TESIS

Universidad de Jaén

Escuela de doctorado

SEGURIDAD DIGITAL: PERFIL COMPETENCIAL DEL PROFESORADO ANDALUZ

Autor: Rafael Villén Contreras

Director de la tesis: **JAVIER RODRÍGUEZ MORENO**
MIRIAM AGREDA MONTORO

Departamento: Pedagogía

Fecha: 26/09/2024

ISBN:

La memoria titulada **Seguridad Digital: Perfil Competencial del profesorado andaluz** que presenta D. Rafael Villén Contreras para optar al grado de doctor, ha sido realizada dentro del Programa de Doctorado en Innovación didáctica y formación del profesorado de la Universidad de Jaén, bajo la dirección Dr. D. Javier Rodríguez Moreno y la Dra. Miriam Agreda Montoro. Para su evaluación, esta memoria de tesis se presenta como un conjunto de trabajos publicados en razón a lo establecido en el punto 2 del artículo 25 del Reglamento de los Estudios de Doctorado de la Universidad de Jaén, aprobado el 6 de febrero de 2012 y modificado el 18 de febrero de 2019 por el Consejo de Gobierno.

“Los sueños no se cumplen
como los años.
Los sueños se madrugan,
se trabajan, se estudian
y a lo mejor, algún día,
ese sueño se hace realidad”
Toni Acosta

A mis docentes...

AGRADECIMIENTOS

En primer lugar, quisiera reflejar que este trabajo, que me ha acompañado durante tanto tiempo, no habría sido posible sin el apoyo y la colaboración de muchas personas que, generosamente, me han brindado su tiempo y su ayuda. Aunque resulta imposible mencionar a todas ellas, no quiero dejar de reconocer a aquellos pilares fundamentales que han hecho posible alcanzar este momento. Su inquebrantable apoyo y sus valiosas contribuciones han sido esenciales en esta andadura, y por ello les estaré eternamente agradecido.

En primer lugar, quisiera agradecer a Javier Rodríguez Moreno por su paciencia, dedicación y generosidad durante la dirección de esta tesis. Gracias por inspirar mi fortaleza mental y física en momentos de decaimiento y desorientación. Gracias por trasmitirme que sí se puede; que solo hay que creer en ello y ser constante. Gracias por creer en mi por encima de mis posibilidades. No me olvido de Miriam Agreda Montoro, siempre atenta y precisa. Gracias por tus orientaciones, arrojando luz en momentos de oscuridad; siempre en mi equipo.

Quiero destacar a aquellos docentes que, desde mi infancia, encendieron en mí la pasión por la enseñanza. Su dedicación, cercanía y amor por el conocimiento no solo avivaron mi interés por aprender, sino que también hicieron posible la culminación de este trabajo. Desde Doña Pura y María del Carmen Cea en mis años de Educación Primaria, hasta Isabel y Francisco Cabello, entre muchos otros, todos han dejado una huella imborrable en mi camino. A cada uno de ellos, mi más sincero agradecimiento por ser pilares fundamentales en este logro.

Inmensamente agradecido a mi querido Emilio Cerezo, amigo y director del Ceper Ventura Rodríguez (Montefrío-Algarinejo) pues fue allí donde comenzó a rodar este proyecto. Por supuesto, a los que fueron mis compañeros, siempre prestados para la causa.

Gracias a mis amigos, los del pueblo, los docentes y los que no lo son… por involucrarse cuando los necesité y por convertirse en un apoyo moral.

Gracias, querido Andrés por ofrecerme siempre rueda y momentos de liberación, seguiremos “robándole tiempo al tiempo”.

Gracias a todo un referente, Jesús Fernández por acogerme y ponerme en el camino, la vida está llena de pequeñas casualidades. Y por supuesto no me olvido de la familia Lumen, fuente de inspiración.

Gracias a mi familia, en especial a mis padres por su apoyo en momentos difíciles cuando esto solo era un sueño y a mi hermana. Agradecido también a mis otros “padres”, es una suerte teneros cerca.

Gracias a mi maravillosa gran casualidad… Mi esposa María, por visionarme siempre el lado bueno de las cosas, por tu cariño y dedicación. Gracias de manera especial, por ofrecerme el tesoro más preciado; tu tiempo, elemento clave para culminar este trabajo aquí y ahora. Gracias por traer al mundo a lo mejor de nuestras vidas, la pequeña Lola y llenar el hogar de felicidad. Vuestro amor, alegría y viveza son mi motor de vida.

No quisiera olvidar a nadie, por lo que, si estás leyendo estas líneas, puedes sentirte parte de mi más sincera gratitud.

ÍNDICE

Índice de contenidos

Listado de figuras

RESUMEN

RESUMEN

En el contexto educativo los docentes se enfrentan a desafíos actuales, como los riesgos y amenazas vinculados al uso de internet y dispositivos inteligentes, siendo crucial desarrollar competencias en seguridad digital y actuar éticamente en entornos digitales. La presente tesis doctoral *"Seguridad Digital: Perfil Competencial del profesorado andaluz"* tuvo como objetivo analizar las dimensiones de seguridad basadas en el Marco Europeo de Competencias Digitales para la Ciudadanía (DigComp 2.2) a través del diseño y validación del instrumento COSEDI. Este instrumento amplio se divide en cuatro dimensiones: Protección de Dispositivos, Protección de datos Personales, Protección de la Salud y el Bienestar y Protección Medioambiental, centrándose este trabajo en las dos primeras. Cada una de ellas compuesta por 15 ítems, lo cual ha permitido evaluar el nivel y perfil competencial de los docentes en su práctica profesional.

Este trabajo se organiza en cinco capítulos. El primer capítulo ofrece una introducción breve que presenta la motivación del estudio, sus objetivos y la estructura general de la tesis. A continuación, el segundo capítulo desarrolla el marco teórico, donde se identifican los distintos marcos de referencia para la competencia digital y se revisan investigaciones previas relacionadas con la competencia digital docente, así como el uso seguro y ético de los dispositivos digitales y la gestión de los datos personales.

El tercer capítulo detalla la metodología utilizada para el desarrollo de la tesis, proporcionando una visión clara de los enfoques y técnicas aplicadas en la investigación.

El cuarto capítulo recoge los estudios publicados derivados de la tesis doctoral, que incluyen un compendio de tres artículos. El primer artículo aborda la validación y el estudio piloto de una escala para evaluar la competencia en seguridad digital del profesorado en centros educativos. El segundo artículo presenta los resultados cuantitativos de la aplicación del instrumento COSEDI para analizar el perfil competencial del profesorado andaluz en seguridad digital, específicamente en la dimensión de protección

de datos y privacidad, según el marco DigComp. Finalmente el tercer artículo evalúa la protección de dispositivos conforme al mismo marco.

En el quinto capítulo se presentan los resultados y la discusión de los hallazgos, y finalmente, en el sexto establecen las conclusiones generales de la investigación, así como las discusiones acerca de las limitaciones del estudio y posibles líneas de investigación futuras.

Con respecto a los resultados, estos demostraron la validez y fiabilidad del instrumento COSEDI, evidenciando relaciones causales significativas entre los constructos de protección de datos y privacidad, protección de dispositivos, protección medioambiental y protección de la salud y el bienestar.

El análisis de los mismos reveló que las cuatro variables latentes están interrelacionadas, con influencias mutuas. La relación más fuerte y significativa se encontró entre la protección de datos y privacidad y la protección de dispositivos, lo que indica una fuerte conexión entre la gestión segura de la información personal y el uso correcto de los dispositivos tecnológicos. En cambio, la relación más débil se observó entre la protección de datos personales y la protección medioambiental, sugiriendo que, aunque ambas forman parte del marco de competencias digitales, su interdependencia es menos marcada. Estos resultados subrayan la importancia de enfoques formativos diferenciados para fortalecer cada dimensión de la seguridad digital en el ámbito educativo.

Otro de los hallazgos destacados fue la identificación de disparidades significativas tanto en la protección de datos personales como en la salvaguarda de sus dispositivos digitales, relacionados con la edad, la antigüedad docente y las horas de formación recibidas. Las revelaciones indican que los docentes de mayor edad, con más años de experiencia y mayor formación en seguridad digital tienden a obtener calificaciones más elevadas en ambas dimensiones.

Por otro lado, se observó una considerable variabilidad en el uso de medidas de seguridad entre los docentes, específicamente en el uso de software de

rastreo para dispositivos perdidos o robados y en la implementación de cortafuegos en entornos públicos y laborales. Esta variabilidad indica diferencias en la conciencia y aplicación de prácticas de seguridad digital, lo que sugiere la necesidad de fortalecer la formación en estas áreas. Es crucial mejorar el conocimiento y la adopción de herramientas de protección, así como el desarrollo de políticas claras que aseguren una implementación uniforme de medidas de seguridad digital en los entornos educativos.

Tras la realización de esta tesis doctoral, se proponen como futuras líneas de investigación la indagación de la efectividad de las diversas modalidades de formación y estrategias pedagógicas en el desarrollo de competencias en seguridad digital para docentes de primaria y secundaria. Esto permitiría identificar las metodologías más efectivas y adaptarlas para optimizar el aprendizaje y su aplicación práctica en contextos escolares. Además, se sugiere la puesta en práctica de evaluaciones longitudinales de los efectos de la formación en seguridad digital, analizando su evolución y el impacto a largo plazo en la práctica docente y en la seguridad del contexto escolar.

Palabras clave: Formación de profesores; competencia digital; competencia en seguridad digital y ética; DigComp.

ABSTRACT

In the educational context, teachers face current challenges, such as the risks and threats associated with the use of the internet and smart devices, making it crucial to develop digital security competencies and act ethically in digital environments. The present doctoral thesis “Digital Security: Competence Profile of Andalusian Teachers” aimed to analyze security dimensions based on the European Digital Competence Framework for Citizens (DigComp 2.2) through the design and validation of the COSEDI instrument. This comprehensive instrument is divided into four dimensions: Device Protection, Personal Data Protection, Health and Well-being Protection, and Environmental Protection, with this work focusing on the first two. Each dimension is composed of 15 items, allowing for the evaluation of the level and competence profile of teachers in their professional practice.

This work is organized into five chapters. The first chapter provides a brief introduction that presents the motivation of the study, its objectives, and the overall structure of the thesis. The second chapter develops the theoretical framework, identifying the different reference frameworks for digital competence and reviewing previous research related to teachers' digital competence, as well as the safe and ethical use of digital devices and the management of personal data.

The third chapter details the methodology used for the development of the thesis, providing a clear view of the approaches and techniques applied in the research. The fourth chapter presents the studies published from the doctoral thesis, including a compendium of three articles. The first article addresses the validation and pilot study of a scale to assess digital security competence in teachers in educational institutions. The second article presents the quantitative results of the application of the COSEDI instrument to analyze the digital security competence profile of Andalusian teachers, specifically in the dimension of data protection and privacy, according to the DigComp framework. Finally, the third article evaluates device protection according to the same framework.

The fifth chapter presents the results and discusses the findings, and finally, the sixth chapter establishes the general conclusions of the research, as well as discussions on the limitations of the study and possible future lines of research.

Regarding the results, they demonstrated the validity and reliability of the COSEDI instrument, showing significant causal relationships between the constructs of data protection and privacy, device protection, environmental protection, and health and well-being protection.

The analysis revealed that the four latent variables are interrelated, with mutual influences. The strongest and most significant relationship was found between data protection and privacy and device protection, indicating a strong connection between the secure management of personal information and the correct use of technological devices. In contrast, the weakest relationship was observed between personal data protection and environmental protection, suggesting that although both are part of the digital competence framework, their interdependence is less pronounced. These results highlight the importance of differentiated training approaches to strengthen each dimension of digital security in the educational field.

Another key finding was the identification of significant disparities in both personal data protection and safeguarding of digital devices, related to age, teaching experience, and hours of digital security training received. The findings indicate that older teachers, with more years of experience and more training in digital security, tend to score higher in both dimensions.

Additionally, considerable variability was observed in the use of security measures among teachers, particularly in the use of tracking software for lost or stolen devices and the implementation of firewalls in public and work environments. This variability indicates differences in awareness and application of digital security practices, suggesting the need to strengthen training in these areas. It is crucial to improve knowledge and adoption of protection tools, as well as the development of clear policies to ensure the uniform implementation of digital security measures in educational settings.

Following the completion of this doctoral thesis, future research lines are proposed to investigate the effectiveness of different training modalities and pedagogical strategies in developing digital security competencies for primary and secondary school teachers. This would allow the identification of the most effective methodologies and adapt them to optimize learning and its practical application in school contexts. Additionally, it is suggested to implement longitudinal evaluations of the effects of digital security training, analyzing its evolution and long-term impact on teaching practice and the security of the school environment.

Keywords: Teacher training; digital competence; digital security and ethics competence; DigComp.

CAPÍTULO 1. PRESENTACIÓN

1.1 Marco de la investigación

En términos generales, esta tesis doctoral se sustenta sobre el acercamiento al nivel de competencia en seguridad digital de docentes en activo. Para ello, tomaremos como referente el marco de competencia digital europeo (DigComp) en su versión actual. Este proporciona una estructura coherente para la comprensión y valoración de la competencia digital docente, que se consolida y expande a nivel internacional (Vuorikari Rina et al., 2022).

Concretamente nos centraremos en la responsabilidad docente para conocer la autopercepción de su nivel competencial en seguridad digital, sus carencias y necesidades formativas en relación con la protección de los datos personales y la utilización de los dispositivos digitales para el desarrollo de su actividad en el ámbito profesional y personal. Estos serán los aspectos a tener en cuenta durante el desarrollo del presente trabajo doctoral y cuyos resultados serán analizados durante el mismo.

Esta tesis titulada “Seguridad digital: perfil competencial del profesorado andaluz” se enmarca en la normativa actual vigente de la Universidad de Jaén y cuenta con la autorización de los directores de tesis y de la Comisión de Doctorado de esta Universidad, así como de las personas que hayan colaborado en la coautoría de la redacción de las publicaciones incluidas.

Asimismo, se presenta como un conjunto de tres artículos publicados en revistas indexadas en JCR o SJR tras superar el correspondiente proceso de revisión por pares, cumpliendo de este modo los requisitos para su realización y promoción.

Este compendio de tres artículos han sido escritos durante el proceso formativo de los estudios de Doctorado en Innovación Didáctica y Formación del Profesorado, en la línea "Innovación Didáctica y Formación de Profesorado”.

El formato de presentación queda justificado por el hecho de que los tres trabajos pertenecen a uno de los campo de estudio desarrollados durante estos últimos años como docente y entendiendo que sería de gran interés y

relevancia trasladar a mis estudios de doctorado. Su compendio mantiene la coherencia y complementariedad de las hipótesis planteadas, otorgándoles la validez y calidad necesarias para garantizar su importancia en la transferencia de conocimiento.

El aporte científico de esta tesis doctoral se manifiesta en la validación e implementación de un modelo de medida y de relación estructural, “COSEDI”, sobre la autopercepción del profesorado en base a sus competencias digitales en el área de seguridad, y su posterior análisis. Estas aportaciones se desarrollan en los distintos trabajos que componen la tesis doctoral.

1.2. Objetivos de la investigación

Los objetivos generales de la presente tesis doctoral mantienen un carácter de origen reflexivo, así como un componente metodológico. Para una mejor comprensión se mantiene el orden que se presentan los artículos que forman este compendio. Estos objetivos son:

1. Analizar la fiabilidad y validar el instrumento COSEDI, basado en el Marco Europeo de Competencias Digitales para la Ciudadanía (DigComp) para evaluar la percepción de autoeficacia de los docentes en cuanto a la seguridad digital (Artículo 1)
2. Analizar la relación entre las distintas variables del estudio (Artículo 1)
3. Evaluar la competencia digital en seguridad de docentes activos andaluces en relación con la protección de datos personales y la protección de dispositivos a través de un análisis según género, experiencia docente, edad y formación. (Artículos 2 y 3)
4. Analizar la percepción, carencias y necesidades formativas del profesorado andaluz respecto a la competencia digital en el área de seguridad (Artículos 2 y 3).

Los objetivos específicos que han emergido durante el proceso de investigación se detallan en cada una de las publicaciones científicas derivadas de la tesis doctoral. Estos objetivos están relacionados con el manejo de datos personales y el uso de dispositivos digitales, considerando variables como el género, la formación académica y la experiencia docente, que se abordan en cada una de las contribuciones de la presente tesis.

CAPÍTULO 2. MARCO TEÓRICO

2.1 Habilidades tecnológicas esenciales para el mundo actual

El mundo está cambiando a un ritmo vertiginoso, impulsado en gran medida por el creciente uso y la dependencia de las tecnologías digitales, lo que ha traído consigo cambios significativos en la sociedad actual. El desarrollo de habilidades tecnológicas se considera esencial para participar activamente en la sociedad, contribuir al desarrollo sostenible, y adaptarse a un mundo en constante cambio. Esta Transformación Digital no es un proceso nuevo; hay que tener en cuenta que sus raíces se remontan al concepto de digitalización, el cual mantiene una estrecha relación con la conversión de datos y la actualización de procesos analógicos en sus equivalentes digitales (Aras & Büyüközkan, 2023).

La tecnología se ha ido incorporado de manera integral en la sociedad del conocimiento, moldeando de manera significativa el comportamiento de los individuos. Hace unos años algunos autores aludían a una transición social hacia la Cuarta Revolución Industrial, en la cual la mayoría de los empleos del futuro demandarían competencias digitales, requiriendo ciudadanos con habilidades relacionadas con estas, para la realización de sus funciones (Brugia & Zukersteinova, 2019; Williamson et al., 2019).

En cierto modo, es probable que la actual sociedad se encuentre inmersa en esta nueva etapa y por ello, es fundamental que desde el sistema educativo se promueva el uso seguro de la tecnología, integrándola con métodos pedagógicos innovadores, convirtiéndola en un recurso clave para optimizar el proceso de enseñanza y aprendizaje, así como para la difusión del conocimiento y conseguir una sociedad digitalmente alfabetizada y competente (Cabero Almenara et al., 2020).

El incremento de la demanda de aprendizaje en línea unido al crecimiento acelerado son consecuencia inevitable en la sociedad moderna; una sociedad en la que creatividad y tecnología se convierten en el eje principal para un avance social sólido. Hoy en día, es evidente que el aprendizaje y transmisión de conocimientos no se limita únicamente a los centros

educativos, sino que este proceso de aprendizaje se ha visto significativamente apoyado por el uso de las tecnologías fuera del contexto educativo tradicional (Ngoc et al., 2020).

Sin embargo, este rápido desarrollo de las tecnologías emergentes en el ámbito educativo genera al unísono entusiasmo e inquietud, y es que aunque su capacidad para revolucionar los métodos de enseñanza y aprendizaje ha quedado sobradamente demostrada, también es crucial enfrentarlas con cautela, pero sin dejar de explorar las nuevas oportunidades (de Souza Zanirato Maia et al., 2023).

El enfoque de la enseñanza tradicional y unidireccional, donde el conocimiento se centraba únicamente en el docente, está cada vez más en desuso. Esto hace necesario avanzar hacia modelos más flexibles en los que los docentes actúen como guías, promoviendo la autonomía de cada alumno en su proceso de aprendizaje, y es aquí donde cada vez más las tecnologías de la información y la comunicación desempeñan un papel muy relevante, facilitando el desarrollo de la autonomía en cada estudiante y alentando una participación e individualización de los aprendizajes. En este contexto, la competencia digital se convierte en una herramienta óptima para ofrecer una educación cada vez más flexible, innovadora y segura, que permita integrar el uso de dispositivos tecnológicos, la comunicación digital y el intercambio de información de forma segura y responsable en diversos contextos sociales (Flores-Tena et al., 2021).

Otra de las apariciones digitales que se consolidan con fines educativos en la actualidad, es el uso de tecnologías emergentes como la Inteligencia Artificial (IA) y la Inteligencia Artificial Generativa (IAGen). Estas herramientas continúan transformando digitalmente la sociedad y por ende los entornos educativos. Hay evidencias que demuestran que el uso combinado de la tecnología de forma segura, contribuye significativamente a la mejora y evolución de diversos procesos educativos (Sosa Neira et al., 2017). Este nuevo escenario ofrece un amplio abanico de posibilidades, por lo que es fundamental que tanto la sociedad en general como los docentes en particular se capaciten y adquieran las citadas competencias. De esta

manera, podrán complementar sus conocimientos con las oportunidades que estas tecnologías ofrecen, asegurando que sus decisiones sean seguras, éticas y responsables (García-Peñalvo & Vázquez-Ingelmo, 2023).

En contraposición, hay que considerar que la digitalización al igual que cualquier otro proceso puede traer consigo ciertos inconvenientes o deficiencias derivados de un mal uso. Sin embargo, conviene recordar que muchos de estos problemas presentes en el ámbito educativo y que en la actualidad se relacionan directamente con un uso deficiente de la tecnología, ya nos acompañaban tiempo atrás, por lo que no han sido exclusivamente provocados por las tecnologías emergentes, sino que simplemente la velocidad y el alcance actual de estas herramientas los están agravando. A medida que avanzamos en este nuevo entorno tecnológico, debemos equilibrar su exploración con un firme compromiso hacia la ética y la equidad, garantizando que la educación futura se beneficie de una tecnología segura sin sucumbir a sus posibles riesgos (García-Peñalvo, 2024).

En este sentido, resulta indispensable que los docentes comprendan cómo aplicar estas nuevas herramientas en diversos contextos educativos, y que las administraciones adquirieran un serio compromiso que permita avanzar hacia la transformación digital educativa de forma segura. A pesar de los desafíos que acompañan al rápido desarrollo de estas tecnologías, gran parte del profesorado reconoce su potencial para mejorar la colaboración, interacción y comunicación, entre otros aspectos, dentro del contexto educativo.

Por todo ello, adquiere especial relevancia la necesidad de implementar enfoques pedagógicos innovadores, que promuevan la convivencia entre las teorías de aprendizaje actuales y tradicionales, con la tecnología; logrando una enseñanza verdaderamente transformadora y segura; fortaleciendo la capacidad de los docentes para dominar la digitalización de manera responsable (Benavides et al., 2020).

2.2 Competencia digital docente en el área de seguridad digital

El desarrollo de las competencias digitales son una prioridad en la agenda política de la Unión Europea, que busca impulsar las habilidades necesarias para la transformación digital. A través de la Estrategia de Competencias Digitales y otras iniciativas políticas, la UE se enfoca en la mejora de las capacidades digitales tanto en la vida cotidiana como en el ámbito laboral. La Agenda Europea de Capacidades, lanzada el 1 de julio de 2020, apoya el desarrollo de competencias digitales para todos y refuerza los objetivos del Plan de Acción de Educación Digital, centrados la mejora de las habilidades digitales y la creación de un sistema educativo digital avanzado. Además, la Brújula Digital y el Plan de Acción del Pilar Europeo de Derechos Sociales han establecido metas ambiciosas para 2030, como el logro de que al menos el 80% de la población tenga competencias digitales básicas, así como contar con 20 millones de especialistas en TIC (EUROPEA, 2021).

El incremento de amenazas y riesgos cibernéticos, el avance de la inteligencia artificial anteriormente mencionada, unidos al creciente problema del ciberacoso, y la proliferación del uso de las redes sociales y dispositivos móviles por parte de población infantil y adolescentes, está generado una preocupación significativa en la sociedad. De ahí la necesidad urgente de proteger la privacidad de las personas (Gümüş et al., 2023) e intensificar la formulación de estrategias robustas y efectivas para mejorar la seguridad digital. Estas estrategias no solo buscan mitigar los peligros asociados con el ciberacoso y la exposición temprana a tecnologías, sino también establecer mecanismos de protección avanzados que aborden las complejidades emergentes de la inteligencia artificial y las vulnerabilidades de la privacidad en entornos digitales. La combinación de estos factores subraya la importancia de un enfoque integrado y multidisciplinar en la creación de políticas y prácticas que garanticen la seguridad y el bienestar de los usuarios en la era digital.

La competencia digital implica el dominio de habilidades cognitivas, actitudinales y técnicas que contribuyen al afrontamiento de los desafíos que acontecen en la actual sociedad del conocimiento. Pero ser competente digitalmente no solo consiste en utilizar las tecnologías de manera adecuada, sino que también implica un uso responsable, crítico y ético (Gallego-Arrufat et al., 2019). Esta competencia, de naturaleza dinámica y transversal, es esencial para el desarrollo de la ciudadanía digital, además resulta fundamental en los procesos de aprendizaje a lo largo de la vida (Ferrari & Punie, 2013). Por tanto, usar las tecnologías digitales de forma competente en diferentes ámbitos de la vida, conlleva la capacidad de recuperar, evaluar, almacenar, producir, presentar e intercambiar información; comunicarse y colaborar en redes a través de Internet. Asimismo, si tenemos en cuenta el trabajo como docente, se requiere el dominio y la aplicación de herramientas y dispositivos tecnológicos, informacionales, multimedia y comunicativos, que garanticen un uso crítico, responsable y creativo de la tecnología por parte de su alumnado; los cuales resultan fundamentales para el aprendizaje y la participación en la sociedad del siglo XXI (Esteve-Mon et al., 2016).

Una de las áreas fundamentales sobre las que se asienta la competencia digital es la seguridad. En el contexto de las Tecnologías de la Información y la Comunicación (TIC) el concepto de seguridad se puede entender como la protección de la información y la comunicación de los usuarios frente a los problemas derivados del uso de las tecnologías. Esta protección queda estrechamente vinculada con la privacidad, la integridad, la eficiencia de la tecnología y la información en Internet (Anderson, 2003).

En la actualidad, las investigaciones relacionadas con la competencia en seguridad digital en cuestión son menos abundantes si los comparamos con aquellos estudios centrados en la competencia digital ciudadana y la competencia digital docente (Bong & Chen, 2024; Brevik et al., 2019; Cabero-Almenara et al., 2022; Guillén-Gámez et al., 2024). En particular, la competencia digital docente ha sido objeto de un mayor número de análisis, principalmente en contextos universitarios y desde la perspectiva de la

formación inicial del profesorado. Esto resalta una brecha en la investigación sobre la seguridad digital desde el ámbito de la enseñanza primaria, un aspecto que ha cobrado una relevancia significativa, especialmente a raíz de la pandemia de la COVID-19 y sus múltiples repercusiones. Esta crisis sanitaria global provocó una aceleración en el proceso de digitalización de la educación, exponiendo tanto a estudiantes como a docentes a nuevos riesgos y desafíos en términos de seguridad en línea.

En los últimos años el estudio de la competencia en seguridad digital, ha mostrado un crecimiento notable, lo que subraya su creciente importancia e influencia en los resultados educativos (Gallego-Arrufat et al., 2019; Grande de Prado et al., 2021; Khan et al., 2023; Torres-Hernández & Gallego-Arrufat, 2022). Sin embargo, la mayoría de las investigaciones se han centrado en analizar a estudiantes de programas universitarios relacionados con la educación, los cuales preferentemente han tratado de identificar una serie de deficiencias en su formación y que quedan vinculadas a la seguridad digital.

En el ámbito educativo, la competencia en seguridad digital se refiere a aquellas actitudes, conocimientos y habilidades, que los docentes deben poseer para diseñar y desarrollar experiencias de aprendizaje que promuevan, modelen y formen a los estudiantes que contribuyan al desarrollo de una sociedad digitalmente segura y responsable (Gallego-Arrufat et al., 2019). Asimismo, esta competencia se vincula con conceptos como la privacidad, la integridad, la eficiencia y la optimización de la información y de la tecnología derivada del uso de Internet (Honig & Salmon, 2021).

En este contexto, la competencia digital se ha consolidado como un elemento clave en la educación y formación a nivel global. Este reconocimiento ha impulsado el desarrollo de varios marcos internacionales, con la Unión Europea a la vanguardia en la creación de guías detalladas para fomentar dicha competencia. Entre estos se destacan el Marco Europeo de Competencia Digital para la Ciudadanía DigComp 2.2 (Vuorikari Rina et al., 2022), el Marco Europeo para la Competencia Digital Docente

DigCompEdu (Redecker, 2017), y el Marco Europeo para Organizaciones Educativas Digitalmente Competentes DigCompOrg (Kampylis et al., 2015).

Estos marcos han buscado dotar a los individuos de las habilidades y capacidades necesarias para utilizar las tecnologías de manera efectiva y eficiente, al tiempo que promueven una comprensión profunda de su impacto en diversos contextos sociales, educativos y laborales. Su principal objetivo es preparar a la sociedad para desenvolverse con éxito en un entorno digital en constante evolución, equipándola para enfrentarse a los desafíos tecnológicos presentes y futuros. La competencia digital, por tanto, se convierte en un requisito indispensable para la plena participación en la sociedad contemporánea, permitiendo a los ciudadanos navegar con seguridad en un mundo cada vez más digitalizado. Además, la integración de estos marcos en la formación educativa asegura que tanto docentes como estudiantes estén preparados para ofrecer respuestas eficaces y competentes a los retos planteados en los entornos digitales del siglo XXI, promoviendo un uso ético, crítico y creativo de las tecnologías en todos los ámbitos de la vida. Esta preparación es esencial no solo para el desarrollo personal y profesional, sino también para garantizar que la tecnología sea utilizada de manera que beneficie a la sociedad en su conjunto, respetando los principios de seguridad, privacidad y equidad.

Un aspecto prioritario y cada vez más solicitado dentro de la competencia digital es la seguridad en el entorno digital que abarca entre otros la evaluación de fuentes confiables y no confiables. Para ello es importante considerar varios criterios como la autoría, comprobando si el autor es un experto en el tema; la afiliación, si la fuente está respaldada por una institución de prestigio; la fecha de publicación, asegurándose que la información esté actualizada; la presencia de referencias, que nos informa sobre trabajos reconocidos; la imparcialidad, evitando fuentes claramente sesgadas; la revisión por pares, especialmente en publicaciones académicas, y el dominio del sitio web, dando preferencia a dominios como .gov, .edu o .org, aunque siempre con cautela.

Otro de los puntos importantes es la implementación de medidas de seguridad adicionales más allá de las contraseñas entre las que se destaca la autenticación de dos factores (2FA), que requiere un segundo paso de verificación; el uso de biometría, como huellas dactilares o reconocimiento facial; las llaves de seguridad físicas, dispositivos USB o Bluetooth para autenticación; la encriptación de datos para proteger la información; los gestores de contraseñas que generan claves complejas; el acceso mediante tokens de hardware o software; la actualización regular del software para prevenir vulnerabilidades y el monitoreo de actividad para detectar comportamientos sospechosos.

La colaboración entre todos los miembros de la comunidad educativa en estas prácticas puede fortalecer la defensa contra los riesgos en los entornos digitales, proporcionando protección tanto a nivel individual como colectivo.

2.3. Marcos de competencia digital

2.3.1 Marco Europeo para la Competencia Digital de los Educadores (DigCompEdu)

La expansión masiva de las tecnologías digitales ha transformado profundamente casi todos los aspectos de nuestras vidas: la comunicación, el trabajo, el modo en que disfrutamos de nuestro tiempo libre, cómo organizamos nuestras rutinas diarias y sobre todo la forma en que accedemos al conocimiento y la información. Aunque no es menos cierto que nuestro pensamiento, análisis y actuaciones en consonancia también han influido. Esta rápida implementación de las TIC en las instituciones educativas continúa planteando desafíos para la alfabetización digital de los docentes, debido a que el avance tecnológico supera con creces el tiempo necesario para su adaptación (Martínez & López Fernández, 2015)

Hoy día la población infantil y juvenil crece en un entorno donde las tecnologías digitales están en todas partes, sin haber conocido una realidad diferente. Los estudiantes, a menudo considerados "nativos digitales",

poseen habilidades tecnológicas que superan en ocasiones con creces a las de sus profesores, quienes son vistos como "inmigrantes digitales" y, en el mejor de los casos, han sido "realfabetizados". Estas categorías fueron reavivadas por Prensky (2001), sosteniendo que las diferencias entre los estudiantes y sus docentes son una de las principales causas de los desafíos actuales en el ámbito educativo y planteando la más que probable hipótesis de que los cerebros de los nativos digitales se hayan desarrollado de manera diferente debido a la exposición constante a la tecnología desde edades tempranas. No obstante, esto no implica que se conviertan en adultos con habilidades innatas necesarias para usar estas tecnologías de manera eficaz y consciente (Rodriguez Carracedo & de la Barrera Minervini, 2014).

Como resultado, surge la necesidad de equipar a todos los ciudadanos con las habilidades esenciales para utilizar las tecnologías de manera crítica y creativa. El Marco Europeo de Competencia Digital (DigComp 2.2), en el cual se profundizará más adelante, aborda esta demanda, proporcionando una estructura que ayuda a la sociedad a comprender qué significa ser competente en el ámbito digital, así como a evaluar y mejorar su propia competencia digital (Vuorikari Rina et al., 2022).

Para los estudiantes en la educación obligatoria, existe una amplia variedad de iniciativas europeas, nacionales y regionales que ofrecen directrices y recomendaciones sobre cómo capacitar a los jóvenes en el desarrollo de su competencia digital, con un énfasis frecuente en el pensamiento crítico y la ciudadanía digital. En la mayoría de los países miembros de la Unión Europea, se han diseñado o están en proceso de elaboración planes de estudios necesarios que garanticen que la nueva generación pueda participar de manera creativa, crítica y productiva en una sociedad cada vez más digitalizada.

El Marco Europeo para la Competencia Digital de los Educadores (DigCompEdu) surge en respuesta al creciente reconocimiento por parte de numerosos Estados miembros de la Unión Europea de que los docentes adquieran un conjunto específico de competencias digitales, el cual les permita utilizar de manera efectiva las tecnologías digitales y, de ese modo,

impulsar la innovación, el rigor y el progreso en el ámbito educativo. Por tanto, el DigCompEdu ofrece un análisis de los recursos disponibles relacionados con la competencia digital de los docentes y los unifica en un modelo coherente, el cual les permite evaluar y mejorar de manera integral sus habilidades digitales pedagógicas.

Además, el valor añadido del citado marco radica en su capacidad para proporcionar una base robusta que guíe las políticas educativas en todos los niveles, un modelo adaptable que permite a las partes interesadas locales desarrollar rápidamente herramientas concretas ajustadas a sus necesidades, así como un lenguaje y una lógica común que facilita el intercambio de buenas prácticas. Asimismo, ofrece un punto de referencia para que puedan validar la coherencia y el enfoque de sus propios marcos y herramientas, tanto actuales como futuros.

Figura 1. Áreas y alcance del marco DigCompEdu.

Fuente: *DigCompEdu 2.2 (Redecker, 2020)*

Este modelo de competencia digital para docentes diferencia seis áreas competenciales:

1. **Compromiso profesional:** Esta área se enfoca en el entorno laboral de los docentes, destacando la capacidad de utilizar tecnologías digitales no solo para mejorar la enseñanza, sino también para

interactuar profesionalmente con amistades, estudiantes, familias y otros miembros de la comunidad educativa. Este ámbito representa el núcleo profesional, abarcando las competencias esenciales que los docentes deben desarrollar en un entorno educativo comprometido con la Sociedad del Conocimiento. Son diferentes los estudios que apoyan la importancia dominar el uso de bases de datos, la nube para almacenar información o la creación de repositorios digitales entre otros para fomentar la creación a través de la cooperación y la colaboración (de Oca et al., 2015; Montoya et al., 2018). Otros aseguran que los recursos digitales son usados principalmente para comunicarse con otros docentes, compartiendo información, experiencias e inquietudes. Entre estas herramientas destacan foros, debates virtuales y blogs (Suárez-Carballo, 2020).

2. **Recursos digitales:** Relacionada con la identificación, creación y distribución de material digital, por ello es de vital relevancia que los docentes sean capaces de seleccionar recursos educativos de calidad, adaptarlos, crearlos y compartirlos para que se alineen con sus objetivos pedagógicos y estilos de enseñanza, respetando al mismo tiempo los derechos de autor y protegiendo tanto dispositivos como datos personales. En este sentido, algunos estudios indican que los docentes tienen un alto nivel de competencia en la búsqueda y organización de información, mientras que otros destacan que los profesores emplean herramientas, programas y aplicaciones adicionales, como Kahoot, para recopilar y compartir la información (de Oca et al., 2015; Grisales & Palacio, 2019; Montoya et al., 2018). Esta área forma parte del núcleo pedagógico del marco, enfocándose en cómo los docentes pueden integrar estos recursos en los procesos de enseñanza y aprendizaje.

3. **Pedagogía digital:** Se refiere a la capacidad de diseñar, planificar e implementar tecnologías digitales de forma segura en todas las etapas del proceso de enseñanza y aprendizaje, promoviendo un enfoque didáctico y metodológico centrados en el alumnado. A colación, son diversos los estudios que resaltan la integración de

recursos digitales por parte del profesorado para mejorar significativamente los procesos de enseñanza-aprendizaje, donde destaca Moodle como una de las plataformas más utilizadas. Además, defienden la implementación de diversas técnicas y metodologías de aprendizaje para optimizar la enseñanza de procesos educativos, fomentando el uso de competencias tecnológicas. Entre estas metodologías se incluyen el aprendizaje colaborativo, cooperativo, basado en proyectos, en problemas, y el uso de debates (de Oca et al., 2015; Durán, 2019; Grisales & Palacio, 2019; Montoya et al., 2018; Petelin et al., 2019; Ríos Ariza et al., 2018). Al igual que la anterior área, esta es parte del núcleo pedagógico, quedando directamente vinculada a la mejora de estrategias educativas mediante la integración de herramientas digitales.

4. **Evaluación y retroalimentación:** Esta área se ocupa del uso de herramientas y estrategias digitales para evaluar y mejorar los procesos educativos, que permiten la implementación de métodos de evaluación más efectivos e innovadores. Diferentes trabajos destacan el potencial de las competencias tecnológicas para optimizar la evaluación y la retroalimentación, beneficiando tanto a profesores como a estudiantes. Además, se evidencia la efectividad de un buen nivel de competencia digital en la realización de evaluaciones formativas y sumativas de manera eficiente (Barroso Osuna et al., 2019; Habibi et al., 2019; Montoya et al., 2018). Esta área también se identifica con el núcleo pedagógico del marco, pues se enfoca en cómo las tecnologías digitales pueden transformar las evaluaciones convirtiéndose en un proceso de carácter dinámico y personalizado.
5. **Empoderar a los estudiantes:** Enfatiza el potencial de las tecnologías digitales para fomentar la participación activa y autónoma de los estudiantes en el proceso de enseñanza y aprendizaje, ofreciendo actividades adaptadas a sus niveles de competencia, intereses, motivaciones y necesidades. En esta misma línea, algunos autores sostienen que el uso de estas herramientas permite a los profesores una mejor gestión del tiempo, la captación de la atención

de los estudiantes y el incremento de su participación (Grisales & Palacio, 2019; Habibi et al., 2019; Rodríguez, 2019). Sin embargo, la falta de conocimiento por parte de los docentes en el manejo de estas tecnologías puede llevar a un uso inadecuado, generando malestar entre los estudiantes al afectar a la secuencia y el ritmo de las clases (Montoya et al., 2018).

El área destaca el cómo las herramientas digitales pueden transformar el rol de los estudiantes en su propio proceso de aprendizaje, siendo parte del núcleo pedagógico.

6. **Facilitar la competencia digital de los estudiantes:** finalmente esta área se centra en el desarrollo y promoción de la competencia digital ciudadana entre el alumnado. Son varios los estudios que confirman que las actividades que incorporan el uso de competencias tecnológicas en el aula facilitan el acceso rápido a la información por parte del alumnado, lo que a su vez potencia el máximo desarrollo de las habilidades investigativas a través de estas herramientas (Del Valle et al., 2018; Gómez, 2017).

   Finalmente, este ámbito se orienta a que los estudiantes desarrollen las competencias necesarias para convertirse en ciudadanos digitales responsables y seguros, estructurándose de acuerdo con el Marco de Competencia Digital para Ciudadanos (DigComp 2.2).

Figura 2. Competencias DigCompEdu y sus conexiones.

Fuente: *DigCompEdu (Redecker, 2020)*

2.3.2 Marco de Competencias Digitales para la Ciudadanía (DigComp)

Desde el lanzamiento de la primera versión del Marco de Competencia Digital Europeo, conocido como DigComp (Ferrari & Punie, 2013), que surgió tras la inclusión de las competencias digitales como una de las ocho categorías establecidas por el Parlamento Europeo en 2006, se han producido varias actualizaciones. La versión inicial delineaba cinco dominios de competencia, basados en un documento previo de la UNESCO (United Nations, 2011) que eran: Información, Comunicación, Creación de Contenido, Seguridad y Resolución de Problemas. Cada dominio comprendía 21 competencias específicas y ofrecía tres niveles de habilidad (básico, intermedio y avanzado). La primera revisión del DigComp 2.0 solo modificó algunos nombres de áreas, sino que también incorporó ejemplos de aplicación en distintos países europeos, incluido España, y una lista de conceptos esenciales (Vuorikari et al., 2016). La versión siguiente; DigComp 2.1 introdujo cuatro niveles de habilidad, subdivididos en dos niveles adicionales, sumando un total de ocho niveles (Carretero et al., 2017). Actualmente, el marco está siendo adaptado a distintos contextos profesionales, incluyendo el ámbito educativo (Redecker, 2017). La presente propuesta presentada a continuación se ha ajustado para docentes y se basa principalmente en la última versión del DigComp 2.2 (Vuorikari Rina et al., 2022), la cual clasifica cada competencia en 8 niveles de dificultad. Aunque se ha tenido en cuenta el DigCompEdu y el DigCompOrg, no se ha seguido estrictamente, ya que el rol del docente incluye funciones adicionales a las meramente didácticas.

El Marco de Competencias Digitales para la Ciudadanía, conocido como DigComp, es una herramienta de la Unión Europea que ofrece un lenguaje común para identificar y describir las competencias digitales clave. Su objetivo es mejorar las habilidades digitales de la ciudadanía, ayudar a los responsables de las administraciones en la creación de políticas que fomenten el desarrollo de estas competencias y guiar iniciativas de educación y formación dirigidas a grupos específicos.

El informe sobre la versión 2.2 del DigComp (Vuorikari Rina et al., 2022) presenta una actualización de los ejemplos de conocimientos, habilidades y actitudes necesarias. Además, reúne los principales documentos de referencia para apoyar su implementación efectiva e identifica cinco áreas clave que definen la competencia digital como son: Búsqueda y gestión de información y datos, Comunicación y colaboración, Creación de contenidos digitales, Seguridad y Resolución de problemas.

Las tres primeras áreas se centran en competencias asociadas con actividades desarrolladas de forma específica en entornos digitales. En contraposición, las áreas de Seguridad y Resolución de problemas destacan por presentar un carácter transversal, pudiendose aplicar a cualquier actividad digital desarrollada por los usuarios en los diferentes ámbitos necesarios para su progreso en actuaciones relacionadas con su vida cotidiana.

Figura 3. El modelo de referencia conceptual de DigComp

Fuente: *Digcomp 2.2* (Vuorikari Rina et al., 2022)

A continuación, se profundiza en las 4 dimensiones del área de seguridad digital como son la protección de dispositivos, la protección de datos personales y privacidad, la protección de la salud y del bienestar y la protección medioambiental, con el objetivo de describir y analizar de forma breve el recorrido por los diferentes niveles e indicadores que implica cada una de estas dimensiones y por ende, la contribución a la creación de una sociedad digital y competentemente segura.

La **protección de dispositivos** se caracteriza por una implementación de medidas y prácticas que permiten salvaguardar los datos personales y la privacidad en entornos digitales. Esto implica aprender a usar contraseñas seguras, nociones básicas sobre firewall, antivirus y herramientas de detección de intrusos, así como la comprensión de cómo compartir la información personal de manera segura a través de dispositivos usados en el día a día.

El desarrollo de competencias digitales abarca una progresión que va desde habilidades básicas hasta capacidades altamente especializadas. En los **niveles básicos (1 y 2)**, una persona, con orientación o de manera autónoma, puede identificar y aplicar medidas sencillas para proteger dispositivos y contenidos digitales. Esto incluye diferenciar riesgos y amenazas simples, elegir medidas básicas de seguridad y protección, y tener en cuenta la fiabilidad y la privacidad de la información en entornos digitales. La principal diferencia entre dichos niveles radica en el grado de independencia, así el nivel 2 permite una mayor autonomía mientras se mantiene la posibilidad de recibir orientación cuando sea necesario.

En contraste, los **niveles altamente especializados (7 y 8)**, la persona tiene la capacidad de desarrollar soluciones avanzadas para problemas complejos que involucran múltiples factores interrelacionados en la protección de dispositivos y contenidos digitales. Esto incluye la gestión de riesgos y amenazas, la aplicación de medidas de seguridad y protección, y la fiabilidad y privacidad en entornos digitales. Además, en el nivel 8, se espera que la persona proponga nuevas ideas y procesos innovadores para mejorar las prácticas en el sector y guiar a otros en la protección de dispositivos.

La **protección de datos personales y privacidad** tiene como finalidad lograr la comprensión del cómo utilizar y cómo y con quién compartir la información personal que identifica a cada individuo, con el propósito de protegerse a sí mismo y al resto de la comunidad ante posibles daños ocasionados por una mala praxis docente. Ello supone una lectura minuciosa que facilite la comprensión de la política de privacidad que los servicios digitales utilizan para informar sobre el uso y finalidad de los datos personales que se comparten.

La adquisición de competencias digitales en el ámbito de la protección de datos personales y la privacidad en entornos digitales sigue una trayectoria progresiva que va desde habilidades básicas hasta capacidades altamente especializadas. En los **niveles básicos (1 y 2)**, los usuarios a través de una orientación adecuada o de manera autónoma, deben ser capaces de seleccionar métodos simples para proteger los datos personales y su privacidad en entornos digitales. Esto incluye identificar formas seguras de utilizar y compartir información identificable para evitar daños, así como comprender políticas básicas de privacidad en servicios digitales.

En los **niveles altamente especializados (7 y 8)**, la persona tiene la capacidad de desarrollar soluciones avanzadas para problemas complejos relacionados con la protección de datos personales y la privacidad, abordando múltiples factores interrelacionados. Estos niveles implican la integración de conocimientos para contribuir a la práctica profesional, guiar a otros en la protección de datos y proponer innovaciones en el sector. En el nivel 8, se espera además la creación de nuevas ideas y procesos que optimicen la protección de datos y la privacidad en entornos digitales.

El trayecto desde los niveles básicos hasta los especializados demuestra una progresión desde la aplicación de medidas sencillas hasta la capacidad de resolver problemas complejos, liderar e innovar en el ámbito de la protección de datos y privacidad.

La **protección de la salud y del bienestar** favorece el desarrollo de capacidades que previenen riesgos para la salud tanto física como mental

mientras se hace uso de las tecnologías digitales. Para ello se hace indispensable adquirir una serie de habilidades y estrategias que permitan la protección eficaz de sí mismos y de otros ante los riesgos en los entornos digitales.

El desarrollo de competencias digitales relacionadas con la salud y el bienestar requiere de un punto de partida que comienza con la adquisición de habilidades fundamentales y continúa en su vía hacia capacidades más avanzadas y especializadas.

En los **niveles básicos (1 y 2),** una persona es capaz de identificar y diferenciar formas sencillas de evitar riesgos para la salud y amenazas al bienestar físico y psicológico mientras utiliza tecnologías digitales. Además, puede seleccionar métodos simples para protegerse de peligros en entornos digitales y reconocer tecnologías digitales que promuevan el bienestar social y la inclusión.

Por otro lado, en los **niveles altamente especializados (7 y 8),** la persona adquiere la capacidad de desarrollar soluciones avanzadas para problemas complejos y multifactoriales relacionados con la salud, el bienestar, y la seguridad en entornos digitales. Estos niveles también implican la integración del conocimiento para contribuir profesionalmente, guiar a otros en la protección de la salud digital, y proponer innovaciones que mejoren el bienestar social e inclusión a través de la tecnología. El último de ellos (nivel 8) se distingue por su enfoque en la creación de soluciones que aborden interacciones complejas entre múltiples factores, y en la generación de nuevas ideas y procesos dentro del sector.

La **protección medioambiental** queda asociada a la consciencia del impacto que produce el uso de las tecnologías digitales, entendiendo cómo afecta al medioambiente y favoreciendo prácticas sostenibles que ayuden a minimizar dichos niveles. Para ello, es importante crear conciencia energética eficiente implementando dispositivos y prácticas que reduzcan el consumo de energía, contribuyendo a la sostenibilidad ambiental. Asimismo, es crucial minimizar los desechos de los dispositivos electrónicos a través

del reciclaje, promoviendo la reutilización y el reciclaje adecuado de estos aparatos. La sostenibilidad en la nube a la hora de elegir servicios de almacenamiento y procesamiento que utilicen fuentes de energía renovable y adopten prácticas ecológicas es otra de las estrategias a tener en cuenta. Además, hoy día la educación ambiental es esencial para concienciar al alumnado sobre el impacto de sus acciones digitales en el medioambiente, creando comportamientos responsables y sostenibles.

La adquisición de estas competencias medioambientales requiere del paso necesario por una serie de grados, desde los **niveles básicos (1 y 2)**, donde una persona, con cierta orientación o de manera autónoma, es capaz de reconocer los impactos medioambientales simples asociados con las tecnologías digitales y que son derivadas de su uso.

En los **niveles altamente especializados (7 y 8)**, la persona debe ser capaz de desarrollar soluciones avanzadas para problemas complejos relacionados con la protección del medioambiente frente al impacto de las tecnologías digitales. Estos niveles implican la capacidad de integrar conocimientos para contribuir a la práctica profesional y guiar a otros en la protección medioambiental. En el nivel 8, se espera además la creación de soluciones que aborden factores interrelacionados y la propuesta de nuevas ideas y procesos innovadores dentro del sector para mitigar el impacto ambiental de las tecnologías digitales.

Este recorrido parte de los niveles básicos hasta los altamente especializados en competencias digitales y refleja una progresión desde la simple identificación de impactos ambientales hasta la capacidad de innovar y liderar en la protección del medioambiente frente a los desafíos que plantea el uso de tecnologías digitales.

Si tenemos en cuenta las competencias anteriormente citadas, el papel del docente es muy relevante, ya que ofrece un modelo, que lo convierte en el guía involucrado en cuidar, orientar y educar para un uso responsable y sostenible durante la navegación, la comunicación y la colaboración en línea, así como sobre la compartición de datos. Sin embargo, a esto le acompaña

un importante desafío, la erradicación de las concepciones erróneas que pueden tener algunos docentes, quienes, frecuentemente, abordan la seguridad digital de manera superficial, limitándose a ofrecer nociones básicas sobre problemáticas diferidas del uso Internet en lugar de profundizar en innovadoras prácticas seguras y necesarias (Cain et al., 2018).

A pesar de que ha habido un creciente interés en el tema, se consideran escasos los estudios enfocados en los docentes activos que imparten enseñanzas en centros educativos de educación primaria y secundaria. Las principales líneas de investigación destacan la relación entre la competencia digital ciudadana y la competencia digital docente (Chong & Pao, 2022; Ivy et al., 2019; Méndez et al., 2021). Por ello se considera fundamental entender cómo estas dos competencias quedan interrelacionadas, ya que un profesorado bien preparado digitalmente puede influir positivamente en el desarrollo de estas habilidades en su alumnado. Además, la formación continua del profesorado es esencial para asegurar que estén actualizados en relación con las nuevas tecnologías y metodologías educativas activas e innovadoras, lo que a su vez puede mejorar la calidad de la educación y preparar mejor a los estudiantes.

2.3.3 Marco Europeo para Organizaciones Educativas Digitalmente Competentes (DigCompOrg)

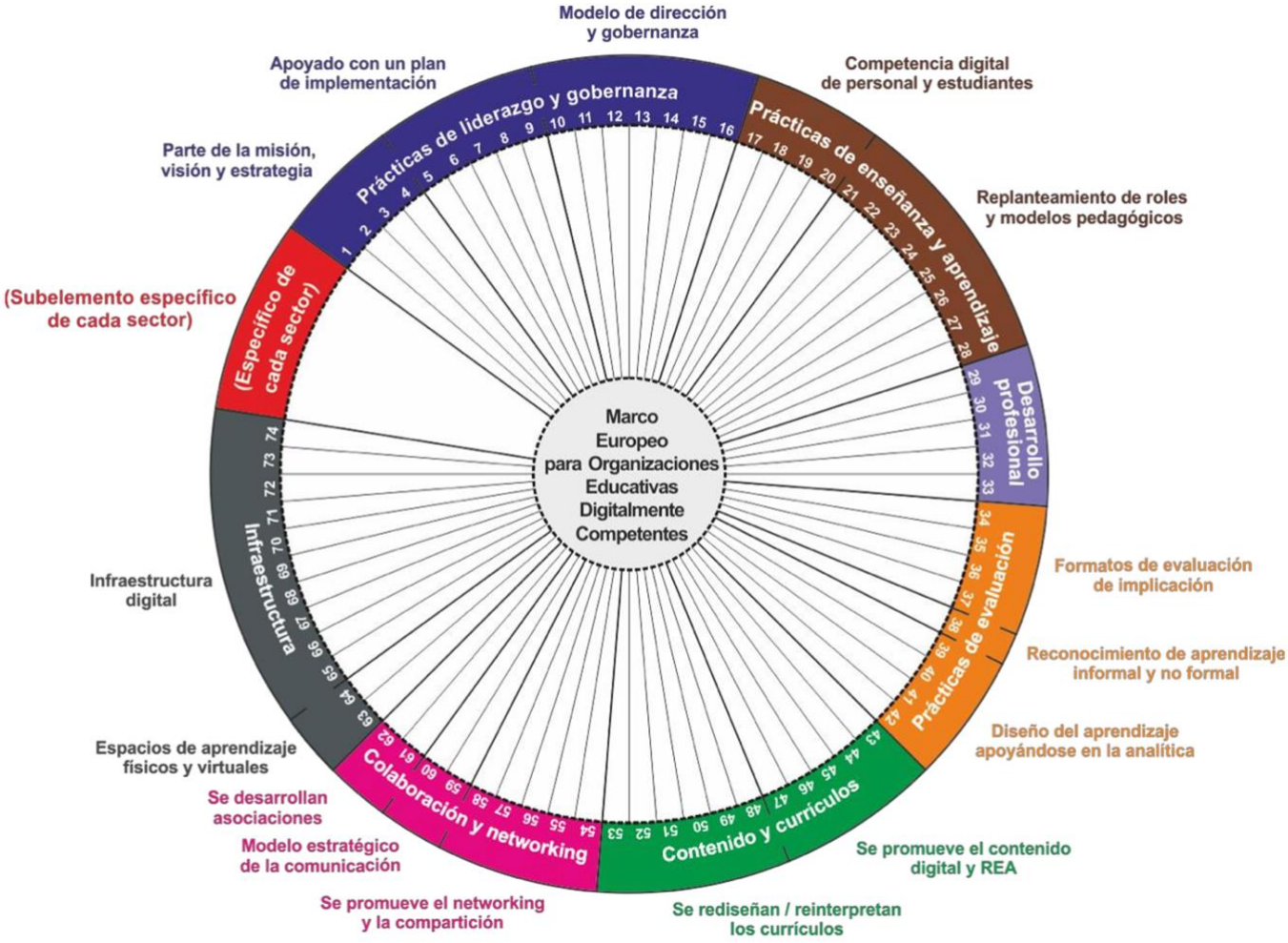
Las tecnologías digitales de uso personal han experimentado una evolución constante, acentuada en la última década, tanto en términos de funcionalidad como de omnipresencia e influencia social. Actualmente, el impacto de las tecnologías, los contenidos y los procesos digitales queda evidenciado en todos los niveles educativos; desde los colegios de educación infantil y primaria hasta las universidades, y por supuesto incluyendo el aprendizaje informal y no formal. Todo ello ha influido en diversos aspectos de la educación como la reforma de los currículos, la innovación de los métodos de enseñanza y aprendizaje, los procesos de evaluación, la formación permanente de los docentes. y por tanto, han

terminado afectando a los diferentes actores involucrados en el proceso, docentes, estudiantes, familias, etc. Esta desbordante y prometedora integración de la tecnología en el ámbito educativo, exige que las instituciones revisen sus estrategias organizativas para impulsar su capacidad de innovación, aprovechando al máximo el potencial de las tecnologías digitales, y de este modo, asegurar un progreso significativo, sostenible y duradero. Las conexiones entre la tecnología, las competencias digitales y las políticas educativas adquieren una creciente importancia en el contexto de la Sociedad del Conocimiento. Las TIC se han convertido en un recurso imprescindible en los centros educativos, donde un adecuado nivel de competencia por parte de docentes y alumnos resulta esencial para garantizar la calidad del proceso de enseñanza-aprendizaje (Scherer et al., 2019; Uerz et al., 2018).

En este contexto, el Marco Europeo para Organizaciones Educativas Digitalmente Competentes (DigCompOrg) destaca entre sus principales objetivos promover la autoevaluación de las organizaciones educativas tras la integración de las tecnologías y modelos pedagógicos digitales, y proporcionar a las autoridades políticas una base para diseñar, implementar y evaluar estrategias de adopción efectiva de tecnologías digitales en la educación a nivel regional, nacional y europeo.

El núcleo del marco se organiza en torno a siete bloques temáticos recogidos en la (Figura 4), los cuales son compartidos por todos los niveles educativos, lo que los convierte en multisectoriales. Cada uno de estos componentes aborda un aspecto distinto del complejo proceso que trata de incorporar y usar de forma efectiva las tecnologías digitales en el aprendizaje. Además, todos se encuentran estrechamente vinculados y deben ser considerados como partes integradas de un conjunto coherente. Además de estos elementos transversales, el DigCompOrg permite la inclusión de componentes específicos adaptados a cada sector educativo.

Figura 4. Elementos y subelementos clave de DigCompOrg



Fuente: DigCompOrg (Kampylis et al., 2015).

1. **Prácticas de liderazgo y gobernanza**

   La relevancia del rol del equipo directivo es altamente influyente en la incorporación y uso efectivo de las tecnologías digitales dentro de las instituciones educativas colegios, institutos, centros de formación, universidades, etc. Para lograr una integración exitosa de estas herramientas, es fundamental partir de un enfoque institucional sólido, el cual debería estructurarse mediante planes estratégicos a corto y medio plazo. El aprendizaje en la era digital, así como la integración de tecnologías digitales, deben estar claramente reflejados en la misión, visión y estrategias de la institución. La misión proporciona una dirección común para individuos y equipos, otorgando coherencia y estructura al proceso de diseñar estrategias, establecer objetivos, realizar tareas y tomar decisiones. Por otro lado, la visión establece

los objetivos futuros de la organización, delineando lo que aspira a ser. Actúa como una guía que motiva e inspira a los equipos a avanzar hacia sus metas. Las estrategias deben ser claras, compartidas y bien comunicadas, además de estar alineadas con la misión y visión de la organización. Esto se traduce en un plan de desarrollo de competencias digitales bien estructurado, con prioridades claras y metas medibles. Asimismo, el liderazgo debe asumir una responsabilidad compartida para coordinar, supervisar y evaluar la eficacia de la integración de las tecnologías digitales en la cultura de la institución educativa.

2. **Prácticas de enseñanza y aprendizaje**

   Este eje temático enfatiza la urgencia de que las instituciones educativas actualicen sus métodos de enseñanza integrando tecnologías digitales como herramientas pedagógicas. El aprendizaje se extiende más allá del entorno escolar, abarcando aspectos de la vida personal, familiar y de ocio. Se promueve la adopción de prácticas pedagógicas innovadoras que utilicen TIC en diversos contextos, tanto dentro como fuera de la escuela, y que cubran tanto la educación formal como la informal. En este contexto, es esencial que tanto estudiantes como docentes desarrollen competencias digitales para un uso efectivo de estas tecnologías. Además, las instituciones tienen la responsabilidad de asegurar un uso seguro y consciente de las TIC, priorizando la seguridad y la comprensión de los riesgos asociados a su empleo.

3. **Desarrollo profesional**

   El desarrollo profesional continuo de los docentes es clave para fomentar pedagogías innovadoras y la adopción de tecnologías digitales en la enseñanza. Es crucial seleccionar áreas de formación que se alineen con los objetivos institucionales. A menudo, la oferta formativa existente no cubre estas necesidades, lo que obliga a la institución a crear o promover programas específicos. Además, se sugiere el uso de modelos de formación mixtos, que incluyan tanto componentes presenciales como virtuales, dentro y fuera de la organización. Para garantizar la efectividad de este desarrollo, es

esencial proporcionar tiempo y recursos adecuados, así como incentivos que motiven a los docentes a participar.

4. **Prácticas de evaluación**

   La evaluación debe ser vista como una herramienta central para el avance institucional. Se debe concebir como un proceso que proporciona retroalimentación valiosa, lo que facilita la mejora continua, especialmente a través de la evaluación formativa. Es importante considerar diferentes enfoques evaluativos, como la autoevaluación y la evaluación entre pares. Las tecnologías digitales ofrecen poderosas herramientas para estos procesos, aportando rapidez, adaptabilidad, retroalimentación inmediata y la capacidad de extender la evaluación más allá del aula, integrándola en los contextos social y familiar. La evaluación digital se convierte en una fuente esencial para mejorar la calidad educativa, y los resultados obtenidos son fundamentales para revisar y rediseñar planes de innovación y mejora.

5. **Contenidos y currículos**

   Las instituciones educativas deben incentivar y facilitar el uso de contenido digital apropiado y accesible, que responda a las necesidades tanto de docentes como de estudiantes. La formación en competencias digitales es esencial, lo que implica que las tecnologías deben ser una parte integral tanto del currículo como de los contenidos educativos. Esto incluye el aprendizaje con y a través de las tecnologías. Según DigCompOrg, las organizaciones deben:

   - Fomentar la creación y consumo de contenido digital tanto transversal como específico para cada materia.
   - Apoyar la identificación y utilización de repositorios de contenido relevantes.
   - Establecer políticas para garantizar que la comunidad educativa esté bien informada sobre la propiedad intelectual y los derechos de autor.
   - Implementar procedimientos claros sobre licencias para contenido, software y recursos adquiridos de proveedores comerciales.

- Promover la creación y el uso de Recursos Educativos Abiertos (REA) y licencias Creative Commons.
- Impulsar el aprendizaje en entornos digitales y fomentar el desarrollo de la competencia digital en todo el currículo.

6. **Colaboración y redes profesionales**

   Fomentar la creación de redes de colaboración y aprendizaje entre profesionales es crucial. Las instituciones deben promover iniciativas que permitan compartir experiencias y conocimientos más allá de las fronteras organizativas. Para lograrlo, es esencial proporcionar las herramientas, la infraestructura y el apoyo necesario para desarrollar una cultura de aprendizaje conectada, que se extienda fuera de los límites de la organización y promueva un aprendizaje continuo y ubicuo.

7. **Infraestructura**

   Las instituciones deben contar con recursos tecnológicos adecuados y una infraestructura digital bien gestionada y planificada. Es fundamental organizar los espacios educativos de manera que faciliten la integración de tecnologías en los diseños pedagógicos, considerando tanto criterios pedagógicos como técnicos. Las decisiones sobre inversión en tecnología, recursos y servicios deben ser tomadas de manera estratégica. Además, es esencial abordar las desigualdades socioeconómicas y proporcionar apoyo adicional a estudiantes con necesidades especiales. Un plan sólido de mantenimiento de los servicios tecnológicos también es clave para asegurar su funcionamiento continuo.

8. **Elementos específicos de cada sector**

   El modelo de DigCompOrg es adaptable y permite la incorporación de elementos específicos que se ajusten a las características únicas de cada contexto educativo. Esto asegura que el marco pueda ser personalizado para responder a las necesidades particulares de cada institución educativa.

2.4. Ética y seguridad en la protección de datos y la privacidad

En la actual era digital, la seguridad y la privacidad de los datos se han convertido en uno de los principales problemas de la sociedad y por ende en un componente esencial para la protección, tanto de la información personal, como profesional. A medida que las interacciones cotidianas y las actividades laborales se asientan progresivamente sobre cimientos digitales, las competencias en seguridad y privacidad se convierten en imprescindibles para permitir a los individuos y organizaciones proteger eficazmente sus datos, entender los riesgos asociados y adoptar medidas preventivas y reactivas ante posibles amenazas.

Aunque la seguridad y la privacidad se muestran como conceptos distintos, se encuentran estrechamente relacionados cuando se contextualizan en la protección de datos. Hoy día, si tenemos en cuenta que la mayoría de las conversaciones son digitalizadas y se almacenan como información, es lícito afirmar que la privacidad de la comunicación personal y la privacidad de los datos personales se consideran parte de la privacidad de la información (Mutimukwe et al., 2020).

Uno de los temas que se analizan más adelante será la formación docente en el área de seguridad, a través del uso seguro, crítico y responsable de las tecnologías digitales (Ferrari & Punie, 2013). Esta formación se considera primordial para poder formar a estudiantes digitalmente competentes en esta área, incluyendo la enseñanza de prácticas seguras en línea, el manejo de datos personales y la protección contra ciberataques debiéndose convertir en una prioridad educativa (Jin et al., 2018). Los docentes necesitan no solo comprender los riesgos asociados al uso de tecnologías digitales, sino también ser capaces de divulgar este conocimiento a sus estudiantes para que puedan aplicarlo en situaciones de su vida cotidiana.

Uno de los problemas asociados a la protección de datos y la privacidad de las personas es la recopilación ilícita de datos personales para fines

comerciales y políticos, destacando la necesidad de que las personas comprendan los riesgos, protejan sus datos y ejerzan sus derechos de privacidad al utilizar servicios en Internet. Muammar et al., (2023) confirman que la comprensión de los usuarios sobre la seguridad de la información personal compartida a través de la red se encuentra muy limitada, llegando a confiar su seguridad a los proveedores de servicios en línea.

Otra de las preocupaciones crecientes relacionada con la privacidad es la suplantación de identidad y el acceso no autorizado a datos personales en entornos educativos digitales. Este problema subraya la necesidad urgente de que tanto estudiantes como docentes sean conscientes de los riesgos asociados y adopten prácticas seguras para proteger su información personal. La suplantación de identidad no solo compromete la privacidad de los individuos, sino que también puede ocasionar el robo de datos sensibles y el aumento de la vulnerabilidad frente a ataques cibernéticos. En este contexto, es esencial la inclusión de prevención de conductas en la alfabetización digital para preparar a los usuarios contra peligros en la era digital (Sonck et al., 2011) promoviendo la educación en ciberseguridad dentro de las instituciones educativas, fomentando la implementación de medidas de protección como la autenticación de dos factores, el uso de contraseñas robustas y la sensibilización sobre la importancia de no compartir información personal en plataformas digitales sin las debidas precauciones. Al abordar estos riesgos de manera proactiva, se puede contribuir a crear un entorno digital más seguro y confiable para todos los actores involucrados en el proceso educativo.

Krutka et al., (2019) anticiparon que los docentes tendrían que abordar en sus aulas cuestiones relacionadas con el uso, la aplicación y la regulación de las redes sociales. Es posible que ese futuro ya haya llegado y con ello un creciente uso de las mismas en la educación, lo cual está revolucionando los procesos de enseñanza y aprendizaje. El aumento en la recopilación y compartición de información personal en plataformas y redes sociales hace imprescindible considerar los factores tanto positivos como negativos que los docentes perciben en relación con la seguridad y privacidad de los datos.

Este cambio genera una constante preocupación entre los docentes en cuanto a la privacidad de los datos y la falta de conocimientos sobre cómo protegerlos (Marín et al., 2023). Por ello, es crucial que los educadores sean conscientes de los beneficios potenciales, como la personalización del aprendizaje y la mejora en la comunicación, al tiempo que reconozcan los riesgos, como la vulnerabilidad a brechas de seguridad y la exposición indebida de datos personales. Esta dualidad subraya la necesidad de una formación continua en ciberseguridad y el desarrollo de políticas claras que protejan la privacidad en el entorno educativo digital. La transición hacia el aprendizaje digital ha aumentado la importancia de estos datos, intensificando el fenómeno de la "datificación" en el ámbito educativo (Williamson et al., 2020), lo que subraya la necesidad de una mayor formación y conciencia en torno a la gestión y protección de la información en estos entornos.

La experiencia previa en el uso de redes y los incidentes relacionados con la privacidad tienen un impacto significativo en la preocupación de las personas por la protección de sus datos personales (Barroso & Feijóo, 2020). Este fenómeno resalta la importancia de prestar especial atención, tanto a la protección de los datos personales del alumnado como a la de los docentes, ya que la privacidad está profundamente vinculada con los derechos individuales en relación con el control de cómo se recopila y utiliza su información personal (Vartiainen et al., 2024).

Estudios recientes han revelado que tanto estudiantes universitarios (Antonopoulou et al., 2020) como maestros en formación (Gallego-Arrufat et al., 2019) presentan bajos niveles de competencia en seguridad digital. Este último destaca que la mitad de ellos muestra un riesgo digital medio debido al uso de prácticas poco seguras mientras hacen uso de sus dispositivos digitales. En esta misma línea, Hernández-Martín et al., (2021) destacan la importancia de una formación en competencia digital que contemple la privacidad y seguridad de los datos. Por ello, se considera crucial ampliar las áreas de estudio en seguridad digital para desarrollar estrategias educativas que doten a los docentes y, por tanto, al alumnado de

las habilidades y destrezas necesarias que permitan comprender de una forma critica, ética y segura la información que comparten, analizando las amenazas de los entornos digitales que visita. En definitiva, contribuir al desarrollo de una sociedad digital crítica y competencialmente segura.

En este contexto, la implementación de programas de formación específicos sobre el tratamiento de datos ha demostrado ser más efectiva que el mero establecimiento de normas, ya que tales programas pueden equipar a los docentes con las herramientas necesarias para manejar de manera segura la información en entornos digitales. Un nivel competencial óptimo en tecnología digital entre los docentes no solo facilita un entorno de enseñanza y aprendizaje más seguro y eficaz, sino que también permite la aplicación de criterios didácticos, pedagógicos y metodológicos de una forma más adecuada, promoviendo el desarrollo de una conciencia crítica, moral y ética en el uso de la tecnología, tanto por parte de los educadores como de los estudiantes (Tigelaar et al., 2004). Por lo tanto, es fundamental integrar la formación en ciberseguridad y en el manejo ético de los datos en la formación docente, para garantizar que las prácticas educativas en el entorno digital respeten y protejan los derechos de todos los involucrados.

2.5. Seguridad digital para protección de dispositivos

La rápida evolución de la tecnología digital y la creciente integración de dispositivos electrónicos en el entorno educativo presentan un conjunto complejo de desafíos relacionados con la seguridad digital para los docentes. En un contexto donde el uso de plataformas en línea y dispositivos electrónicos se está convirtiendo en una práctica estándar dentro de las aulas, la capacidad de los docentes para proteger la privacidad y seguridad de los dispositivos electrónicos se vuelve de vital importancia.

La incorporación de tecnologías, incluyendo dispositivos multimedia como ordenadores portátiles, tabletas digitales o pizarras interactivas entre otros a la educación ha incrementado de manera significativa la relevancia de la

alfabetización digital dentro del ámbito académico, convirtiéndose en una competencia esencial tanto para docentes como para estudiantes (Mendivil Caldentey et al., 2022). El uso de herramientas interactivas, plataformas de aprendizaje en línea y otros recursos digitales han impulsado una transformación en las prácticas educativas, requiriendo que las administraciones e instituciones educativas realicen una inversión considerable en infraestructura tecnológica. Esta inversión no solo incluye la adquisición de hardware y software, sino también la capacitación del personal para utilizar eficazmente estas herramientas en la enseñanza. Como resultado, se ha facilitado la gestión administrativa, se han ampliado las posibilidades de investigación y se ha enriquecido la experiencia docente, permitiendo un enfoque más dinámico e interactivo en el proceso de enseñanza-aprendizaje (Estrada et al., 2022). Además, estas tecnologías han abierto nuevas oportunidades para la personalización del aprendizaje, adaptándose mejor a las necesidades individuales de los estudiantes y promoviendo una educación más inclusiva y accesible.

El auge de la tecnología educativa, caracterizada no solo por la implementación de herramientas digitales avanzadas, sino también por la confección de entornos virtuales de aprendizaje, ha incrementado la exposición a amenazas y vulnerabilidades cibernéticas que pueden comprometer la integridad y seguridad tanto de los usuarios como de la información almacenada en sus medios electrónicos. Esta continua evolución de la tecnología ha dado lugar en los últimos años a la aparición y consolidación de nuevos conceptos imprescindibles para comprender el impacto de la digitalización en la educación y en la vida cotidiana. Entre estos conceptos se incluyen cultura digital**,** competencia digital**,** seguridad digital**,** peligros de Internet**,** Internet de las cosas y las citadas IA e IAGen (Casal-Otero et al., 2023; García-Peñalvo & Vázquez-Ingelmo, 2023; Hutson et al., 2018; Mugariri et al., 2022).

La gestión de la seguridad en entornos digitales es un tema que exige una profunda reflexión sobre los beneficios y perjuicios que el uso de la tecnología aporta a la sociedad actual. Para abordar adecuadamente esta

cuestión, es fundamental entender los riesgos asociados que conlleva la posesión y el uso de los dispositivos digitales en la actualidad, adoptando una perspectiva equilibrada que tenga en cuenta tanto sus posibles consecuencias físicas como psicológicas derivadas de un uso inadecuado de estas (Castillejos López et al., 2016). Como docentes resulta esencial que se tenga un conocimiento completo de las amenazas y desafíos que el mal uso continuado de estos dispositivos plantea para nuestra privacidad y bienestar físico y mental (Mugariri et al., 2022). Asimismo, la ética en el uso de dispositivos tecnológicos adquiere una especial relevancia cuando son los proveedores de este tipo de tecnología, incluidos aquellos que desarrollan recursos y productos educativos, los que tienen la posibilidad de acceder y almacenar una gran cantidad de información personal de carácter sensible (Hillman, 2023). Es en este mismo contexto, donde la protección de datos personales y la implementación de medidas de seguridad efectivas en los dispositivos se vuelven cruciales. A pesar de que la sociedad suele emplear mecanismos básicos de protección, como antivirus; la gestión de contraseñas o la seguridad en redes inalámbricas, especialmente en entornos públicos, sigue siendo insuficiente, dejando la información personal vulnerable (Hall, 2016). De ahí la necesidad imprescindible de priorizar la protección de la privacidad, evaluando cuidadosamente la seguridad antes de conectarse a redes públicas.

La seguridad de los dispositivos digitales y la navegación a través de Internet exigen un conjunto integral de habilidades, conocimientos y actitudes para garantizar un uso seguro y responsable (Torres-Hernández & Gallego-Arrufat, 2022). En este contexto, la educación en seguridad digital adquiere un significado profundo cuando su objetivo principal es proporcionar a los docentes, y ende a los estudiantes, las herramientas y competencias digitales necesarias para consolidar una seguridad robusta que garantice una sociedad presente y futura digitalmente segura, crítica y consciente del potencial y los riesgos asociados con el uso de dispositivos digitales (Pham et al., 2019). Es crucial que estos dispositivos sean utilizados de manera inteligente, con un enfoque en la prevención de riesgos innecesarios que pueden surgir del uso de la Red, y que se adopte un enfoque prudente al

compartir cualquier tipo de información (Moreira et al., 2015). Esta educación debe fomentar un equilibrio entre la explotación de las oportunidades que ofrecen las tecnologías digitales y la adopción de prácticas seguras que protejan la privacidad y la integridad de los datos en un entorno digital cada vez más complejo y vulnerable. Por todo ello, resulta fundamental promover, analizar y profundizar en el conocimiento y el uso de los dispositivos digitales que se utilizan de forma diaria, fomentando una actitud más responsable hacia su manejo (Cózar-Gutiérrez et al., 2016). Este enfoque no solo implica una mayor comprensión de las tecnologías, sino también una adopción consciente y segura de las prácticas digitales cotidianas, que permita a los usuarios manejar las herramientas tecnológicas de manera efectiva y protegerse adecuadamente contra posibles riesgos.

Por lo tanto, en el ámbito de la seguridad digital, se considera de suma importancia que los docentes comprendan y gestionen una variedad de riesgos y amenazas en línea para proteger sus dispositivos y datos. Estos riesgos incluyen virus y malware, es decir, un software diseñado para dañar, interrumpir o acceder a dispositivos y redes sin autorización y que pueden dañar o comprometer los sistemas informáticos; spam, que puede servir como vehículo para otros ataques; Amenazas Persistentes Avanzadas (APT), ataques sofisticados dirigidos a robar información confidencial; o el phishing, que implica intentos de obtener información sensible, como contraseñas o datos bancarios, mediante engaños. Los atacantes suelen enviar correos electrónicos que parecen provenir de fuentes legítimas, solicitando que los usuarios hagan clic en enlaces o proporcionen información personal (Chhikara et al., 2013). Cada una de estas amenazas representa un peligro significativo que puede afectar la seguridad de los dispositivos, así como la privacidad de la información personal y académica. Para mitigar estos riesgos, es fundamental que los docentes implementen prácticas de seguridad proactivas, como mantener el software actualizado, utilizar soluciones ofrecidas por antivirus y antimalware, formarse sobre técnicas de phishing y optar por el uso de contraseñas seguras que incluyan un doble factor o capa de seguridad que garantice así un entorno digital seguro y protegido (Hall, 2016).

En este sentido hay que tener en cuenta que no se considera adecuado abordar la seguridad digital sin tener en cuenta su vinculación con la ética digital, ya que ambos conceptos mantienen una profunda interrelación; la seguridad digital constituye la base sobre la cual se edifica la ética en el entorno digital. Mientras que seguridad digital se erige para proteger la información, garantizar la confidencialidad, integridad y disponibilidad de los datos, así como la seguridad de las infraestructuras tecnológicas en entornos digitales (Khan et al., 2023), la ética digital tiene como principal objetivo la aplicación de principios éticos que promuevan un comportamiento responsable y equitativo en el uso de los dispositivos conectados a la red, asegurando un acceso justo a la tecnología y reflexionando sobre las consecuencias éticas de nuestras decisiones y comportamientos en el mundo digital (Burr et al., 2020).

De este modo, la seguridad digital no solo protege los recursos tecnológicos, sino que también establece los cimientos sobre los cuales se desarrollan comportamientos éticos en el mundo digital. Al garantizar la seguridad, se crean las condiciones necesarias para que las interacciones a través de la comunicación o la compartición de información en línea se realicen de manera responsable y consciente, comprendiendo el impacto de nuestras acciones en este entorno. Esta interdependencia entre seguridad y ética digital subraya la importancia de una formación integral en ambos aspectos, ya que solo a través de una comprensión profunda de estas áreas podemos fomentar una cultura digital que valore tanto la protección de la información como la promoción de conductas éticas y equitativas (Kumar & Nanda, 2019).

Recientes estudios destacan que tanto los docentes en ejercicio como los futuros educadores poseen un bajo nivel de dominio en temas de seguridad digital. Esta carencia de conocimientos puede resultar en importantes brechas en la protección de datos personales y académicos, lo que a su vez puede dejar tanto a docentes como a estudiantes vulnerables a ataques cibernéticos, violaciones de privacidad y otros incidentes de seguridad vinculados al uso de sus dispositivos (De Waal & Grösser, 2014).

Novella-García & Cloquell-Lozano (2021) destacan que los futuros docentes españoles reciben poca formación ética orientada al desarrollo de las competencias digitales relacionadas con la seguridad digital, dando lugar a necesidades y carencias formativas latentes como la actualización de amenazas y riesgos en línea o falta de conocimientos específicos sobre cómo proteger los datos de los estudiantes y garantizar un uso adecuado de sus dispositivos.

Dada esta situación, se hace imprescindible ofrecer una formación especializada a los docentes, centrada en la gestión de riesgos digitales, la protección de datos sensibles y la adopción de prácticas seguras en el uso de sus dispositivos. Convirtiéndose así la adquisición de competencias digitales docentes (CDD) en un componente esencial de la formación del profesorado, proporcionándoles la profesionalidad necesaria para enfrentar con éxito los desafíos de la sociedad digital (Pozos Pérez & Tejada Fernández, 2018).

Otros autores aseguran que, tras recibir una adecuada formación los docentes y estudiantes incrementaron la adopción de prácticas seguras (Ferrag et al., 2019; Khan et al., 2023). De ahí surge la necesidad imperiosa de desarrollar experiencias digitales, y que además modelen y fomenten comportamientos responsables en toda la comunidad educativa. Estas experiencias educativas deben estar diseñadas para cultivar un entorno donde docentes y discentes se conviertan en usuarios conscientes y competentes, capaces de proteger sus dispositivos, sus datos personales y de navegar por la red de manera segura y ética. La formación continua en estos aspectos es clave para fortalecer la resiliencia digital en un mundo cada vez más interconectado y vulnerable a amenazas cibernéticas (Amador-Alarcón et al., 2021; Gallego-Arrufat et al., 2019; Torres-Hernandez, 2023).

Por lo tanto, es fundamental desarrollar programas de formación continua que equipen a los docentes con las competencias necesarias para identificar y mitigar riesgos, garantizar la seguridad de los sistemas y mantener un entorno educativo seguro en la era digital.

CAPÍTULO 3. METODOLOGÍA

3.1 Metodología de la investigación

De acuerdo con la normativa específica de la Universidad de Jaén para tesis doctorales basadas en compendios de publicaciones, a continuación, se detalla la metodología aplicada en el diseño e implementación de los tres trabajos que conforman esta tesis. Es importante señalar que cada uno de los estudios científicos incluidos en esta tesis proporciona una descripción específica y exhaustiva de la metodología utilizada en su desarrollo.

La investigación siguió un enfoque de corte no experimental, con una naturaleza descriptiva y abordándose de manera transversal. Para ello, se utilizó el método por encuesta y se optó por un diseño ex post facto, que se concretó en la creación y aplicación de un cuestionario.

A continuación, se detallan cada uno de los elementos de la misma.

3.2 Instrumento

El instrumento utilizado en este estudio fue diseñado *ad hoc* tomando como referencia el Marco Común Europeo de Competencia Digital para la Ciudadanía, conocido como DigComp en su versión 2.2, con un enfoque particular en el área de seguridad y sus cuatro dimensiones. Este marco, desarrollado por Vuorikari Rina et al., (2022), proporciona una estructura integral para evaluar las competencias digitales en la ciudadanía europea, haciendo énfasis en la importancia de la seguridad digital.

A partir de ahí, se desarrolló el cuestionario denominado "Competencia en Seguridad Digital" (COSEDI), el cual se diseñó para medir de manera detallada y específica la competencia en seguridad digital de docentes andaluces en activo. El cuestionario aborda las cuatro áreas de seguridad, como son la protección de dispositivos, la protección de datos personales, la salud y el medioambiente. La creación de COSEDI buscó capturar de manera precisa habilidades y conocimientos de los docentes encuestados con el fin de ofrecer respuestas a sus necesidades formativas que garanticen un uso ético y responsable de sus dispositivos y una navegación segura en

entornos digitales, alineándose con los estándares establecidos en el DigComp 2.2.

El proceso de validación del instrumento se llevó a cabo en dos fases principales. En la primera fase, se realizó una validación de contenido mediante un juicio de expertos, siguiendo la metodología de Escobar y Cuervo (2008) evaluando la claridad, coherencia, relevancia y suficiencia de los ítems del cuestionario. Esto permitió eliminar los ítems menos relevantes para el objetivo del estudio y reformular aquellos que presentaban confusión o dificultad de comprensión.

En la segunda fase, tras incorporar las recomendaciones de los expertos, se llevó a cabo un estudio piloto con 60 docentes del sistema educativo público andaluz, seleccionados según la fórmula de Viechtbauer et al., (2015) mediante consentimiento informado. Para ello se realizó un análisis factorial exploratorio (AFE) para identificar las dimensiones latentes que explican la variabilidad en las respuestas.

Por tanto, el instrumento de medición se delimitó a un total de 53 ítems repartidos en 4 dimensiones, mediante una escala tipo Likert de 4 puntos (1=Nunca; 2= A veces; 3= Casi siempre; 4= Siempre):

- **PrDpP:** Protección de datos personales y privacidad (15 ítems).
- **PrDi:** Protección de dispositivos (13 ítems).
- **PrMe:** Protección medioambiental (14 ítems).
- **PrSB:** Protección de la salud y el bienestar (11 ítems).

3.3 Población y muestra

El tamaño muestral ha sido determinado a través de un muestreo simple aleatorio, de una población total de n=107.837 de docentes, y donde todos los miembros de la población han tenido las mismas oportunidades de ser seleccionados (Hernández et al., 2014). Para ello, se implementó la fórmula para poblaciones finitas para obtener una muestra representativa, con un nivel de confianza del 95% y un margen de error del 5%, obteniendo una

muestra representativa de la población, y habiéndose llevado a cabo un estudio piloto con un total de 60 docentes que fueren eliminados para el análisis final

Finalmente, la muestra ha quedado conformada por un total de 497 docentes del sistema educativo público andaluz, de los cuales más del 60% son mujeres, respecto al 33% de hombres, y destacando el 1.4% residual que prefiere no decirlo y cuya media de edad ha sido de 44.89 años.

3.4 Procedimiento de recogida de datos

La versión final del instrumento (COSEDI) fue convertida a formato digital (https://lc.cx/eSw1Rh) para facilitar su aplicación a la población seleccionada. Los docentes que participaron en el estudio piloto fueron excluidos de la base de datos muestral, por lo tanto, el instrumento no se les aplicó, evitando así posibles sesgos y errores en la investigación. Asimismo, en cumplimiento de la normativa vigente y siguiendo los principios éticos de la investigación, se informó a los participantes asegurando la anonimización de sus respuestas, garantizando la confidencialidad y su uso exclusivo con fines de investigación

3.5 Análisis de datos

Para llevar a cabo la limpieza, tabulación y tratamiento estadístico de los datos se empleó el software estadístico SPSS (IBM-SPSS Statistics Version 28.0).

En el artículo de validación del cuestionario además se usó el programa SmartPLS4 para el modelizado de ecuaciones estructurales (Becker et al., 2023; Ringle et al., 2024).

Dicho análisis se llevó a cabo en distintas fases, en primer lugar, se analizaron de forma univariante cada uno de los ítems computando las respuestas de todas las observaciones, se estimó el poder discriminativo de los ítems a partir de un análisis univariante, se comprobaron las medidas de centralidad (media y mediana) de distribución de los resultados (asimetría,

curtosis y normalidad), así como, la dispersión de los valores (desviación estándar, valores máximos y mínimos y rango intercuartílico), también se empleó. el análisis bivariante (correlaciones de Pearson y Rho de Spearman).

En la siguiente fase del análisis se emplearon técnicas estadísticas multivariantes, en este caso el análisis factorial exploratorio que permite la identificación de las variables o factores latentes que permiten agrupar los temas de la escala en cuestión, para comprobar si la estructura a priori se ajustaba con la original propuesta se realizó un análisis factorial confirmatorio que permite la comprobación de los supuestos teóricos.

Por otro lado, en los artículos en los cuales se analizó la protección de dispositivos y la protección de datos personales se realizó un análisis descriptivo y exploratorio inicial de cada variable e ítem, utilizando medidas de centralidad como la Media (M), Mediana (Me), Cuartil 1 (P25) y Cuartil 3 (P75), así como medidas de dispersión como la Desviación Estándar (DE), el Rango Intercuartil, y los valores mínimos y máximos registrados.

En el análisis inferencial, se aplicó la prueba t de Student para muestras independientes o la U de Mann-Whitney en escenarios con dos segmentaciones. Para situaciones con tres o más categorías segmentadas, se utilizó el análisis de varianza de un factor para muestras independientes (ANOVA) en contextos paramétricos y la prueba de Kruskal-Wallis en contextos no paramétricos. Se llevaron a cabo contrastes post-hoc utilizando el método Tukey (para casos paramétricos) y el procedimiento Dwass-Steel (no paramétrico) para comparaciones por pares. El tamaño del efecto se determinó utilizando $\eta 2$ parcial o $\varepsilon 2$, interpretado en base a los siguientes criterios: Insignificante (<0.01), Pequeño (<0.06), Mediano (<0.14) y Grande (>0.14).

CAPÍTULO 4. COMPENDIO DE TRABAJOS

1. Villén-Contreras, R., Rodríguez-Moreno, J. & Agreda-Montoro, M. (2024). **VALIDACIÓN Y ESTUDIO PILOTO DE UNA ESCALA PARA LA COMPETENCIA EN SEGURIDAD DIGITAL DEL PROFESORADO EN CENTROS EDUCATIVOS DESDE UN ENFOQUE PLS-SEM.**

2. **Breve resumen:**
   Ante los retos y desafíos actuales, como son los riesgos y amenazas inherentes al uso de internet y los dispositivos inteligentes, se hace indispensable ser competentes en seguridad digital y comportarnos éticamente en los entornos digitales. Por ello, el estudio ha tenido como objetivo diseñar y validar el instrumento COSEDI, basado en el Marco Europeo de Competencias Digitales para la Ciudadanía (DigComp). Para ello, se ha realizado un análisis basado en el modelado de ecuaciones estructurales (PLS-SEM), con una metodología de corte no experimental y cuantitativa. La muestra representativa ha quedado conformada por 497 profesores del sistema educativo público de Andalucía. Los resultados muestran la validez y fiabilidad del instrumento a través de la demostración de las relaciones causales entre los constructos de protección de datos y privacidad, protección de dispositivos, protección medioambiental y protección de la salud y el bienestar, así como la pertenencia de las variables observadas que los conforman, a través de los valores de las cargas factoriales y significancia. Por tanto, el modelo avala la idea de que las cuatro variables latentes tienen una influencia las unas sobre las otras, siendo la relación entre la protección de datos y privacidad y la protección de dispositivos la más fuerte y significativa, mientras que la más débil se da entre la protección de datos personales y protección medioambiental.

3. **Fecha de publicación:** 09-08-2024
4. **Estado:** publicado
5. **Tipo de publicación:** artículo
6. **Categoría:** monografía
7. **Ubicación.** *Revista Electrónica Interuniversitaria de Formación del Profesorado, 27*(3), 69-84. https://doi.org/10.6018/reifop.614841
8. **Otros datos de interés:**

1. Villén-Contreras, R., Rodríguez-Moreno, J. & Agreda-Montoro, M. (2024). **PERFIL COMPETENCIAL DEL PROFESORADO ANDALUZ EN SEGURIDAD DIGITAL: EVALUACIÓN DE LA PROTECCIÓN DE DATOS Y PRIVACIDAD DE ACUERDO CON EL MARCO COMÚN DE COMPETENCIA DIGITAL CIUDADANA (DIGCOMP) (COMPETENCY PROFILE OF ANDALUSIAN TEACHERS IN DIGITAL SECURITY: EVALUATION OF DATA PROTECTION AND PRIVACY IN ACCORDANCE WITH THE COMMON FRAMEWORK OF DIGITAL CITIZEN COMPETENCE (DIGCOMP)**

2. **Breve resumen:**
   Este artículo presenta los hallazgos de una investigación enfocada en la evaluación de la competencia digital de los educadores en lo que respecta a la salvaguarda de datos personales, conforme al marco europeo DigComp 2.2. En el estudio tomaron parte 497 docentes del sistema educativo andaluz a través de un cuestionario validado por expertos sobre Competencia en Seguridad Digital. Este instrumento, de enfoque integral y dividido en cuatro dimensiones, se centra en la Dimensión "Protección de Datos Personales", abarcando 15 ítems. Este enfoque nos posibilita comprender el nivel competencial de los docentes durante su desempeño. Se observan disparidades significativas en la salvaguarda de datos personales asociadas a la edad, la antigüedad docente y las horas de formación, indicando que aquellos de mayor edad, antigüedad y mayor formación obtienen calificaciones más elevadas. En resumen, los docentes andaluces que participan en este estudio exhiben una disposición favorable a la seguridad para proteger sus datos personales, aunque presentan carencias asociadas al trato seguro y responsable de estos durante la navegación por la red.

3. **Fecha de publicación:** 01-05-2024

4. **Estado:** publicado

5. **Tipo de publicación:** artículo

6. **Categoría:** monografía

7. **Ubicación.** Pixel-Bit. Revista de Medios y Educación, 70, 123-142| 2024

   DOI: **https://doi.org/10.12795/pixelbit.104153**

8. **Otros datos de interés:**

1. Villén-Contreras, R., Rodríguez-Moreno, J. & Agreda-Montoro, M. (2024). **PERFIL COMPETENCIAL DEL PROFESORADO ANDALUZ EN SEGURIDAD DIGITAL: EVALUACIÓN DE LA PROTECCIÓN DE DISPOSITIVOS DE ACUERDO CON EL MARCO DIGCOMP**

2. **Breve resumen: Introducción:** La utilización de dispositivos electrónicos conectados a la red plantea desafíos y riesgos asociados con la seguridad digital, especialmente en lo que respecta a la protección de los dispositivos. Este texto tiene como objetivo conocer la autopercepción de la Competencia Digital Docente (CDD) en relación con la protección de dispositivos, conforme al marco europeo DigComp 2.2**. Método:** Participan 497 docentes del sistema educativo andaluz durante el curso 2022/23 y se aplica un cuestionario sobre la competencia en seguridad digital, validado por expertos. Se trata de un instrumento más amplio que se divide en cuatro dimensiones, centrándonos en la dimensión "Protección de Dispositivos", compuesta por 15 ítems y que nos permite conocer el nivel y perfil competencial de los docentes durante el desempeño de su trabajo. **Resultados:** En general, los participantes demuestran habilidades sólidas para garantizar la "Protección de Dispositivos". Se destacan diferencias significativas en la competencia digital relacionadas con la antigüedad docente y las horas de formación, resaltando que aquellos con más experiencia y mayor formación obtienen puntuaciones más altas. Sin embargo, se observa variabilidad en las respuestas en relación con el uso de software de rastreo ante pérdida o robo, así como en la implementación de cortafuegos en entornos públicos y laborales. **Discusión:** En resumen, los docentes andaluces que participan en este estudio exhiben una disposición favorable en cuanto a la seguridad para proteger sus dispositivos electrónicos, aunque presentan carencias en conocimientos, habilidades y prácticas asociadas al uso seguro y responsable de estos dispositivos cuando permanecen conectados a la red.

3. **Fecha de publicación:** probable abril de 2025
4. **Estado**: Recibido: enero 2023 • Evaluado: marzo 2024 • Aceptado: abril 2024
5. **Tipo de publicación:** artículo
6. **Categoría:** monografía
7. **Ubicación.** Revista Complutense de Educación (sin DOI hasta su publicación)
8. **Otros datos de interés:** previsiblemente se publicará en el número 2 del año que viene, hasta la fecha de publicación no se le asignará el doi.

CAPÍTULO 5. RESULTADOS Y DISCUSIÓN

RESULTADOS Y DISCUSIÓN

Dada la perspectiva adoptada en la presente tesis doctoral, a continuación, se presentan los principales resultados obtenidos en base a los objetivos marcados al inicio, así como la discusión integrada de los mismos. Aunque estos resultados han quedado desarrollados con mayor detalle en los tres artículos que conforman el compendio, se enumeran de manera diferenciada para cada trabajo aportado, según se detalla a continuación.

Los resultados obtenidos en relación con el objetivo 1, “Analizar la fiabilidad y validar el instrumento COSEDI, basado en el Marco Europeo de Competencias Digitales para la Ciudadanía (DigComp), para evaluar la percepción de autoeficacia de los docentes en cuanto a la seguridad digital”, han demostrado la validez del modelo propuesto, evidenciado en los valores de fiabilidad obtenidos a través del análisis de la validez de los constructos.

En cuanto a los resultados específicos, el apartado de "protección de dispositivos" obtuvo un coeficiente alfa de Cronbach de .859, "protección de datos personales y privacidad" alcanzó un valor de .858, "protección medioambiental" logró un .895, y "protección de la salud y el bienestar" obtuvo un .771. De manera general, el análisis de la fiabilidad compuesta muestra que los valores superan el umbral de .827, lo cual refleja un alto nivel de validez y fiabilidad del instrumento de medición utilizado.

Por tanto, estos resultados confirman que el instrumento COSEDI es confiable y válido para evaluar la autoeficacia percibida por los docentes en relación con la seguridad digital, abarcando distintos aspectos clave como la protección de dispositivos, datos, medio ambiente, salud y bienestar.

Con respecto al segundo objetivo del estudio, “Analizar la relación entre las distintas variables del estudio”, los resultados respaldan la hipótesis inicial en cuanto a la capacidad de influencia entre sí de las cuatro variables latentes. La relación más fuerte y significativa dada, acontece entre la protección de datos y privacidad y la protección de dispositivos, mientras que la relación más débil se percibe entre la protección de datos personales y la protección medioambiental.

Asimismo, se verifica la adecuación de las variables observadas o indicadores a sus respectivos constructos, con valores de carga que superan 0.4 y niveles de significatividad estadística (p-valor) inferiores a .05. Esto confirma la robustez de las relaciones propuestas en el modelo y la coherencia entre los indicadores y sus constructos asociados.

En cuanto al tercer objetivo, “Evaluar la competencia digital en seguridad de los docentes activos andaluces en relación con la protección de datos personales y la protección de dispositivos, a través de un análisis según género, experiencia docente, edad y formación”, y el cuarto, “Analizar la percepción, carencias y necesidades formativas del profesorado andaluz respecto a la competencia digital en el área de seguridad", se realizó un análisis inferencial de los datos.

A continuación, se presentan los resultados obtenidos del análisis inferencial de los datos sobre la protección de datos personales, la privacidad y la protección de dispositivos. En este análisis, se examinaron distintas variables sociodemográficas y contextuales con el fin de identificar su influencia en las prácticas de los docentes.

A continuación, se presentan los resultados obtenidos del análisis inferencial de los datos sobre la protección de datos personales, la privacidad y la protección de dispositivos. En este análisis, se examinaron distintas variables sociodemográficas y contextuales con el fin de identificar su influencia en las prácticas de los docentes.

En el ámbito de la protección de datos personales y privacidad, algunas variables sociodemográficas, como el género de los docentes, mostraron una asociación cercana a la significancia estadística con un tamaño de efecto pequeño. Esto sugiere diferencias leves en las prácticas de protección de datos entre hombres y mujeres, lo cual concuerda con investigaciones previas que no encontraron diferencias significativas (Vuorikari Rina et al., 2022). Aunque los resultados no son concluyentes, estas diferencias podrían ser objeto de estudios futuros.

En referencia al análisis de la dimensión "Protección de Dispositivos" según el género, no se encontraron diferencias significativas en función del género, con puntuaciones similares entre hombres y mujeres. Sin embargo, estudios previos han señalado que los hombres tienden a tener una mayor autopercepción de competencia en seguridad digital en comparación con las mujeres (Hargittai & Shafer, 2006).

Del mismo modo, al considerar el tipo y la ubicación del centro educativo, no se identificaron diferencias relevantes en las puntuaciones acumuladas sugiriendo que estos factores no influyen de manera significativa en la protección de dispositivos y en la protección de datos personales. Este hallazgo sugiere que, independientemente de si los docentes trabajan en centros de características distintas o en ubicaciones geográficas diversas, sus prácticas son relativamente consistentes, lo que podría reflejar la influencia de políticas generales y normativas homogéneas en el ámbito educativo.

En cuanto a la relación entre la edad y la antigüedad docente, los resultados mostraron diferencias significativas en la protección de datos, aunque con tamaños de efecto pequeños. Este hallazgo coincide con investigaciones previas que han identificado una conexión significativa entre la edad (Cabezas González et al., 2017; Gallego-Arrufat et al., 2019) y, especialmente, la antigüedad docente, asociando mayor antigüedad con un nivel más alto de competencia digital (Pozo Sánchez et al., 2020; Rodríguez Espinosa et al., 2016). Estos resultados invitan a pensar que los docentes en edades diferentes y con niveles de experiencia variados adoptan prácticas de protección de datos de manera distinta, lo que destaca la importancia de considerar estos factores al diseñar programas de formación y concienciación en privacidad y seguridad digital para los docentes.

En línea con estos hallazgos, se observó que los docentes mayores de 60 años presentaron una puntuación media ligeramente superior en comparación con los docentes menores de 30 años. No obstante, estas diferencias no fueron estadísticamente significativas, lo que indica que la edad no es un factor determinante en la dimensión de protección de

dispositivos. Sin embargo, el análisis de la antigüedad del docente con esta misma dimensión sí reveló diferencias significativas particularmente entre los docentes con menor antigüedad (0-5 años) y aquellos con 21 años o más de experiencia. Además, se identificaron diferencias cuando se comparó los grupos de edad entre 11-15 años de antigüedad y aquellos con 21 o más años, lo que sugiere que la antigüedad podría tener cierta influencia en la protección de dispositivos. Estos resultados concuerdan con otros estudios en los cuales se establece que la antigüedad docente es un factor influyente en los niveles de competencia digital en el área de seguridad (Pozo Sánchez et al., 2020).

En referencia a la etapa educativa en la que enseñan los docentes, no se identificaron diferencias significativas en cuanto a la protección de datos y privacidad ni en la protección de dispositivos, aunque en esta última se observó un pequeño tamaño de efecto. Por tanto, se advierte que la protección de datos y privacidad que ejercen los docentes no varía sustancialmente independientemente de la etapa educativa en la que imparta docencia, lo que refuerza la idea de prácticas estandarizadas en los distintos niveles educativos.

Sin embargo, al comparar a los docentes de educación infantil con los de educación para adultos, aunque las diferencias no fueron significativas, sí se mostraron más pronunciadas, lo que sugiere una posible tendencia que podría investigarse más a fondo. Este hallazgo es coherente con estudios previos que indican que la etapa educativa en la que enseña el profesorado puede influir en su nivel de competencia digital en el área de seguridad (Fuentes et al., 2019).

El análisis de las horas de formación reveló un impacto significativo tanto en las prácticas de protección de datos y privacidad como en la protección de dispositivos. Los docentes que habían recibido más de 60 horas de formación se diferenciaron significativamente de aquellos con menos de 60 horas o sin formación, lo que subraya la importancia de una formación prolongada para el desarrollo de prácticas efectivas en la protección de datos y privacidad.

Estas diferencias fueron significativas en todos los contrastes post-hoc, destacando la relevancia de la formación continua en la mejora de las prácticas relacionadas con la protección de datos personales y de dispositivos. Los resultados sugieren la necesidad de explorar más a fondo la relación entre la cantidad de horas de formación y las puntuaciones acumuladas en estas dimensiones.

Sin embargo, en cuanto a la protección de datos, no se encontraron diferencias significativas entre los docentes sin formación y aquellos con menos de 60 horas, lo que indica la posible existencia de un umbral de formación necesario para influir sustancialmente en las conductas de protección de datos. Este hallazgo destaca la necesidad de programas formativos extensivos para garantizar la adopción de medidas adecuadas de privacidad y protección de datos entre los docentes. En consonancia con otros estudios, se evidencia que los futuros docentes carecen de una formación digital adecuada, lo cual respalda la idea de una capacitación y nivel de competencia insuficiente en seguridad respecto a la protección de sus dispositivos y el uso de Internet (Gallego-Arrufat et al., 2019).

CAPÍTULO 6. CONCLUSIONES Y PERSPECTIVAS FUTURAS

Conclusiones y perspectivas futuras

Esta tesis doctoral se ha centrado en explorar diversas perspectivas sobre la competencia digital en el ámbito de la seguridad, enfocándose en profesionales de la docencia que trabajan en distintos centros educativos de la comunidad andaluza y que conviven diariamente con esta realidad.

En base a los objetivos 1 y 3, establecidos en esta tesis doctoral, se puede afirmar que una de las primeras conclusiones extraídas ha sido la aceptación del modelo propuesto. La relevancia del cuestionario (COSEDI) recae en la posibilidad de proporcionar una evaluación de la autopercepción del profesorado que actualmente presta servicio en el sistema público de educación andaluz en relación a la competencia en seguridad digital; para ello se toman como referencia los marcos de competencia digital. El análisis de esta competencia se ha fundamentado en la interrelación entre distintas variables o dimensiones latentes, tales como la protección de datos personales y privacidad, la protección de dispositivos, la protección medioambiental, y la protección de la salud y el bienestar. En este contexto concreto, las dimensiones se alinean con el Marco Común Europeo de Competencias Digitales para la Ciudadanía (DigComp 2.2) (Vuorikari Rina et al., 2022), específicamente en el ámbito de la seguridad y el uso responsable de la tecnología.

Los hallazgos resaltan la necesidad de contar con un profesorado con competencias sólidas en seguridad digital, siendo crucial en el contexto educativo actual, donde la digitalización y el uso intensivo de la tecnología han aumentado significativamente. La protección de la información sensible, tanto del profesorado como del alumnado, se ha convertido en una necesidad imperativa para evitar los riesgos derivados de posibles violaciones de datos. Según Matarrita-Cascante et al. (2022) una formación adecuada en seguridad digital actúa como un escudo protector, minimizando las vulnerabilidades y garantizando la integridad y confidencialidad de los datos manejados en el entorno escolar.

En esta misma línea, estudios recientes han destacado la trascendencia de estas competencias, reflejada en la evidencia de que el profesorado, en

muchos casos, almacena información y datos personales de carácter sensible en sus dispositivos personales, lo cual incrementa el riesgo de acceso no autorizado (Witsenboer et al., 2022). Esta práctica, aunque común, expone tanto a los docentes como a los estudiantes a amenazas que podrían comprometer no solo la privacidad de los datos, sino también la confianza en las infraestructuras educativas. Por tanto, es esencial que el profesorado desarrolle habilidades específicas para gestionar y mitigar estos riesgos, implementando medidas de protección adecuadas, como el uso de contraseñas seguras, la encriptación de datos y el uso de plataformas certificadas para el manejo de información académica.

Otra de las conclusiones derivadas de esta investigación, vinculada directamente con los objetivos 3 y 4, es la necesidad de establecer formaciones obligatorias en competencias de seguridad digital para el profesorado. El propósito de estas formaciones sería subsanar las carencias formativas identificadas, especialmente en lo que respecta al uso seguro y la protección de dispositivos dentro del entorno educativo. Esta recomendación responde a la creciente importancia de la tecnología en los procesos educativos y la consecuente necesidad de que el profesorado posea habilidades sólidas para gestionar los riesgos asociados al uso de dispositivos digitales. En consonancia con otros estudios como el de Mori (2019), se destaca que a pesar de que los docentes de Educación Primaria muestran un buen dominio en competencia digital, presentan dificultades especialmente en cuanto a la seguridad y el uso adecuado de los medios digitales, donde se sitúan por debajo del promedio europeo.

Por otro lado, el análisis de las inferencias del presente trabajo en relación con el objetivo 2, destaca la importancia y necesidad de profundizar en ciertos aspectos, especialmente en la relación entre la cantidad de horas dedicadas a la formación en competencias digitales y las puntuaciones obtenidas en la dimensión "Protección de Dispositivos". De aquí se deduce que no solo es crucial ofrecer formación, sino también optimizar la duración y el contenido de estos programas para maximizar su efectividad. Una correlación positiva entre el tiempo de formación y la competencia en protección de dispositivos indicaría que una formación más extensa o mejor

estructurada podría fortalecer significativamente las habilidades del profesorado en esta área.

Además de la protección de datos, una competencia avanzada en seguridad digital capacita al profesorado para reconocer y enfrentar las amenazas inherentes a los espacios cibernéticos, tales como el phishing, el malware y otros tipos de ataques que puedan comprometer las redes educativas. Esto es particularmente relevante dado que muchas infraestructuras escolares están interconectadas a través de intranets, lo que podría facilitar la propagación de amenazas si no se cuenta con las medidas de seguridad adecuadas. La capacidad de los docentes para gestionar estas situaciones no solo protege a las instituciones educativas de ataques potenciales, sino que también contribuye a la resiliencia y seguridad del entorno educativo en su conjunto.

Asimismo, al desarrollar estas competencias, los docentes no solo se protegen a sí mismos y a su alumnado, sino que también se empoderan para proporcionar una formación más robusta en seguridad digital a sus estudiantes. Esto es particularmente importante en un mundo donde los jóvenes son usuarios frecuentes de tecnología y, por lo tanto, también vulnerables a las amenazas digitales. Según Attai (2020) y Latorre-Medina & Tnibar-Harrus, (2023) el empoderamiento del profesorado en esta área es esencial para que puedan guiar a los estudiantes en el uso seguro y responsable de la tecnología, fomentando una cultura de ciberseguridad desde edades tempranas.

En definitiva, la formación en seguridad digital del profesorado no solo se traduce en una protección directa contra las amenazas cibernéticas, sino que también tiene un impacto multiplicador en la comunidad educativa, fortaleciendo las competencias digitales de los estudiantes y contribuyendo a un entorno de aprendizaje más seguro y confiable. Esto refuerza la idea de que la seguridad digital no es solo una competencia técnica, sino una necesidad pedagógica fundamental en la era digital.

No existen demasiados estudios que se centren específicamente en el profesorado de enseñanza primaria y secundaria en el ámbito de la competencia en seguridad digital, lo cual indica una brecha significativa en la literatura actual. Por lo tanto, investigaciones futuras deberían orientarse hacia la exploración de estas competencias en estos niveles educativos, considerando las características y desafíos particulares que enfrentan los docentes de primaria y secundaria en la integración segura de la tecnología en sus prácticas pedagógicas.

Asimismo, sería pertinente explorar la efectividad de diferentes modalidades de formación (presencial, en línea, híbrida) y estrategias pedagógicas (talleres prácticos, mentoría, aprendizaje basado en proyectos) en el desarrollo de competencias en seguridad digital en el profesorado de primaria y secundaria. Esto permitiría identificar qué metodologías son más efectivas, y adaptarlas para maximizar el aprendizaje y la aplicación práctica en contextos escolares.

Además, se considera de sumo interés que futuras investigaciones abordasen una evaluación longitudinal de los efectos de la formación en seguridad digital, examinando cómo estas competencias evolucionan con el tiempo y su impacto a largo plazo en la práctica docente y la seguridad de los entornos escolares. Estos estudios podrían proporcionar datos valiosos para la elaboración de políticas educativas que promuevan una formación continua y adaptativa en competencias digitales para los docentes de todos los niveles educativos.

Finalmente, esta investigación reconoce limitaciones metodológicas que deben considerarse al interpretar los resultados. Una de las principales limitaciones es la composición de la muestra, que está formada exclusivamente por docentes voluntarios del sistema educativo andaluz durante el curso 2022/23. Esta limitación podría introducir sesgos de selección, ya que los participantes voluntarios podrían tener una predisposición positiva hacia la tecnología o un mayor interés en la formación en competencias digitales, lo que no necesariamente representa al conjunto total del profesorado. Por tanto, se sugiere que futuros estudios amplíen la

muestra para incluir una representación más diversa y aleatoria de docentes, lo que podría proporcionar resultados más generalizables.

Adicionalmente, el estudio no aborda de manera exhaustiva otros factores que podrían influir en las competencias digitales del profesorado, como la disponibilidad de recursos tecnológicos en los centros educativos, el apoyo institucional para la formación continua, o la existencia de incentivos para la mejora de las competencias digitales. La integración de estos factores en futuros análisis podría ofrecer una visión más completa de las necesidades formativas y estructurales del profesorado en relación con la seguridad digital.

En suma, la implementación de formaciones obligatorias en competencias en seguridad digital, específicamente en la protección de dispositivos e información y datos personales, se perfila como una estrategia esencial para fortalecer la capacidad del profesorado en la gestión segura de la tecnología en el ámbito educativo. Para maximizar el impacto de estas formaciones, es fundamental considerar no solo la cantidad de horas dedicadas, sino también la calidad y la relevancia del contenido, así como garantizar una muestra representativa de los participantes para que los resultados reflejen las necesidades reales del sistema educativo en su conjunto. Este enfoque contribuiría a la creación de un entorno educativo más seguro y eficaz, alineado con las exigencias de la era digital.

REFERENCIAS BIBLIOGRÁFICAS

Amador-Alarcón, M. P., Torres-Gastelú, C. A., Lagunes-Domínguez, A., Angulo-Armenta, J., Argüello-Rosales, C. A., & Medina-Cruz, H. (2021). Marcos de competencias digitales relacionados con seguridad para docentes. *PÄDI Boletín Científico de Ciencias Básicas e Ingenierías Del ICBI*, *9*(Especial), 48-52. https://doi.org/10.29057/icbi.v9iEspecial.7490

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

Antonopoulou, H., Halkiopoulos, C., Barlou, O., & Beligiannis, G. N. (2020). Leadership types and digital leadership in higher education: Behavioural data analysis from University of Patras in Greece. *International Journal of Learning, Teaching and Educational Research*, *19*(4), 110-129. https://doi.org/10.26803/ijlter.19.4.8

Aras, A., & Büyüközkan, G. (2023). Digital transformation journey guidance: A holistic digital maturity model based on a systematic literature review. *Systems*, *11*(4), 213.

Attai, L. (2020). *Student data privacy: Managing vendor relationships*. Rowman & Littlefield.

Avello Martínez, R., & López Fernández, R. (2015). Alfabetización digital de los docentes de las escuelas de hotelería y turismo cubanas. Experiencias en su implementación. *International Journal of Educational Technology in Higher Education*, *12*, 3-16. https://doi.org/10.7238/rusc.v12i3.1994

Barroso, J. L. G., & Feijóo, C. (2020). Un análisis del comportamiento de la sociedad española con respecto a la protección de la privacidad en internet. *RES. Revista Española de Sociología*, *29*(2), 213-232. https://doi.org/doi:10.22325/fes/res.2020.12

Barroso Osuna, J. M., Matos Alcántara, V. Y., & Aguilar Gavira, S. (2019). Análisis de los recursos, usos y competencias tecnológicas del profesorado universitario para comprender y mejorar el proceso de aprendizaje del alumnado. *Revista Iberoamericana de Educación*. https://doi.org/10.35362/rie8013466

Becker, J.-M., Cheah, J.-H., Gholamzade, R., Ringle, C. M., & Sarstedt, M. (2023). PLS-SEM's most wanted guidance. *International Journal of*

Contemporary Hospitality Management, *35*(1), 321-346. https://doi.org/10.1108/IJCHM-04-2022-0474

Benavides, L. M. C., Tamayo Arias, J. A., Arango Serna, M. D., Branch Bedoya, J. W., & Burgos, D. (2020). Digital Transformation in Higher Education Institutions: A Systematic Literature Review. *Sensors*, *20*(11). https://doi.org/10.3390/s20113291

Bong, W. K., & Chen, W. (2024). Increasing faculty's competence in digital accessibility for inclusive education: A systematic literature review. *International Journal of Inclusive Education*, *28*(2), 197-213. https://doi.org/10.1080/13603116.2021.1937344

Brevik, L. M., Gudmundsdottir, G. B., Lund, A., & Strømme, T. A. (2019). Transformative agency in teacher education: Fostering professional digital competence. *Teaching and Teacher Education*, *86*, 102875. https://doi.org/10.1016/j.tate.2019.07.005

Brugia, M., & Zukersteinova, A. (2019). Continuing vocational training in EU enterprises. *Luxembourg: Publications Office of the European Union*, *73*. https://data.europa.eu/doi/10.2801/704583

Burr, C., Taddeo, M., & Floridi, L. (2020). The Ethics of Digital Well-Being: A Thematic Review. *Science and Engineering Ethics*, *26*(4), 2313-2343. https://doi.org/10.1007/s11948-020-00175-8

Cabero Almenara, J., Barroso Osuna, J. M., Rodríguez Gallego, M. R., & Palacios Rodríguez, A. de P. (2020). La Competencia Digital Docente. El caso de las universidades andaluzas. *Aula Abierta, 49 (4), 363-372.* https://doi.org/10.17811/rifie.49.4.2020.363-372.

Cabero-Almenara, J., Guillén-Gámez, F. D., Ruiz-Palmero, J., & Palacios-Rodríguez, A. (2022). Teachers' digital competence to assist students with functional diversity: Identification of factors through logistic regression methods. *British Journal of Educational Technology*, *53*(1), 41-57. https://doi.org/10.1111/bjet.13151

Cabezas González, M., Casillas Martín, S., Sánchez Ferreira, M., & Teixeira Diogo, F. L. (2017). Do Gender and Age Affect the Level of Digital Competence? A Study with University Students. *Fonseca*, *15*, 109-125. ProQuest One Academic; Publicly Available Content Database; Social Science Premium Collection.

https://doi.org/10.14201/fjc201715109125

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

Carretero, S., Vuorikari, R., & Punie, Y. (2017). *DigComp 2.1 – The digital competence framework for citizens with eight proficiency levels and examples of use*. Publications Office.

Casal-Otero, L., Catala, A., Fernández-Morante, C., Taboada, M., Cebreiro, B., & Barro, S. (2023). AI literacy in K-12: A systematic literature review. *International Journal of STEM Education*, *10*(1), 29. https://doi.org/10.1186/s40594-023-00418-7

Castillejos López, B., Torres Gastelú, C. A., & Lagunes Domínguez, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura (Guadalajara, Jal.)*, *8*(2), 54-69. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-61802016000300054&lng=es&tlng=es.

Chhikara, J., Dahiya, R., Garg, N., & Rani, M. (2013). Phishing & anti-phishing techniques: Case study. *International Journal of Advanced Research in computer science and software engineering*, *3*(5).

Chong, E. K., & Pao, S. S. (2022). Promoting digital citizenship education in junior secondary schools in Hong Kong: Supporting schools in professional development and action research. *Asian Education and Development Studies*, *11*(4), 677-690.

Cózar-Gutiérrez, R., De Moya-Martínez, M. V., Hernández-Bravo, J. A., & Hernández-Bravo, J. R. (2016). Conocimiento y Uso de las Tecnologías de la Información y las Comunicaciones (TIC) según el Estilo de Aprendizaje de los Futuros Maestros. *Formación universitaria*, *9*, 105-118. http://dx.doi.org/10.4067/S0718-50062016000600010

de Oca, Á. R. M. M., Zermeño, M. G. G., & Gailbraith, L. A. G. (2015). Uso de la plataforma Moodle como apoyo a la docencia presencial universitaria. *Edmetic*, *4*(1), 133-155. https://doi.org/DOI:10.21071/edmetic.v4i1.2903

de Souza Zanirato Maia, J., Bueno, A. P. A., & Joao Ricardo Sato. (2023). Applications of Artificial Intelligence Models in Educational Analytics and Decision Making: A Systematic Review. *World*, *4*(2), 288-313. https://doi.org/10.3390/world4020019

De Waal, E., & Grösser, M. (2014). On safety and security in education: Pedagogical needs and fundamental rights of learners. *Educar*, *50*(2), 0339-0361. https://doi.org/10.5565/rev/educar.44

Del Valle, D. V., Fuente, J. P., & González, J. H. (2018). Competencias tecnológicas de los docentes de universidades colombianas. *Revista Espacios*, *39*(43), 26.

Durán, G. H. (2019). Desarrollo de competencias tecnológicas: Reto fundamental para los profesores universitarios costarricenses. *Revista electrónica calidad en la educación superior*, *10*(2), 34-52. https://doi.org/10.22458/caes.v10i2.1924

Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). Validez de contenido y juicio de expertos: Una aproximación a su utilización. *Avances en medición*, *6*(1), 27-36.

Esteve-Mon, F. M., Gisbert Cervera, M., & Lázaro Cantabrana, J. L. (2016). *La competencia digital de los futuros docentes:¿ cómo se ven los actuales estudiantes de educación?* https://dx.doi.org/10.4151/07189729-Vol.55-Iss.2-Art.412

Estrada, F. J. R., George-Reyes, C. E., & Glasserman-Morales, L. D. (2022). Security as an emerging dimension of Digital Literacy for education: A systematic literature review. *Journal of e-Learning and Knowledge Society*, *18*(2), 22-33.

EUROPEA, C. (2021). Plan de Acción del pilar europeo de derechos sociales. *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. Bruselas: CE*.

Ferrag, M. A., Maglaras, L., Janicke, H., & Smith, R. (2019). Deep learning techniques for cyber security intrusion detection: A detailed analysis. *6th International Symposium for ICS & SCADA Cyber Security Research 2019*. https://doi.org/DOI: 10.14236/ewic/icscsr19.16

Ferrari, A., & Punie, Y. (2013). *DIGCOMP: A framework for developing and*

understanding digital competence in Europe. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC83167/lb-na-26035-enn.pdf,

Flores-Tena, M. J., Ortega-Navas, M. del C., & Sousa-Reis, C. (2021). El uso de las TIC digitales por parte del personal docente y su adecuación a los modelos vigentes. *Revista Electrónica Educare*, *25*(1), 300-320. http://dx.doi.org/10.15359/ree.25-1.16

Fuentes, A., López, J., & Pozo, S. (2019). Análisis de la competencia digital docente: Factor clave en el desempeño de pedagogías activas con Realidad Aumentada. *REICE. Revista Iberoamericana sobre Calidad, eficacia y cambio en educación*, *17*(2), 27-40. https://doi.org/10.15366/reice2019.17.2.002

Gallego-Arrufat, M.-J., Torres-Hernández, N., & Pessoa, T. (2019). Competencia de futuros docentes en el área de seguridad digital. *Comunicar*, *27*(61), 57-67. https://doi.org/10.3916/C61-2019-05

García-Peñalvo, F. J. (2024). Inteligencia artificial generativa y educación: Un análisis desde múltiples perspectivas. *Education in the Knowledge Society (EKS)*, *25*, e31942. https://doi.org/10.14201/eks.31942

García-Peñalvo, F. J., & Vázquez-Ingelmo, A. (2023). What Do We Mean by GenAI? A Systematic Mapping of The Evolution, Trends, and Techniques Involved in Generative AI. *International Journal of Interactive Multimedia & Artificial Intelligence*, *8*(4). https://doi.org/10.9781/ijimai.2023.07.006

Gómez, A. O. T. (2017). Índice de competencias TIC en docentes de educación superior. *Campus Virtuales*, *6*(2), 113-125.

Grande de Prado, M., García-Peñalvo, F. J., Corell, A., & Abella García, V. (2021). Evaluación en Educación Superior durante la pandemia de la COVID-19. *Campus virtuales*, *1*(10), 49-58.

Grisales, N. E. M., & Palacio, E. V. G. (2019). Competencias TIC en docentes de nivel técnico y tecnológico. Un estudio de caso en un centro de formación del SENA. *Revista Virtual Universidad Católica del Norte*, *58*, 74-95. https://doi.org/Doi: 10.35575/rvucn.n58a3

Guillén-Gámez, F. D., Colomo-Magaña, E., Ruiz-Palmero, J., & Tomczyk, Ł.

(2024). Teaching digital competence in the use of YouTube and its incidental factors: Development of an instrument based on the UTAUT model from a higher order PLS-SEM approach. *British Journal of Educational Technology*, *55*(1), 340-362. https://doi.org/10.1111/bjet.13365

Gümüş, M. M., Çakır, R., & Korkmaz, Ö. (2023). Investigation of pre-service teachers' sensitivity to cyberbullying, perceptions of digital ethics and awareness of digital data security. *Education and Information Technologies*, *28*(11), 14399-14421. https://doi.org/10.1007/s10639-023-11785-7

Habibi, A., Razak, R. A., Yusop, F. D., & Mukminin, A. (2019). Preparing future EFL teachers for effective technology integration: What do teacher educators say. *Asian EFL Journal*, *21*(2), 9-30.

Hall, M. (2016). Why people are key to cyber-security. *Network Security*, *2016*(6), 9-10.

Hargittai, E., & Shafer, S. (2006). Differences in actual and perceived online skills: The role of gender. *Social science quarterly*, *87*(2), 432-448. https://doi.org/10.1111/j.1540-6237.2006.00389.x

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (Vol. 6). méxico: mcGraw-Hill. https://dialnet.unirioja.es/servlet/libro?codigo=775008

Hernández-Martín, A., Martín-del-Pozo, M., & Iglesias-Rodríguez, A. (2021). Pre-adolescents' digital competences in the area of safety. Does frequency of social media use mean safer and more knowledgeable digital usage? *Education and Information Technologies*, *26*(1), 1043-1067. https://doi.org/10.1007/s10639-020-10302-4

Hillman, V. (2023). Bringing in the technological, ethical, educational and social-structural for a new education data governance. *Learning, Media and Technology*, *48*(1), 122-137. https://doi.org/10.1080/17439884.2022.2052313

Honig, C. A., & Salmon, D. (2021). Learner presence matters: A learner-centered exploration into the community of Inquiry Framework. *Online Learning*, *25*(2), 95-119.

Hutson, E., Kelly, S., & Militello, L. K. (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.

Ivy, J., Lee, S. B., Franz, D., & Crumpton, J. (2019). Seeding Cybersecurity Workforce Pathways With Secondary Education. *Computer*, *52*(3), 67-75. https://doi.org/10.1109/MC.2018.2884671

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150-158. https://doi.org/10.11591/edulearn.v12i1.7736

Kampylis, P., Punie, Y., & Devine, J. (2015). *Promoting effective digital-age learning-A European framework for digitally-competent educational organisations*. Joint Research Centre (Seville site). https://ideas.repec.org/p/ipt/iptwpa/jrc72277.html

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal*, *36*(2), 373-405. https://doi.org/10.1057/s41284-022-00343-4

Krutka, D. G., Manca, S., Galvin, S. M., Greenhow, C., Koehler, M. J., & Askari, E. (2019). Teaching “against” social media: Confronting problems of profit in the curriculum. *Teachers College Record*, *121*(14), 1-42. https://doi.org/10.1177/016146811912101410

Kumar, V., & Nanda, P. (2019). Social Media to Social Media Analytics: Ethical Challenges. *International Journal of Technoethics (IJT)*, *10*(2), 57-70. https://doi.org/10.4018/IJT.2019070104

Latorre-Medina, M. J., & Tnibar-Harrus, C. (2023). DIGITAL SECURITY IN EDUCATIONAL TRAINING PROGRAMS: A STUDY BASED ON FUTURE TEACHERS’ PERCEPTIONS. *Information Technologies and Learning Tools*, *95*(3), 102-111. https://doi.org/10.33407/itlt.v95i3.5204

Marín, V. I., Carpenter, J. P., Tur, G., & Williamson-Leadley, S. (2023). Social media and data privacy in education: An international comparative study of perceptions among pre-service teachers. *Journal of Computers in Education*, *10*(4), 769-795.

https://doi.org/10.1007/s40692-022-00243-x

Matarrita-Cascante, D., Trejos, B., Qin, H., Joo, D., & Debner, S. (2022). Conceptualizing community resilience: Revisiting conceptual distinctions. En *Community Development for Times of Crisis* (pp. 34-55). Routledge.

Méndez, V. G., Tort, E. G., Rodríguez, M. L. F., & Laverde, A. C. (2021). El profesorado de Educación Infantil y Primaria: Formación tecnológica y competencia digital. *Innoeduca: international journal of technology and educational innovation*, *7*(2), 19-31. https://doi.org/ 10.24310/innoeduca.2021.v7i2.12261

Mendivil Caldentey, J., Sanz Urquijo, B., & Gutierrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: Una revisión sistemática de literatura. *Pixel-Bit: Revista de Medios y Educación, 63, 197-225.* https://doi.org/10.12795/pixelbit.91640.

Montoya, N. E., Mosquera, S. P., Peréz, M. C., & Arroyave, D. I. (2018). Competencias TIC del docente siglo XXI en educación superior. *Revista Espacios*, *39*(53).

Moreira, M. A., Machado, J. F. B., & Santos, M. B. S. N. (2015). Educar a la generación de los Millennials como ciudadanos cultos del Ciberespacio. *Revista de estudios de juventud*, *109*, 13-32.

Mori, I. (2019). *2nd survey of schools ICT in education: Spain country report. Study*. https://doi.org/10.2759/916605

Muammar, S., Hashim, K. F. B., & Panthakkan, A. (2023). Evaluation of digital competence level among educators in UAE Higher Education Institutions using Digital Competence of Educators (DigComEdu) framework. *Education and Information Technologies*, *28*(3), 2485-2508. https://doi.org/10.1007/s10639-022-11296-x

Mugariri, P., Abdullah, H., García-Torres, M., Parameshchari, B. D., & Abdul Sattar, K. N. (2022). Promoting Information Privacy Protection Awareness for Internet of Things (IoT). *Mobile Information Systems*, *2022*, 4247651. https://doi.org/10.1155/2022/4247651

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual

privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413. https://doi.org/10.1016/j.giq.2019.101413

Ngoc, H. D., Hoang, L. H., & Hung, V. X. (2020). Transforming education with emerging technologies in higher education: A systematic literature review. *International Journal of Higher Education*, *9*(5), 252-258.

Novella-García, C., & Cloquell-Lozano, A. (2021). The ethical dimension of digital competence in teacher training. *Education and Information Technologies*, *26*(3), 3529-3541. https://doi.org/10.1007/s10639-021-10436-z

Petelin, A., Galustyan, O., Prosvetova, T., Petelina, E., & Ryzhenkov, A. (2019). Application of educational games for formation and development of ICT competence of teachers. *International Journal of Emerging Technologies in Learning (Online)*, *14*(15), 193. https://doi.org/DOI:10.3991/ijet.v14i15.10572

Pham, H. C., Pedro, A., Le, Q. T., Lee, D.-Y., & Park, C.-S. (2019). Interactive safety education using building anatomy modelling. *Universal Access in the Information Society*, *18*(2), 269-285. https://doi.org/10.1007/s10209-017-0596-y

Pozo Sánchez, S., López Belmonte, J., Fernández Cruz, M., & L´ópez Núñez, J. A. (2020). Análisis correlacional de los factores incidentes en el nivel de competencia digital del profesorado. *Revista Electrónica Interuniversitaria de Formación del Profesorado*, *23*(1). https://doi.org/10.6018/reifop.396741

Pozos Pérez, K. V., & Tejada Fernández, J. (2018). Competencias Digitales en Docentes de Educación Superior: Niveles de Dominio y Necesidades Formativas. *Revista Digital de Investigación en Docencia Universitaria*, *12*, 59-87. http://dx.doi.org/10.19083/ridu.2018.712

Prensky, M. (2001). Digital natives, digital immigrants part 2: Do they really think differently? *On the horizon*, *9*(6), 1-6.

Quan-Haase, A., & Ho, D. (2020). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology*,

71(9), 1089-1102. https://doi.org/10.1002/asi.24364

Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu*. Joint Research Centre (Seville site). https://doi.org/10.2760/159770

Redecker, C. (2020). *Marco europeo para la competencia digital de los educadores: DigCompEdu*.

Ringle, C. M., Wende, S., & Becker, J. M. (2024). *SmartPLS 4. Monheim am Rhein: SmartPLS*. Retrieved from https://www.smartpls.com

Ríos Ariza, J. M., Gómez Barajas, E. R., & Rojas Polanco, M. P. (2018). Valoración de competencias TIC del profesorado universitario: Un caso en Chile. *Pixel-Bit, 52, 55-65.* https://doi.org/10.12795/pixelbit.2018.i52.04

Rodriguez Carracedo, M. C., & de la Barrera Minervini, J. J. (2014). Alfabetización tecnológica para mayores.Experiencia en la UNED Senior, Argentina. *VIRTUALIDAD EDUCACION Y CIENCIA*, *5*(9), 56-69. https://doi.org/DOI: https://doi.org/10.60020/1853-6530.v5.n9.9550

Rodríguez, E. D. C. C. (2019). Importancia del manejo de competencias tecnológicas en las prácticas docentes de la Universidad Nacional Experimental de la Seguridad (UNES). *Revista educación*, 196-218. https://doi.org/10.15517/revedu.v43i1.27120

Rodríguez Espinosa, H., Restrepo Betancur, L. F., & Aranzazu Taborda, D. (2016). Desarrollo de habilidades digitales docentes para implementar ambientes virtuales de aprendizaje en la docencia universitaria. *Sophia*, *12*(2), 261-270. http://dx.doi.org/10.18634/sophiaj.12v.2i.561

Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. *Computers & Education*, *128*, 13-35. https://doi.org/10.1016/j.compedu.2018.09.009

Sonck, N., Livingstone, S., Kuiper, E., & de Haan, J. (2011). *Digital literacy and safety skills*.

Sosa Neira, E. A., Salinas, J., & De Benito, B. (2017). Emerging Technologies

(ETs) in Education: A Systematic Review of the Literature Published between 2006 and 2016. *International Journal of Emerging Technologies in Learning (iJET)*, *12*(05), 128-149. https://doi.org/10.3991/ijet.v12i05.6939

Suárez-Carballo, F. (2020). La enseñanza del diseño gráfico en los grados españoles vinculados a la comunicación publicitaria: Perfil del profesorado, métodos docentes y competencias tecnológicas. *grafica*, *8*(15), 33-42. https://doi.org/10.5565/rev/grafica.170

Tigelaar, D. E., Dolmans, D. H., Wolfhagen, I. H., & Van Der Vleuten, C. P. (2004). The development and validation of a framework for teaching competencies in higher education. *Higher education*, *48*, 253-268.

Torres-Hernandez, N. (2023). Análisis de marcos de competencia digital docente para la formación inicial de profesorado en seguridad digital. *Revista de Estilos de aprendizaje*, *16*(31), 56-68. https://doi.org/10.55777/rea.v16i31.5407

Torres-Hernández, N., & Gallego-Arrufat, M.-J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and Information Technologies*, *27*(6), 8583-8602. https://doi.org/10.1007/s10639-022-10978-w

Uerz, D., Volman, M., & Kral, M. (2018). Teacher educators' competences in fostering student teachers' proficiency in teaching and learning with technology: An overview of relevant research literature. *Teaching and Teacher Education*, *70*, 12-23. https://doi.org/10.1016/j.tate.2017.11.005

United Nations. (2011). *UNESCO ICT Competency Framework for Teachers* (United Nations Educational,Scientific and Cultural OrganizationUNESCO&Microsoft). UNESCO & Microsoft.

Vartiainen, H., Pellas, L., Kahila, J., Valtonen, T., & Tedre, M. (2024). Pre-service teachers' insights on data agency. En *New Media & Society* (Vol. 26, Número 4, pp. 1871-1890). https://doi.org/10.1177/14614448221079626

Viechtbauer, W., Smits, L., Kotz, D., Budé, L., Spigt, M., Serroyen, J., & Crutzen, R. (2015). A simple formula for the calculation of sample size in pilot studies. *Journal of Clinical Epidemiology*, *68*(11), 1375-

1379. https://doi.org/10.1016/j.jclinepi.2015.04.014

Vuorikari, R., Punie, Y., Gomez, S. C., & Van Den Brande, G. (2016). *DigComp 2.0: The digital competence framework for citizens. Update phase 1: The conceptual reference model*. Joint Research Centre. https://ideas.repec.org/p/ipt/iptwpa/jrc101254.html

Vuorikari Rina, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens—With new examples of knowledge, skills and attitudes* (JRC Research Reports JRC128415). Joint Research Centre. https://doi.org/10.2760/115376 (online),10.2760/490274 (print)

Williamson, B., Bayne, S., & Shay, S. (2020). The datafication of teaching in Higher Education: Critical issues and perspectives. *Teaching in Higher Education*, *25*(4), 351-365. https://doi.org/10.1080/13562517.2020.1748811

Williamson, B., Potter, J., & Eynon, R. (2019). New research problems and agendas in learning, media and technology: The editors' wishlist. *Learning, Media and Technology*, *44*(2), 87-91. https://doi.org/10.1080/17439884.2019.1614953

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education*, *186*, 104536. https://doi.org/10.1016/j.compedu.2022.104536