítems de los 19 que están ligados a competencias de uso responsable cuando utilizan tecnologías y a las acciones de protección personal y de datos. En este sentido, el comportamiento de seguridad en línea de los usuarios está relacionado con su nivel de conocimiento en ello (Shillair et al., 2015). Y se ha constatado que el área de conocimiento y la edad no influyen en gran medida en la competencia, pero si en sus hábitos de uso.

Es indudable que las universidades apuestan por la formación digital de sus docentes, pero es esencial profundizar que tan relevante es el uso seguro y crítico de internet en las políticas de formación, puesto que solamente una parte muy reducida de la muestra manifestó tener capacitación en seguridad tecnológica y muchos desconocen si disponen en su universidad de normas internas y procedimientos relacionadas con uso de aplicaciones digitales. Se coincide con Prendes et al. (2018), que casi nunca se abordan contenidos éticos en los procesos de formación. Para minimizar incidencias en la red, no basta ser consciente de los riesgos existentes, al igual que Baruh et al. (2017) y Shillair et al. (2015) señalamos que para tener un comportamiento de hábitos seguros y realizar buenas prácticas de uso informático, es esencial adquirir competencias, habilidades y experiencia sobre ello.

La investigación permite el objetivo, mostrar una aproximación a las características de hábitos y actitudes que tienen los profesores universitarios ante la multitud de acciones que llevan a cabo en Internet y vislumbrar tendencias de competencias que necesitan fortalecer para asegurar su bienestar físico, psicológico y social como ciudadanos digitales ante las diferentes puertas de acceso a fuentes de información y de utilidades de intercomunicación con diversos canales de comunicación. Los hallazgos de factores de riesgos hacen imprescindible un compromiso tanto del docente como de la institución para la implementación de formación en ese tema digital. El docente es un elemento clave para integrar las tecnologías en la educación y se le presenta el desafío de atenuar el impacto tecnológico en la vida cotidiana de los estudiantes (Tejada y Pozos, 2018) al observar pautas de comportamiento adecuadas y sentido común en sus movimientos en Internet.

CONCLUSIONES

De acuerdo a los resultados, análisis y discusión del estudio, se llega a las siguientes conclusiones: (1) Es pertinente que se tomen medidas adecuadas para evitar que los docentes se vean comprometidos. El desconocimiento de aspectos de uso ético, legal y seguro lleva a cometer errores, por lo que es significativo además de concientizar al profesorado de los peligros de la sociedad digital, el prepararlos con competencias para que realicen permanentemente prácticas de navegación de forma segura acorde a esas exigencias. Los mejores hábitos de protección y mayor nivel competencial se relacionan con la capacitación de los sujetos en el ámbito de seguridad digital. (2) El punto medular para las universidades y/o para los mismos docentes será reflexionar sobre un proceso de capacitación preciso y diferenciado que esté en concordancia con el nivel específico de requerimiento profesional.

Es pertinente, por lo tanto, hacer una integración estratégica de formación que reconozca las competencias previas para reforzar medidas críticas y seguras de lo que se debe hacer y lo que se puede hacer con las tecnologías impidiendo riesgos y peligros. El estudio sienta las bases para desarrollar pautas de formación docente precisa y continuada que permitan dar solución a esta problemática que se suscita en lo digital.

REFERENCIAS

Amor, M.I., y Serrano, R., *Las competencias generales en la formación inicial del profesorado. Un estudio comparativo entre estudiantes, docentes y graduados de los títulos universitarios de educación*, https://doi.org/10.5944/educXX1.21341, Educ. XX1, 22(1), 239-261 (2019)

Baruh, L., Secinti, E., y Cemalcilar, Z., *Online privacy concerns and privacy management: a meta-analytical review*, https://doi.org/10.1111/jcom.12276, J. Commun., 67(1), 26-53 (2017)

Blayone, T., Mykhailenko, O., y otros cuatro autores, *Surveying digital competencies of university students and professors in Ukraine for fully online collaborative learning*, https://doi.org/10.1080/1475939X.2017.1391871, Technol. Pedagog. Educ., 27(3), 279-296 (2018)

Boerman, S.C., Kruikemeier, S., y Zuiderveen, F.J., *Exploring motivations for online privacy protection behavior: insights from panel data*, https://doi.org/10.1177/0093650218800915, Commun. Res., 1-25 (2018)

Büchi, M., Just, N., y Latzer, M., *Caring is not enough: the importance of internet skills for online privacy protection*, https://doi.org/10.1080/1369118X.2016.1229001, Inform. Commun. Soc., 20(8), 1261-1278 (2017)

Carretero, S., Vuorikari, R., y Punie, Y., *DigComp 2.1: the digital competence framework for citizens with eight proficiency levels and examples of use*, https://doi.org/10.2760/38842, Office of the European Union (2017)

Chatzakou, D., Leontiadis, I., y otros cinco autores, *Detecting cyberbullying and cyberaggression in social media*, https://doi.org/10.1145/3343484, ACM T. Web, 13(3), 1-51 (2019)

Chiasson, S., Abdelaziz, Y., y Chanchary, F., *Privacy concerns amidst OBA and the need for alternative models*, https://doi.org/10.1109/MIC.2017.3301625, IEEE Internet Comput., 22(2), 52-61 (2018)

De Wolf, R., Willaert, K., y Pierson, J., *Managing privacy boundaries together: exploring individual and group privacy management strategies in facebook*, https://doi.org/10.1016/j.chb.2014.03.010, Comput. Hum. Behav., 35(1), 444–454 (2014)

Dourish, P., y Anderson, K., *Collective information practice: exploring privacy and security as social and cultural phenomena,* https://doi.org/10.1207/s15327051hci2103_2, Hum-Comput. Interact., 21(3), 319–342 (2006)

Escudero, J.M., Martínez-Domínguez, B., y Nieto. J.M., *Las TIC en la formación continua del profesorado en el contexto español*, doi: 10.4438/1988-592X-RE-2018-382-392, Rev. Educ-Madrid., 382, 57-80 (2018)

European Commission, *European framework for the digital competence of educators: DigCompEdu,* (2017)

Ferrari, A., *DIGCOMP: a framework for developing and understanding digital competence in Europe*, European Commission, (2013)

Fraser, J., Atkins, L., y Hall, R., *DigiLit Leicester. Supporting teachers, promoting digital literacy, transforming learning*, Leicester City Council, (2013)

Gamito, R., Aristizabal, P., y otros dos autores, *La necesidad de trabajar los riesgos de internet en el aula*, ISSN: 1138-414X, Profesorado, 21(3), 409-426 (2017)

Gisbert, M., González, J. y Esteve, F.M., *Competencia digital y competencia digital docente: una panorámica sobre el estado de la cuestión*, http://dx.doi.org/10.6018/riite2016/257631, Revista Interuniversitaria de Investigación en Tecnología Educativa, 0, 74-83 (2016)

Instefjord, E.J., y Munthe, E., *Educating digitally competent teachers: a study of integration of professional digital competence in teacher education*, https://doi.org/10.1016/j.tate.2017.05.016, Teach. Teach. Educ., 67, 37-45 (2017)

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), *Marco común de competencia digital docente*, (2017)

International Society for Technology in Education (ISTE), *ISTE Standards teachers*, (2018)

Jansen, J., y van Schaik, P., *Testing a model of precautionary online behavior: the case of online banking*, https://doi.org/10.1016/j.chb.2018.05.010, Comput. Hum. Behav., 87, 371-383 (2018)

Kowalski, R.M, Toth, A., y Morgan M., *Bullying and cyberbullying in adulthood and the workplace*, https://doi.org/10.1080/00224545.2017.1302402, J. Soc. Psychol., 158(1), 64-81 (2018)

Mingming, Z., y Xiaotian, Z., *Online social networking and subjective well-being: mediating effects of envy and fatigue*, https://doi.org/10.1016/j.compedu.2019.103598, Comput. Educ., 140 (2019)

Ministerio de Educación de Chile, *ENLACES competencias y estándares TIC en la profesión docente*, (2010)

Mishra, P., y Koehler, M.J., *Technological pedagogical content knowledge; a framework for integrating technology in teacher knowledge*, ISSN: 0161-4681, Teach. Coll. Rec., 108(6), 1017-1054 (2006)

Prendes, M.P., Gutiérrez, I., y Martínez, F., *Competencia digital: una necesidad del profesorado universitario en el siglo XXI*, http://dx.doi.org/10.6018/red/56/7, Revista de Educación a Distancia, 56, 1-22 (2018)

Redmond, P., Lock, J. V., y Smart, V., *Pre-service teachers´ perspectives of cyberbullying*, https://doi.org/10.1016/j.compedu.2017.12.004, Comput. Educ., 119, 1-13 (2018)

Shillair, R., Cotton, S. R., y otros cuatro autores, *Online safety begins with you and me: convincing internet users to protect themselves*, https://doi.org/10.1016/j.chb.2015.01.046, Comput. Hum. Behav., 48, 199-207 (2015)

Tejada, J., y Pozos, K., *Nuevos escenarios y competencias digitales docentes: hacia la profesionalización docente con TIC*, ISSN: 1138-414X, Profesorado, 22(1), 25-51 (2018)

Villarreal-Villa, S., García-Guliany, J., y otros dos autores, *Competencias docentes y transformaciones en la educación en la era digital*, http://dx.doi.org/10.4067/S0718-50062019000600003, Form. Univ., 12(6), 3-14 (2019)

Vuorikari, R., Punie, Y., y otros dos autores, *DigComp 2.0: the digital competence framework for citizens. Update phase 1: the conceptual reference model*, doi:10.2791/11517, Office of the European Union, (2016)