UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS DE LA EDUCACIÓN

Departamento de Didáctica y Organización Escolar

TESIS DOCTORAL

PROGRAMA DE DOCTORADO EN CIENCIASDE LA EDUCACIÓN

ANÁLISIS Y PERCEPCIÓN DE LAS COMPETENCIAS DIGITALES EN SEGURIDAD ADQUIRIDAS DURANTE LA FORMACIÓN INICIAL DEL ALUMNADO UNIVERSITARIO EN CIENCIAS DE LA EDUCACIÓN

DOCTORANDA

CARMEN RODRÍGUEZ JIMÉNEZ

DIRECTOR

JUAN MANUEL TRUJILLO TORRES

CODIRECTOR

SANTIAGO ALONSO GARCÍA

GRANADA, 2023

A mi tío Ricardo, sé que estés donde estés estarás orgulloso de mí

UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS DE LA EDUCACIÓN

Departamento de Didáctica y Organización Escolar

TESIS DOCTORAL

PROGRAMA DE DOCTORADO EN CIENCIASDE LA EDUCACIÓN

ANÁLISIS Y PERCEPCIÓN DE LAS COMPETENCIAS DIGITALES EN SEGURIDAD ADQUIRIDAS DURANTE LA FORMACIÓN INICIAL DEL ALUMNADO UNIVERSITARIO EN CIENCIAS DE LA EDUCACIÓN

PRESENTADO POR CARMEN RODRÍGUEZ JIMÉNEZ

Para optar al Grado de Doctor Internacional por la Universidad de Granada

DIRECTOR

JUAN MANUEL TRUJILLO TORRES

CODIRECTOR

SANTIAGO ALONSO GARCÍA

Trabajo de investigación financiado por el Ministerio de Educación, Cultura y Deporte del Gobierno de España en el Marco del Plan Nacional de Formación del Profesorado Universitario (FPU) con referencia FPU18/01595.

Granada, 2023

Editor: Universidad de Granada. Tesis Doctorales
Autor: Carmen Rodríguez Jiménez
ISBN: 978-84-1195-231-6
URI: https://hdl.handle.net/10481/90555

Agradecimientos

La realización y finalización de este trabajo supone para mí el culmen de uno de los momentos más felices y a la vez más duros de mi vida. Durante estos años como doctoranda han sucedido muchas cosas en vida tanto personal como profesional. Escribir estas líneas supone plasmar en palabras todos aquellos pensamientos que durante este tiempo han estado en mi mente y que, en ocasiones, tan difícil se me ha hecho expresar.

En primer lugar, me gustaría empezar con la persona que apostó por mí, me indicó el camino a seguir y me abrió las puertas de esta gran institución, el profesor Eudaldo Corchón Álvarez. Desde aquel segundo curso en la asignatura de Organización de Centros Educativos supe que algo iba a cambiar en mi vida, pero no sabía hasta qué punto. Comienzo diciendo que, sin duda, esa asignatura me hizo ver lo que es ser un gran docente, solo hacía falta ver cómo daba usted sus clases para darse cuenta de lo que realmente es la pasión y la vocación por ser profesor. Gracias por mostrarme el mundo universitario y haber apostado por mí, por haber estado pendiente de mi camino en todo momento incluso cuando ya no está como profesor, sin embargo, para mí sigue estando presente cada vez que voy a dar clase. Pero sobre todo gracias por ese día que me dijo que me presentaría al que iba a ser mi tutor, que lo hacía porque era una gran persona y que yo no me merecía menos, gracias por presentarme a Juanma. Espero algún día acércame algo a ser lo gran docente que es usted.

Gracias a mis directores, Juan Manuel Trujillo Torres y Santiago Alonso García por haberme acompañado en este camino. Santi gracias por tu buen hacer y tu buen humor siempre que hacen que el camino sea más fácil y agradable.

Pero sin duda, tengo que dedicarle unas líneas más extensas a la persona que ha sido mi tutor de dos becas y mi director de tesis. Juanma, son muchos años ya los que nos unen de manera profesional. No se equivocó Eudaldo cuando me dijo que me presentó a la mejor persona de Didáctica y Organización Escolar y cada día lo confirmo. Sin tu apoyo profesional y personal sabes que no hubiera podido llegar hasta aquí hoy. Gracias por nunca soltarme de la mano, animarme siempre y tener la mentalidad más positiva posible ante cualquier circunstancia. Gracias por respetar mis momentos personales difíciles con comprensión y amabilidad. Sé que es un tópico, pero es necesario decir que eres tan grande por fuera como por dentro.

Estas personas forman parte del gran grupo de investigación AREA (HUM-672), grupo del

que soy afortunada al pertenecer y en primer lugar les doy las gracias en general por tener este sentimiento de unión y pertenencia que nos caracteriza y que hace que todos avancemos como grandes profesionales. Me gustaría hacer una mención especial a Inmaculada Aznar Díaz y a María Pilar Cáceres Reche por haber compartido momentos juntas en su despacho, con anécdotas para el recuerdo y haber aprendido de dos grandes profesionales como ellas; a Francisco Javier Hinojo Lucena por ser siempre un líder que nos guía y nos tiene presentes queriendo siempre lo mejor para cada uno de nosotros; a Juan Antonio López Núñez por su ayuda su buena disposición siempre que le hemos necesitado.

Quiero hacer una mención especial a mis compañeros Juan Carlos de la Cruz, Magdalena Ramos Navas-Parejo, Gerardo Gómez García y Natalia Campos Soto. Gracias por cuidarme y ayudarme y por todos esos momentos de felicidad compartida que hacen que el trabajo diario sea más ameno.

Por otro lado, no puedo olvidarme de la que ahora es mi casa, Melilla. Quiero agradecerles a todos mis compañeros de allí su acogida, su generosidad y hacer que mi estancia allí sea cada día mejor. Gracias a Antonio Manuel Rodríguez García por ser un gran compañero, una gran persona y un gran profesional, la sección de Melilla es mejor porque tú formas parte de ella. Gracias a Marina García Carmona por su simpatía y su ayuda en todo momento. Y gracias a Adrián Segura Robles, por ser mi compañero de batallas, por preocuparte por mí siempre desde que llegué y por abrirme las puertas de tu casa y hacerme sentir que es la mía.

Por último, he dejado a unas personas que, aunque las he conocido en el ámbito académico ya son parte de mi vida personal. Blanca Berral Ortiz, José Antonio Martínez Domingo y Carmen Rocío Fernández Fernández. A vosotros solo puedo deciros que si yo lo he conseguido no dudéis ni por un segundo que sois los siguientes. Me siento tremendamente orgullosa de vosotros y lo que conseguís cada día. Gracias de verdad por haber estado diariamente preocupándoos de si necesitaba ayuda y ofreciéndoos a echarme una mano, porque sé que esos ofrecimientos nacían del corazón. Hemos pasado por muchos momentos como becarios y quiero y deseo que los sigamos pasando como docentes de la universidad.

A mis amigas, ellas saben las que son, sobran las palabras. Pero quiero hacer especial mención a Paloma y a Rocío que me han cuidado en Melilla y me han animado, os llevaré siempre conmigo.

Y ahora sí que paso al terreno personal. Gracias a mi familia, sin ellos no soy nada. Mis padres

Carmen y José Manuel y mi hermano José Manuel. Solo nosotros sabemos lo que me ha costado llegar hasta aquí y cuántas veces he querido dejarlo por no creerme capaz. Gracias porque cuando peor he estado no me habéis soltado la mano y me habéis acompañado en todo este camino sin dudar de mi en ningún momento.

Y ahora, a mi pilar fundamental en la vida, a Jorge. Sin ti no hubiera podido llegar hasta este momento, pero esto solo es un paso más para nuestra vida soñada juntos. Gracias por darme otra familia, otros padres, otros hermanos, Nicolás y Laura y otro hogar, gracias por ser el hombro en el que llorar y la persona que me hace sonreír cada día. Estaremos donde las acreditaciones y las oposiciones nos lleven, pero siempre juntos. Te quiero.

Por último, quiero decir que hoy estoy aquí pero no soy la Carmen de cuando empecé esta tesis, he mejorado como persona y profesional gracias a todas las personas nombradas. He aprendido a quererme y a respetar mi salud mental, a cuidarla y a valorarme como mujer y como profesional. Espero devolveros todo lo que habéis hecho por mí.

Gracias de corazón

ÍNDICE

RESUMEN

La presente tesis doctoral se encuadra dentro de la modalidad de Agrupación de Publicaciones, acorde con las Normas Reguladoras de las Enseñanzas Oficiales de Doctorado y del Título de Doctor por la Universidad de Granada. Esta tesis se compone de las siguientes publicaciones:

Rodríguez-Jiménez, C., Trujillo-Torres, J. M., Berral-Ortiz, B., y De la Cruz-Campos, J. C. (2022). La seguridad dentro de la competencia digital: formación docente en esta área. C. Hervás-Gómez, A. Luque de la Rosa, J.C. de la Cruz-Campos, M.A. Domínguez-González (ed.), *Espacios de aprendizaje e implicaciones prácticas* (pp. 69-79). Dykinson. ISBN 978-84-1122-697-4

Rodríguez-Jiménez, C., Trujillo-Torres, J. M., Moreno-Guerrero, A. J, y Alonso-García, S. (2020). Educación en seguridad digital: estudio bibliométrico sobre el cyberbullying en web of science. *Texto Livre: Linguagem e Tecnologia*, *13*(3), 140-160. https://doi.org/10.35699/1983-3652.2020.25110

Trujillo-Torres, J.M., Rodríguez-Jiménez, C., Alonso-García, S., y Berral-Ortiz, B. (2024). Revisión sistemática de la literatura sobre la Seguridad Digital en estudiantes de Educación Superior. *Información Tecnológica*, En Prensa.

Rodríguez-Jiménez, C., Trujillo-Torres, J.M., Alonso-García, S., y Martínez-Domingo, J.A. (2025). Metaanálisis sobre la Seguridad Digital en Estudiantes de Educación Superior [Metaanalysis on Digital Safety in Higher Education Students]. *Pixel-Bit. Revista de Medios y Educación*, 72, En Prensa.

Rodríguez-Jiménez. C., Trujillo-Torres, J.M., Alonso-García, S., y Martínez-Domingo, J.A. (2023). Evaluación de las Competencias en Seguridad Digital de los Estudiantes de Educación Superior de la Universidad de Granada. En (Coords. G. Estuardo Ceballos Uve, M.J. Santos Villalba, M.J. Alcalá del Olmo Fernández y D. Álvarez Ferrándiz) *Educación integral con perspectivas innovadoras para el desarrollo educativo* (pp. 43-53). Dykinson. ISBN 978-84-1170-706-0.

En este compendio de publicaciones se aborda la relevancia del nivel de competencia en seguridad digital de los estudiantes, pues la competencia digital es un elemento presente en su formación y en todos los procesos de enseñanza-aprendizaje actuales, pero para que esta

sea totalmente eficaz y se haga un uso responsable de la misma es fundamental que se desarrolle el área de seguridad y todas sus características. Si bien, esto debe estar presente en todos los estudiantes de todas las etapas del sistema educativo, resulta aún más importante cuando se trata de discentes que están formándose para ser docentes. Es decir, estudiantes de educación, pues serán aquellos que incluirán también este aspecto en los procesos de enseñanza de sus futuros alumnos.

La seguridad digital como elemento de la competencia digital lleva ya algunos años siendo de vital importancia, pues no solo es importante desarrollar las demás áreas de esta última, si no que estas no pueden alcanzar su máximo exponen sin una correcta seguridad digital, pues el simple hecho de emplear las Tecnologías de la Información y la Comunicación (TIC) y las redes sociales, supone una exposición a diferentes peligros y riesgos.

La primera publicación se trata de una revisión bibliográfica, que tiene como objetivo analizar el contenido de los diferentes estudios realizados y obtener información sobre el estado actual de la cuestión. Se confirma a través de este trabajo la importancia de la seguridad digital en el área educativa y, concretamente, dentro de la formación de los docentes o estudiantes de educación para que estos puedan transmitirla en el ejercicio de su profesión a la vez que ponerla en práctica para su propio aprendizaje.

La segunda publicación tiene la finalidad de analizar la producción científica a través de un estudio bibliométrico sobre la educación existente en cuanto a seguridad digital, especificando dentro de toda la producción sobre una de las mayores problemáticas dentro del ámbito de la seguridad digital, el ciberbullying. Así, a través de el se pretende exponer el rendimiento y producción de la literatura científica sobre ciberbullying; del mismo modo, precisar la evolución científica del concepto de estudio, determinar las temáticas más relevantes en el campo de estudio y establecer los autores más notables dentro de la literatura científica sobre la temática estudiada. La base de datos escogida para la recolección de los documentos fue Web of Science, y se incluyen todas las publicaciones desde el inicio de estas hasta el año 2020, obteniendo así un total de 474 publicaciones científicas tras refinar y emplear determinadas categorías dadas por la propia base de datos. se llega a la conclusión de que este fenómeno se ha acrecentado como forma de comunicación entre los estudiantes en los últimos años y, a la par, ha aumentado, aunque de manera discontinua, el número de investigaciones específicas a este respecto.

La tercera publicación consiste en una revisión sistemática de la literatura sobre la seguridad digital en la etapa de la Educación Superior. La finalidad de esta investigación reside en el análisis de las prácticas actuales de seguridad digital, ciberseguridad o seguridad en internet o en línea, así como el empleo de las tecnologías en Educación Superior. Lo que se quiere lograr es obtener las mejores prácticas y estrategias que mejoren la seguridad digital en esta etapa educativa para poder así, reducir el riesgo de ciberdelitos o problemas derivados del uso de la tecnología que puedan tener estos estudiantes.

Tras todo esto, la cuarta publicación realiza un metaanálisis sobre la seguridad digital en estudiantes de Educación Superior. Esta investigación tiene como finalidad estimar el beneficio de una serie de investigaciones sobre la temática expuesta. Los estudios que analiza este metaanálisis abordan los aspectos más relevantes de los riesgos en línea, la alfabetización digital de futuros docentes y la necesidad de capacitación en seguridad digital de los docentes universitarios. La producción analizada llega hasta el año 2022 y se centra en estudios empíricos dentro de la etapa educativa ya indicada. Se analizan un total de ocho estudios que establecen que dentro de la competencia digital la seguridad es el área menos desarrollada, a pesar de que esta está presente como contenido trasversal en los programas de estudios de esta etapa.

La última publicación se trata de los resultados obtenidos tras pasar un cuestionario ya validado sobre el nivel de seguridad digital de los estudiantes de educación, en este caso, de la Universidad de Granada. este estudio ha sido realizado con el objetivo de averiguar e interpretar el grado de conocimiento y aplicación de buenos mecanismos de seguridad digital en todas las subáreas de la seguridad digital. La metodología empleada es de corte cuantitativo a través del empleo del cuestionario y el diseño escogido es transversal, exploratorio, descriptivo y correlacional. Como resultados se obtiene el área de seguridad está presente en la competencia digital de los estudiantes; sin embargo, existen algunos elementos más desarrollados que otros. Del mismo modo, existen diferencias entre hombres y mujeres en determinadas subáreas. Además, gracias a el modelo de regresión empleado para el análisis de resultados se puede saber a qué áreas se les proporciona una mayor importancia y presencia en la formación de estudiantes y, es por eso, que obtienen mayores puntuaciones.

Palabras clave: Educación Superior; seguridad digital; competencia digital; TIC y estudiantes

ABSTRACT

This doctoral thesis falls within the modality of Grouping of Publications, in accordance with the Regulatory Norms of the Official Doctoral Studies and the Doctoral Degree of the University of Granada. This thesis is made up of the following publications:

Rodríguez-Jiménez, C., Trujillo-Torres, J. M., Berral-Ortiz, B., y De la Cruz-Campos, J. C. (2022). La seguridad dentro de la competencia digital: formación docente en esta área. C. Hervás-Gómez, A. Luque de la Rosa, J.C. de la Cruz-Campos, M.A. Domínguez-González (ed.), *Espacios de aprendizaje e implicaciones prácticas* (pp. 69-79). Dykinson. ISBN 978-84-1122-697-4

Rodríguez-Jiménez, C., Trujillo-Torres, J. M., Moreno-Guerrero, A. J, y Alonso-García, S. (2020). Educación en seguridad digital: estudio bibliométrico sobre el cyberbullying en web of science. *Texto Livre: Linguagem e Tecnologia*, *13*(3), 140-160. https://doi.org/10.35699/1983-3652.2020.25110

Trujillo-Torres, J.M., Rodríguez-Jiménez, C., Alonso-García, S., y Berral-Ortiz, B. (2024). Revisión sistemática de la literatura sobre la Seguridad Digital en estudiantes de Educación Superior. *Información Tecnológica*, En Prensa.

Rodríguez-Jiménez, C., Trujillo-Torres, J.M., Alonso-García, S., y Martínez-Domingo, J.A. (2025). Metaanálisis sobre la Seguridad Digital en Estudiantes de Educación Superior [Metaanalysis on Digital Safety in Higher Education Students]. *Pixel-Bit. Revista de Medios y Educación*, 72, En Prensa.

Rodríguez-Jiménez. C., Trujillo-Torres, J.M., Alonso-García, S., y Martínez-Domingo, J.A. (2023). Evaluación de las Competencias en Seguridad Digital de los Estudiantes de Educación Superior de la Universidad de Granada. En (Coords. G. Estuardo Ceballos Uve, M.J. Santos Villalba, M.J. Alcalá del Olmo Fernández y D. Álvarez Ferrándiz) *Educación integral con perspectivas innovadoras para el desarrollo educativo* (pp. 43-53). Dykinson. ISBN 978-84-1170-706-0.

This compendium of publications addresses the relevance of students' level of competence in digital security, as digital competence is an element present in their training and in all current teaching-learning processes, but for it to be fully effective and for it to be used responsibly, it is essential that the area of security and all its characteristics are developed. While this must be

present in all students at all stages of the education system, it is even more important when it comes to students who are training to be teachers. Students of education, as they will be the ones who will also include this aspect in the teaching processes of their future students.

Digital safety as an element of digital competence has been of vital importance for some years now, as it is not only important to develop the other areas of digital competence, but they cannot reach their full potential without proper digital safety, as the simple fact of using Information and Communication Technologies (ICT) and social networks means exposure to different dangers and risks.

The first publication is a literature review, which aims to analyse the content of the different studies carried out and to obtain information on the current state of the issue. This work confirms the importance of digital safety in the field of education and, specifically, in the training of teachers or education students so that they can transmit it in the exercise of their profession as well as putting it into practice for their own learning.

The second publication aims to analyse the scientific production through a bibliometric study on existing education in terms of digital security, specifying within all the production on one of the biggest problems within the field of digital security, cyberbullying. Thus, the aim is to expose the performance and production of the scientific literature on cyberbullying; in the same way, to specify the scientific evolution of the study concept, to determine the most relevant topics in the field of study and to establish the most notable authors within the scientific literature on the studied topic. The database chosen for the collection of the documents was Web of Science, and all publications from the beginning of these until the year 2020 are included, thus obtaining a total of 474 scientific publications after refining and using certain categories given by the database itself. The conclusion is that this phenomenon has increased as a form of communication among students in recent years and, at the same time, the number of specific research on this subject has increased, albeit discontinuously.

The third publication is a systematic review of the literature on digital safety in higher education. The aim of this research is to analyse current practices in digital security, cybersecurity or internet or online security, as well as the use of technologies in higher education. The aim is to obtain the best practices and strategies to improve digital security at this educational stage to reduce the risk of cybercrime or problems arising from the use of technology that these students may have.

After all this, the fourth publication carries out a meta-analysis on digital security in higher education students. The aim of this research is to estimate the benefit of a series of studies on the subject. The studies analysed in this meta-analysis address the most relevant aspects of online risks, the digital literacy of future teachers and the need for digital security training for university teachers. The production analysed goes up to the year 2022 and focuses on empirical studies within the educational stage. A total of eight studies are analysed which establish that within digital competence, security is the least developed area, even though it is present as cross-cutting content in the syllabuses of this stage.

The last publication deals with the results obtained after passing a validated questionnaire on the level of digital security of education students, in this case, at the University of Granada. This study has been carried out with the aim of finding out and interpreting the degree of knowledge and application of good digital security mechanisms in all sub-areas of digital security. The methodology used is quantitative through the use of a questionnaire and the chosen design is cross-sectional, exploratory, descriptive and correlational. The results show that the area of security is present in the digital competence of students; however, some elements are more developed than others. Similarly, there are differences between men and women in certain sub-areas. Furthermore, thanks to the regression model used for the analysis of the results, it is possible to know which areas are given greater importance and presence in the training of students and, therefore, obtain higher scores.

Keywords: Higher Education; digital security; digital competence; ICT and students.

INTRODUCCIÓN

Actualmente, las TIC están presentes todos los aspectos de la vida. Desde hace ya varias décadas los dispositivos digitales dominan todas las áreas de la sociedad siendo imprescindibles para el día a día. La capacidad de manejo de estos dispositivos se denomina competencia digital (Cabero-Almenara, et al., 2020). El desarrollo de esta habilidad supone un uso correcto y consciente de las TIC teniendo en cuenta todos y cada uno de sus elementos (Lemus, 2017; Ramas Arauz, et al., 2015).

La competencia digital, por tanto, se ha convertido en uno de los términos en auge en los últimos años por su importancia en la educación. Es una de las ocho competencias clave que se determinan en las diferentes normativas y leyes a nivel nacional e internacional (Manassero-Mas y Vázquez Alonso, 2020). Por eso, conocer en qué se basa este concepto, así como su desglose, se hace imprescindible en el momento presente.

A medida que a lo largo de los años este término se ha ido haciendo más presente, también se ha ido investigando sobre el mismo y qué conlleva. Es así como se llega hasta las áreas de la competencia digital. En concreto, estás áreas son cinco, y desmiembran los elementos, conocimientos, habilidades y actitudes que componen la competencia digital. Trabajar todas ellas de modo que se desarrollen de manera adecuada resulta fundamental para ser competente digitalmente (Cabero Almenara, et al., 2021).

Es el área 4 referente a la seguridad digital la que recientemente ha adquirido más relevancia por lo que supone un inadecuado o inexistente desarrollo de esta parte de la competencia digital, y es esta la que ocupa la temática central de esta tesis doctoral.

A pesar de que las ventajas relativas a la tecnología son incontables, esto no supone que esta quede exenta de inconvenientes y problemas derivados de un mal uso o un desconocimiento por parte de los usuarios (Ghislieri, et al., 2022; Vidal, 2021). Son sobradamente conocidos términos como bullying, cyberbulling o ciberacoso, ghosting, grooming, sexting, suplantación de la identidad, entre un largo etcétera (Mladenović, et al., 2021; Pérez, et al., 2020; Walrave y Heirman, 2011). Todos estos términos han aflorado en los últimos años y son exclusivos del uso de internet a través de diferentes dispositivos.

Así pues, se puede observar cómo en determinados momentos la seguridad digital de todos los usuarios está en jaque por diversas causas. El mecanismo más básico para atajar estas

problemáticas radica entonces en una correcta formación ante estos supuestos.

La formación debe recibirse desde las primeras etapas dentro del sistema educativo pues actualmente todos los estudiantes que ingresan en el sistema son nativos digitales (Kesharwani, 2020), es decir, han nacido en una sociedad del conocimiento y de las TIC y, por ende, disponen desde pequeños de una gran cantidad de educación informal sobre este aspecto.

Por tanto, es necesario establecer que la seguridad digital es un tema crucial en la actualidad, especialmente en el ámbito de la educación.

La inclusión de la tecnología en las aulas ha abierto nuevas posibilidades de enseñanza y aprendizaje, pero también ha expuesto a los estudiantes y educadores a nuevos riesgos (Alvarez-Flores, 2021; García-Ruiz, y Escoda, 2021; López Berlanga y Sánchez Romero, 2019). Por lo tanto, es esencial que se preste atención a la seguridad digital en esta área para garantizar un entorno de aprendizaje seguro y saludable.

Entre los riesgos en línea que pueden sufrir los usuarios están el acoso cibernético, el robo de identidad, el acceso no autorizado a información personal y la exposición a contenido inapropiado, entre otros muchos. Además, las escuelas y las instituciones educativas almacenan gran cantidad de datos sensibles y confidenciales, como información personal y académica de los estudiantes, que deben ser protegidos adecuadamente (Latorre-Medina y Tnibar-Harrus, 2023).

Por lo tanto, este ámbito es esencial para proteger a los estudiantes y los docentes y todo lo que de su formación y trabajo se deriva. Al mismo tiempo, también es necesaria para garantizar un entorno de aprendizaje seguro y saludable para los estudiantes, lo que contribuye a mejorar la calidad de la educación y a la formación de ciudadanos responsables y conscientes en línea (Chou y Peng, 2011; De Waal y Grösser, 2014) dentro de la sociedad de la información y la comunicación en la que actualmente nos enmarcamos.

En este sentido, los sistemas educativos deben prestar especial atención a la formación y capacitación en seguridad digital para los docentes, estudiantes y otros miembros y agentes implicados en la comunidad educativa.

Sin embargo, la pregunta a este respecto es clara ¿Están los educadores, docentes y futuros docentes correctamente formados a este respecto? Y, por otro lado, ¿son conscientes de la

importancia de esta temática hoy en día?

De este modo, la etapa de Educación Superior (Rodríguez-García, et al., 2019) se postula como el momento más adecuado para formar a los futuros docentes (Cabero-Almenara y Martínez, 2019) de las diferentes etapas, pues es en este periodo universitario en el cual adquieren todas las competencias profesionales necesarias para el correcto desarrollo de su labor profesional, en este caso, labor docente, donde se incluye la competencia digital y su seguridad.

Tal es así, que la seguridad digital como elemento de relevancia dentro de la competencia digital, cada vez se tiene más en cuenta como elemento transversal en la formación de estudiantes de educación (Garzón Artacho, et al., 2020).

Se ha optado por la selección del Marco Común De Competencia Digital Docente del año 2017 (INTEF, 2017) como marco de referencia y guía a lo largo de toda la tesis doctoral. De igual manera, tal y como este marco está estructurado ha servido para la elección del cuestionario y la realización del marco teórico. Todo esto a pesar de que existe una versión actualizada del mismo.

Esto se debe a que en la versión que aquí se utiliza, es decir, la del año 2017, el área de seguridad está como área propia dentro de la competencia digital, mientras que en la versión actualizada las diferentes subáreas o aspectos de esta se integran en las nuevas áreas que se establecen que pasan de ser 5 a ser 6.

Se considera que en un primer momento y en una primera investigación es relevante conocer y analizar el nivel de seguridad digital como área propia, para después poder analizarlo en un futuro como área integrada en las demás y comprobar cómo influye la seguridad digital en los demás elementos de la competencia digital.

1. MARCO TEÓRICO

1.1. Competencia digital y competencia digital docente

Actualmente en el sistema educativo conviven diversas generaciones tanto en los docentes como en los estudiantes. Así, los estudiantes que ahora mismo se encuentran en Educación Superior van desde la denominada Generación Z (1994-2010), donde estarían la mayoría, pasando por los Millennials o generación Y (1981-1993), Generación X (1969-1980), etcétera. Esto supone que un porcentaje bastante elevado de ellos son nativos digitales (Prensky, 2011), elemento fundamental en su formación y a lo largo de toda su vida.

Los nativos digitales se caracterizan por tener presente en su vida cotidiana el uso de dispositivos tecnológicos, internet, el móvil, videojuegos, entre otras cosas (Castillejos-López et al., 2016). Sin embargo, esto no quiere decir que su competencia digital esté correctamente desarrollada o que sepa hacer un buen uso de la misma.

El término de competencia digital lleva ya entre nosotros varias décadas, poco a poco desde la aparición de este concepto los sistemas educativos, las diferentes legislaciones, los marcos de referencia y los programas formativos han ido cambiando y adaptándose para adecuarse a este término y todo lo que implica. De este modo, existen muchas definiciones del término competencia digital, si se parte de la Recomendación Europea de 2006 (citado por Rodríguez-García, et al., 2017), la competencia digital es realizar un uso crítico y seguro de las TIC con el objetivo de desempeñar un trabajo o cualquier actividad de tiempo libre y comunicación; para ello hay que disponer de habilidades TIC como el empleo de ordenadores para la recolección, producción, evaluación e intercambio de información de diversos lugares, de igual modo que para la comunicación y participación en redes colaborativas a través de Internet.

Se ha de destacar que desde la implantación en el sistema educativo español de las competencias clave (LOE, 2006), una de ellas es la competencia digital, por lo que su relevancia en todas las etapas educativas es muy significativa. Más adelante, en la Orden ECD/65/2015 se define competencia digital como la necesidad de adaptación a los cambios que van sucediendo como consecuencia del desarrollo de las TIC, necesidad de adoptar una serie de conocimientos y un lenguaje propio de las TIC que permita, por tanto, desarrollar y emplear aptitudes para procesar la información y la comunicación, crear contenidos, tener seguridad digital y resolver problemas asociados al uso de las TIC.

En este mismo sentido, desde el Ministerio de Educación y Formación Profesional, concretamente desde su órgano específico para las tecnologías educativas, el INTEF (Instituto Nacional de Tecnologías Educativas y Formación del Profesorado), se ha proporcionado una definición concreta del concepto de competencia digital:

"Uso creativo, crítico y seguro de las tecnologías de la información y comunicación para alcanzar los objetivos relacionados con el trabajo, la empleabilidad, el aprendizaje, el tiempo libre, la inclusión y la participación en la sociedad" (INTEF, 2017, p.9)

Es, por tanto, evidente la importancia de esta competencia dentro del sistema educativo y, como parte de este sistema, dentro de la formación de los docentes, pues de ellos va a depender que esta se mejore y se traspase al resto de estudiantes independientemente del nivel donde se encuentren (Martínez-Garcés, y Garcés-Fuenmayor, 2020).

En este momento entonces surge el concepto de Competencia Digital Docente (CDD), el cual surge como necesidad de especificar dentro de la competencia digital de todos los usuarios una competencia digital orientada a la labor profesional de los profesores y al proceso de enseñanza-aprendizaje.

El objetivo principal de la CDD no es incluir la tecnología a la enseñanza (Gros, 2016), sino aportar y desarrollar conocimientos, habilidades y actitudes que permitan diseñar oportunidades de aprendizaje para los estudiantes, facilitando así su desarrollo personal y el de los docentes (Ala-Mutka, et al., 2008).

La CDD se refiere a la tecnología, pero es también un concepto pedagógico que se enmarca en un contexto educativo y que dota de sentido la actividad profesional (Tárraga-Mínguez, et al., 2021). Va más allá de la simple eficacia técnica que pueda tener el docente a la hora de manejar diferentes dispositivos tecnológicos. Es por eso por lo que ya se han superado términos como la alfabetización digital, pues esta sería solo una parte o un área específica de la CDD (Suárez-Guerrero, et al., 2020).

La CDD se ha convertido así en una característica esencial del nuevo perfil de docente y es esencial en su formación. Es por eso por lo que se van a desarrollar todos sus elementos y marcos de referencia para comprenderla mejor, conocer sus áreas y poner en el foco concretamente en una de sus áreas por el objeto de estudio de esta tesis doctoral.

1.1.1. Áreas de la competencia digital y sus marcos de referencia

La competencia digital ha sido en los últimos años objeto de multitud de investigaciones, innovaciones y, como consecuencia, se han ido diseñando y perfilando diferentes marcos de referencia de diversa índole para ir definiendo todos los términos y características de este concepto.

A este respecto, existen diferentes niveles de concreción en cuanto a estos marcos de referencia. A nivel internacional el más reseñable es el Informe Horizon (EDUCASE, 2022), se trata de un informe de carácter anual que tiene como finalidad informar sobre las tendencias clave en el mundo educativo y tecnológico, así como de aquellas tecnologías que están emergiendo y que probablemente tengan un papel importante en el futuro. Este informe se centra en la etapa de Educación Superior, analizando su estado actual y realizando previsiones sobre cómo se encontrará en escenarios futuros con todos los datos que expone acerca de las tecnologías y en periodos de corto, medio y largo plazo.

A nivel europeo son muchos los marcos que se ofrecen desde las instituciones. En un primer momento se diseñó el DigComp (European Commission, 2013), el cual pretende desarrollar la competencia digital de todos los ciudadanos de Europa; este establece cuáles son las habilidades necesarias para ser digitalmente competente y organiza estas habilidades en tres categorías: conocimientos, habilidades y actitudes. De igual modo, establece diferentes niveles dentro de cada competencia y ayuda a través de todo este material a los responsables políticos para que puedan crear políticas que favorezcan la adquisición de esta competencia digital.

Más tarde, este fue actualizado y reemplazado por el DigComp 2.0 (European Commission, 2016), las diferencias más significativas con respecto a la versión anterior son redefinir los conceptos clave, aportar más vocabulario y rediseñar los descriptores. En el siguiente año, se actualizó de nuevo a la versión DigComp 2.1 (European Commission, 2017), en la cual se ofrecen 8 niveles de competencia y ejemplos de uso aplicados al ámbito del aprendizaje y el empleo.

Recientemente, en el año 2022, se ha vuelto a realizar una actualización de este marco obteniendo así la versión DigComp 2.2 (European Commission, 2022). En este documento ahora encontramos una mayor cantidad de ejemplos tanto de conocimientos, como de habilitades y actitudes; así como, la introducción de tecnologías emergentes como la Inteligencia Artificial, entre otras. Además, aporta todo el material de referencia existente al respecto y que hasta el momento ha sido publicado.

De manera más específica se elaboró también un marco de referencia derivado de estos, pero específicamente diseñado para los educadores como usuarios de las tecnologías y las redes, el DigCompEdu (European Commission, 2017). Va dirigido a todos los docentes independientemente de la etapa educativa donde estos ejerzan su profesión. Además, tiene en cuenta contextos formales y no formales y la atención al alumnado con necesidades educativas. La finalidad de este marco de referencia es proporcionar a cualquier entidad, pública o privada, nacional o regional, entre otras características, para que formen adecuadamente a los docentes a este respecto.

A nivel nacional destaca el Marco Común de Competencia Digital Docente (INTEF, 2022). Se trata de un documento diseñado por el INTEF (Instituto Nacional de Tecnologías Educativas y Formación del Profesorado), el cual pertenece al Ministerio de Educación y Formación Profesional. Así, puede comprobarse cómo en el 2017 con la primera versión de este, lo que se ofrece es una adaptación al español del DigComp y el DigCompEdu, teniendo en cuanto a contenido los mismos elementos y pretendiendo los mismos objetivos.

De igual modo, en el año 2022, este ha sufrido una actualización. Actualmente a nivel nacional se tiene el Marco de Referencia de la Competencia Digital Docente (MCCDD) (INTEF, 2022). Esta versión aúna todos los marcos europeos y los adapta al contexto español. Asimismo, cambia los criterios a la hora de establecer los niveles para que así estos puedan adaptarse a las etapas del desarrollo profesional del educador. Como se comprobará más adelante, esta no es la única modificación con respecto al contenido que realiza este marco de referencia.

En cuanto a las áreas de competencia son muchos los marcos de referencia, aquí explicados, que abordan la clasificación de estas, así como sus elementos y diferentes niveles.

A continuación, puede comprobarse la comparación entre las áreas de competencia que definen en los diferentes marcos de referencia tanto europeos como nacionales (tabla 1):

Tabla 1

Comparativa de las áreas de la competencia digital entre distintos marcos de referencia

	DigComp (2016)	**DigCompEdu (2020)**	**Marco Común de Competencia**	**Marco de Referencia de la Competencia Digital Docente (2022)**

			Digital Docente (2017)	
Área 1	Información y alfabetización de datos	Selección de contenidos digitales	Información y alfabetización informacional	Compromiso profesional
Área 2	Comunicación y colaboración	Creación y modificación de contenidos digitales	Comunicación y colaboración	Contenidos digitales
Área 3	Crear contenidos digitales	Protección, gestión e intercambio de contenidos digitales	Creación de contenidos digitales	Enseñanza y Aprendizaje
Área 4	Seguridad		Seguridad	Evaluación y retroalimentación
Área 5	Solución de problemas		Resolución de problemas	Empoderamiento del alumnado
Área 6				Desarrollo de la competencia digital del alumnado

Como se puede comprobar en esta tabla, aunque la mayoría de los elementos son comunes, existen diferencias notables, como aquellos huecos en blanco en algunos de los maros, pues para esa área no tienen nada especificado. A nivel europeo se puede comprobar cómo hay bastantes diferencias entre el marco dirigido a la ciudadanía en general y el dirigido a los educadores. Por otro lado, aunque los dos marcos de referencia nacionales son muy parecidos, la diferencia principal reside en la creación de una nueva área competencia en el marco más actual, algo que cambia totalmente el sentido de las otras áreas.

En esta tesis se va a tomar como referencia el MCCDD (INTEF, 2017), pues fue el que estaba en vigor cuando se empezó este trabajo y porque a pesar de existir una actualización del mismo, esta supone una especificación de las áreas de competencia, por lo que se podría estudiar con él no supone lo mismo que se puede estudiar con este.

Así, en este marco las áreas son cinco, como está reflejado en la tabla. Sin embargo, esta clasificación va más allá y todas las áreas a su vez están divididas en subáreas que contienen diferentes ítems. A continuación, se muestra esta división (tabla 2):

Tabla 2.

Áreas y subáreas de la competencia digital según el MCCDD

Áreas	**Subáreas**
Área 1. Información y alfabetización informacional	C.1.1. Navegación, búsqueda y filtrado de información, datos y contenidos digitales
	C.1.2. Evaluación de información, datos y contenidos digitales.
	C.1.3. Almacenamiento y recuperación de información, datos y contenidos digitales
Área 2. Comunicación y colaboración	C.2.1. Interacción mediante las tecnologías digitales
	C.2.2. Compartir información y contenidos digitales
	C.2.3. Participación ciudadana en línea
	C.2.4. Colaboración mediante canales digitales
	C.2.5. Netiqueta
	C.2.6. Gestión de la identidad digital
Área 3. Creación de contenidos digitales	C.3.1. Desarrollo de contenidos digitales
	C.3.2. Integración y reelaboración de contenidos digitales
	C.3.3. Derechos de autor y licencias
	C.3.4. Programación

Área 4. Seguridad	C.4.1. Protección de dispositivos
	C.4.2. Protección de datos personales e identidad digital
	C.4.3. Protección de la salud
	C.4.4. Protección del entorno
Área 5. Resolución de problemas	C.5.1. Resolución de problemas técnicos
	C.5.2. Identificación de necesidades y respuestas tecnológicas
	C.5.3. Innovación y uso de la tecnología digital de forma creativa
	C.5.4. Identificación de lagunas en la competencia digital

Como se puede ver la competencia digital está compuesta por cinco áreas las cuales en total contienen un total de 21 competencias. Además, es importante señalar que el marco establece seis niveles progresivos de manejo de las competencias, estos se dividen de la siguiente manera:

- Nivel básico:
    - A1. El usuario en este nivel necesita apoyo para poder desarrollar su competencia digital.
    - A2. El usuario en este nivel tiene un poco de autonomía y conjuntamente con apoyo puede desarrollar su competencia digital.
- Nivel intermedio:
    - B1. El usuario en este nivel es capaz de resolver por sí mismo problemas sencillos que le surjan a la hora de desarrollar su competencia digital.
    - B2. El usuario en este nivel es capaz de responder a las necesidades propias que le surjan y los problemas asociados para desarrollar su competencia digital.
- Nivel avanzado:

- C1. El usuario en este nivel es capaz de guiar a otras personas para que desarrollen su competencia digital.
- C2. El usuario en este nivel es capaz de responder a las necesidades propias y ajenas en contextos complejos.

1.2.Seguridad digital

La seguridad digital dentro de la competencia digital hace referencia al conjunto de conocimientos, habilidades y actitudes que el usuario tiene y emplea para ser digitalmente responsable (Gallego-Arrufat, et al., 2019). Esto implica proteger la información y la comunicación ante los problemas que puedan surgir derivados de utilizar las TIC, también está relacionada con la privacidad, integridad y eficacia de la tecnología e información existente en la red (Anderson, 2003; Barrow y Heywood-Everett, 2006).

Es necesario entender la seguridad digital como algo fundamental en la sociedad de este siglo. Los entornos digitales donde ya todo el mundo se desenvuelve deben ser seguros y los usuarios deben ser conscientes de los riesgos y peligros existentes (Area, et al., 2015; Muñoz-Rodríguez, et al., 2020).

Como se ha expuesto anteriormente, la competencia en seguridad digital tiene como objetivo que el usuario sepa cómo proteger los dispositivos, cómo proteger los datos personales, cómo proteger el bienestar personal y la salud y cómo proteger el entorno. A continuación, se exponen algunas de las posibles problemáticas relacionadas con estas competencias de la seguridad digital (Dodel y Mesch, 2018; Gamito Gómez, et al., 2020; Schwartz y Lonborg, 2011):

Tabla 3.

Competencias de la seguridad digital y sus peligros

Competencia	Peligros asociados
Protección de dispositivos	Amenazas en red (virus, correo spam, phishing, etc.)
Protección de datos personales	Amenazas, fraudes, cyberbullying, hackeos, extorsión, etcétera.

Protección de la salud y el bienestar personal	Conductas adictivas, trastornos de sueño y atención, problemas corporales. Descenso de la calidad de vida. Nomofobia.
Protección del entorno	Nula optimización de los tiempos de conexión, despilfarro energético, etcétera.

Una vez conocidas las competencias o subáreas dentro del área de seguridad digital, se va a desgranar en qué consiste cada subárea (INTEF, 2017, p. 49-55):

- Protección de dispositivos: proteger los dispositivos y los contenidos digitales propios, comprender los riesgos y amenazas en red, y conocer medidas de protección y seguridad.
- Protección de datos personales: entender los términos habituales de uso de los programas y servicios digitales, proteger activamente los datos personales, respetar la privacidad de los demás y protegerse a sí mismo/a de amenazas, fraudes y ciberacoso.
- Protección de la salud y el bienestar personal: evitar riesgos para la salud relacionados con el uso de la tecnología en cuanto a amenazas para la integridad física y el bienestar psicológico.
- Protección del entorno: tener en cuenta el impacto de las tecnologías sobre el medio ambiente.

En los últimos años son muchas las investigaciones existentes al respecto de la seguridad digital y su papel en diferentes áreas y contextos, no solo el educativo. Así, se pueden observar estudios sobre seguridad digital en el ámbito de derecho (Reigada, 2018), de la economía (Álvarez-Flores, et al., 2019), la psicología (Carabel, et al., 2019). Esto no hace si no reforzar la idea de la importancia de la seguridad digital en todos los aspectos de la sociedad y de cualquier usuario, por lo tanto, la formación a este respecto debe darse en todas las etapas y, sobre todo, en la de formación inicial para el desarrollo de las profesiones, es decir, en Educación Superior.

1.2.1. Seguridad digital en el sistema educativo español

Si se pone el foco en el sistema educativo español, se puede comprobar cómo la situación actual de la seguridad digital en este es compleja y desafiante, debido a los rápidos cambios en las tecnologías digitales y el aumento de los riesgos y amenazas en línea. Aunque se han realizado esfuerzos para mejorar la seguridad digital en el sistema educativo, aún existen áreas de mejora en este ámbito.

En España, se han establecido políticas y regulaciones de seguridad digital en el sistema educativo, incluyendo la Ley Orgánica de Protección de Datos (LOPD, 2018) y la Guía para Centros Educativos (AEPD, 2019), que establecen los requisitos y estándares de seguridad para la protección de datos personales y la privacidad en línea en el ámbito educativo. Además, el Ministerio de Educación y Formación Profesional estableció ya hace una década un Plan de Cultura Digital en la Educación (INTEF, 2013), que tiene como objetivo fomentar la educación en competencias digitales y la cultura digital en las escuelas españolas.

Más recientemente, el gobierno estatal ha lanzado la estrategia España Digital 2026 (MAETD, 2020), esta propuesta tiene varias dimensiones clave, que articulan toda la estrategia, destaca la relativa a Infraestructuras y Tecnología ya que recoge como uno de los puntos principales la ciberseguridad. Demostrando así, su papel crítico para avanzar a nivel digital como sociedad.

A pesar de estos esfuerzos, los riesgos y amenazas en línea siguen siendo un problema en el sistema educativo español. Según el informe "Net Childresn. Go Mobile. Riesgos y oportunidades en internet y uso de dispositivos móviles entre menores españoles (2010-2015)" (Garmendia, et al., 2016), el 55% de los estudiantes españoles ha sufrido algún tipo de riesgo en línea, como acoso cibernético, exposición a contenidos inapropiados y suplantación de identidad. Además, según el mismo informe, solo el 16% de los docentes españoles considera que está suficientemente formado en seguridad digital.

Por lo tanto, es necesario seguir trabajando en la mejora de la seguridad digital en el sistema educativo español, especialmente en la formación y capacitación de los docentes para que así, estos puedan a su vez formar a los estudiantes y que todos sean poseedores de una correcta responsabilidad digital. También es importante fomentar la conciencia y la responsabilidad en línea entre los estudiantes y la comunidad educativa en general, para garantizar un entorno de aprendizaje seguro y saludable en línea.

1.3.Seguridad digital en la etapa de Educación Superior

Como se ha podido ir comprobando, la competencia digital en todas sus áreas resulta fundamental en todas las etapas educativas, destacando la etapa de Educación Superior como objeto de infinidad de investigaciones para comprobar el nivel de implementación de este elemento en los procesos de enseñanza-aprendizaje (Restrepo-Palacio y Segovia Cifuentes; 2020; Vargas-Murillo, 2019), las ventajas y desventajas que tiene (García Vélez, et al., 2021; Limas Suárez y Vargas Soracá, 2020; Matienzo López, 2020), los nuevos roles de todos los agentes implicados (D'Antonio y de Lima Pancorbo, 2019), y otros muchos elementos.

1.3.1. Nivel de seguridad digital en estudiantes de educación

Los futuros docentes en la actualidad cuentan con una formación holística que aborda todas las necesidades que la sociedad les pide para un correcto desarrollo en la misma y una correcta incorporación en el mundo laboral.

Sin embargo, aunque las TIC y la competencia digital llevan presentes muchos años en todos los programas educativos como elementos únicos o transversales, se sigue demostrando que existen dificultades a la hora de que estos docentes en formación apliquen las TIC en los procesos educativos (Cantón, et al., 2017; López-Gil y Bernal-Bravo, 2019; Rodríguez-García, et al., 2019).

A pesar de esto, las TIC y la competencia digital se siguen teniendo siempre presentes y cada vez más surgen propuestas e investigaciones que abogan por proporcionar recursos y materiales que faciliten estos procesos de inclusión. Pero la seguridad digital queda al margen en muchos de estos casos, siendo las demás áreas de la competencia principal las protagonistas olvidándose de la protección de los dispositivos, los datos personales, el bienestar personal o el entorno.

Aun así, algunas investigaciones concretas han abordado el papel que tienen los estudiantes de Educación Superior ante la seguridad digital aplicada al uso de las redes sociales o de los videojuegos. Pérez y Vílchez (2012) establecen que los hombres juegan más a videojuegos online que las mujeres, pero ambos sexos coinciden en el desconocimiento que tienen sobre el impacto que las TIC tienen en su vida en particular y en la sociedad en general.

Por otro lado, Cabezas, et al., (2014), comprueban como el uso que los jóvenes les dan a las TIC está siempre más focalizado en el ocio y el aspecto lúdico que todo lo relacionado con su formación. Relacionado con esto, Moreno, et al., (2018) señalan que la seguridad es uno de los

aspectos que presentan mayores carencias en los estudiantes universitarios, lo que supone que independientemente de que usen las TIC para el ocio y la formación no son conscientes de los peligros y riesgos asociados y, por lo tanto, son más susceptibles de ser víctimas de cualquier problemática asociada a las redes sociales o las TIC.

Si se atiende a lo establecido por Grande-de-Prado, et al., (2019), los estudiantes universitarios de educación se autoperciben competentes en cuestiones que impliquen la gestión de la seguridad del correo electrónico o del antivirus, así como de la gestión de la información personal y profesional. Sin embargo, se establecen diferencias por sexos; los hombres se autoperciben mejor en todo lo relativo a la protección de los dispositivos y las mujeres en todo lo relativo a la protección de los datos y la identidad digital. Algo que puede estar relacionado con cómo usan los dispositivos tanto los hombres como las mujeres, algo que ya establecieron García-Martín y García-Sánchez (2017) donde afirman que las mujeres utilizan más las redes sociales que los hombres, pero a estos se les enseña más a cómo usar los diferentes dispositivos y a cómo manejar elementos web como wikis, etc.

2. JUSTIFICACIÓN

Actualmente, para que la vida cotidiana y todos los elementos que la componen funcionen correctamente resulta indispensable la tecnología. Dentro de esta vida diaria hay infinidad de áreas específicas donde la tecnología se ve involucrada o, que simplemente, sin ella no podrían entenderse tal y como son.

Cuando se habla de tecnología se engloban los dispositivos en su totalidad, las TIC y las redes sociales. Pero desde el plano del usuario también se debe incluir la alfabetización y la competencia digitales. Con el paso del tiempo se ha ido desgranando en qué consiste la competencia digital y qué elementos la conforman. De igual modo, a medida que esta temática ha ido adquiriendo relevancia entre nosotros han ido surgiendo beneficios, ventajas, desventajas, riesgos asociados, etcétera.

En el momento presente, estamos inmersos en una dinámica donde la tecnología e Internet dominan gran parte de la vida diaria de las personas en todos y cada uno de los contextos de actuación. Sin embargo, a pesar de saber introducir estos elementos en nuestra vida y hacer aparentemente un uso adecuado de ellos no significa que este sea responsable y seguro para nosotros. El uso de las TIC supone una serie de consecuencias las cuales pueden ser positivas y negativas. Una de las áreas de mayor importancia para evitar problemas derivados de este uso es el área de seguridad dentro de la competencia digital. Este apartado adquiere aún mayor importancia con la aparición y auge de las redes sociales (Dodel y Mesch, 2018).

Es una realidad palpable que todos los ciudadanos deben tener un correcto nivel de competencia digital para poder desarrollar su vida diaria de la mejor manera posible. Este nivel va aumentando según la generación es más joven. Sin embargo, ser competente digitalmente no significa solamente saber usar de manera correcta los dispositivos o tener bastos conocimientos sobre aplicaciones, softwares o hardware. Es, también, entender que hay que hacer un buen uso de esa competencia digital, ser consciente de los riesgos que conlleva ese manejo de las aplicaciones o dispositivos y cómo evitar o minimizar los problemas derivados que puedan surgir. Del mismo modo, hay que saber cómo aumentar esa seguridad y protección de todo lo relativo a las TIC en todos los aspectos de la vida, ya sea laboral o personal.

El aprendizaje sobre esta seguridad puede ser informal, pues la tecnología está presente allá donde se mire. Por el contrario, desde las instituciones educativas es de vital importancia formar a los estudiantes en este ámbito. La Educación Superior significa una etapa de especialización y formación para el futuro laboral donde este aspecto no puede dejarse de lado.

Así, la formación de los que van a ser formadores, es decir, de los futuros docentes ahora estudiantes de educación, es la mejor vía para que ese conocimiento se transmita a las generaciones venideras. Para ello hay que conocer cuál es el estado actual del nivel de competencia digital, concretamente del área de seguridad digital de estos estudiantes de educación.

Esta investigación pretende conocer y analizar el nivel en seguridad digital de estudiantes de educación de diversas universidades europeas, concretamente de la Península Ibérica. Por tanto, el contexto de esta investigación se centra en las titulaciones de educación de la Universidad de Granada, teniendo en cuenta sus 3 campus (Granada, Ceuta y Melilla), la Universidad de Málaga y el Instituto Politécnico Superior de Coimbra (Portugal).

La elección de estas universidades, sobre todo la comparativa entre las españolas y la portuguesa radica en que según el *The Times Higher Education World University Rankings 2023*, la posición de la Universidad de Granada y la de Coimbra es la misma (puesto 601), por lo que aquello que se analice parte a priori de unas bases similares. Este ranking juzga las instituciones de acuerdo con 13 indicadores de rendimiento clave, incluyendo el ambiente de aprendizaje, la influencia de la investigación y la proyección internacional (The Times Higher Education, 2023). No solo se centra en los aspectos investigativos como el ranking de Shangai, si no que tiene en cuenta el aprendizaje y sus procesos que es donde se enmarcaría lo que se investiga aquí.

La seguridad digital es ahora mismo una de las grandes temáticas investigativas a nivel mundial y también lo es específicamente en el área de educación. La protección de datos, de la identidad personal, de los dispositivos, de la salud y del entorno debe ser una máxima dentro del aprendizaje de los estudiantes, sobre todo de aquellos que en un futuro próximo van a formar a otros estudiantes, independientemente del nivel educativo.

Esta, dentro de la competencia digital docente, supone el conjunto de conocimientos, habilidades y actitudes del docente a la hora de formar a los estudiantes en un uso responsable y seguro de su competencia digital. Esta área engloba la protección de información y datos personales, la protección de la identidad digital, de contenidos digitales, de los diferentes dispositivos y la protección de la propia salud y el entorno (INTEF, 2017). La competencia relacionada con la seguridad promueve la creación de mecanismos de protección de los dispositivos y de la identidad digital y los datos personales asociados, es decir, ser consciente

de los riesgos y amenazas que surgen en la red y ser capaz de contrarrestarlo, al mismo tiempo que fomenta la creación de hábitos mediáticos saludables (Castillejos-López, et al., 2016).

De acuerdo con todo lo anteriormente expuesto, el problema de investigación radica en el estudio de la temática de la seguridad digital en los estudiantes de educación, atendiendo al nivel que poseen estos dentro de las cuatro subáreas que componen la principal y advertir dentro de la formación y competencia digital docente recibida por los discentes, los déficits en la dimensión de seguridad, no sabiendo identificarla. Todo ello en las titulaciones de educación de las universidades de Granada, Málaga y Coímbra.

En resumen, a través del desarrollo de este proyecto de tesis doctoral se tratará de dar respuesta a la siguiente cuestión:

¿Están los futuros docentes, respecto del uso y formación que realizan de las TIC durante la etapa de Ed. Superior, preparados para abordar la seguridad digital y los riesgos en red que pueden encontrarse en el desarrollo de su profesión?

A partir de esta pregunta de investigación surgen las hipótesis que se plantean de cara a la realización de esta investigación:

H0: La seguridad digital como elemento de la competencia digital de los docentes no está presente en los estudiantes de educación durante tu formación inicial

Hi: La seguridad digital como elemento de la competencia digital de los docentes está presente en los estudiantes de educación durante tu formación inicial

La finalidad de esta investigación por tanto será eliminar la hipótesis nula (H0) y a través del análisis y evaluación del tema que se aborda contrastar la premisa que dictamina la hipótesis que plantea el investigador (Hi).

3. OBJETIVOS

Llegados a este punto en el cual ya han quedado establecidas las bases conceptuales del proyecto de investigación que se va a llevar a cabo, se van a delimitar el objetivo general que orienta el trabajo, del mismo modo que sus correspondientes específicos.

1. Objetivo General (O.G.): Analizar el grado de competencia digital en el área de seguridad, los riesgos asociados y el grado de implementación de dicha competencia en el alumnado de la educación.

Los objetivos específicos son los siguientes:

1ª publicación:

Objetivo específico 1:

Conocer el concepto de seguridad digital, a qué marco teórico y legislativo pertenece. Caracterización del término y trabajo de esta desde el área educativa.

2ª publicación:

Objetivo específico 1:

Exponer el rendimiento y producción de la literatura científica sobre “cyberbullying”.

Objetivo específico 2:

Precisar la evolución científica del concepto de estudio.

Objetivo específico 3:

Determinar las temáticas más relevantes en el campo de estudio sobre el concepto.

Objetivo específico 4:

Establecer los autores más notables en la literatura sorbe el término que se estudia.

3ª publicación:

Objetivo específico 1:

Obtener una panorámica integral de la situación actual, a fin de desarrollar recomendaciones y pautas para mejorar la seguridad digital en el contexto educativo superior.

4ª publicación:

Objetivo específico 1:

Determinar el efecto global y particular de todas las investigaciones analizadas sobre la seguridad digital en estudiantes de Educación Superior.

5ª publicación:

Objetivo específico 1:

Conocer e interpretar cuál es el grado de conocimiento y aplicación de buenos mecanismos sobre seguridad en todas las subáreas de esta.

4. METODOLOGÍA

En este epígrafe se aborda el aspecto metodológico de la tesis doctoral. Esto incluye el diseño de investigación escogido, la selección de la muestra, los instrumentos empleados para la recolección de datos, el proceso estadístico seguido y el análisis de datos.

4.1.Diseño de investigación

Esta investigación responde a un método deductivo, esto es, partiendo de unos antecedentes y una base teórica consolidada se fundamentan las intervenciones pertinentes para poder alcanzar los objetivos propuestos (Romero-Rodríguez, 2020).

Este método se integra en una metodología de carácter cuantitativo y carácter descriptivo y exploratorio. Es un diseño no experimental realizado con el método de encuesta.

4.2.Muestra

Se ha aplicado un muestreo por conveniencia siguiendo las siguientes condiciones:

- Estudiantado de Educación Superior de titulaciones de educación
- Pertenecer a cualquiera de los tres campus de la Universidad de Granada (Granada, Ceuta y Melilla)

La elección de esta población se debe a la facilidad de disponer de profesorado que esté dispuesto a colaborar a la hora de pasar el cuestionario en sus clases en las diferentes titulaciones de educación.

La muestra está compuesta por un total de 269 participante; 76 alumnos y 191 alumnas, solo dos de ellos prefirieron no responder acerca de su sexo; todos ellos estudiantes de las titulaciones de Educación Primaria, Educación Infantil, Educación Social y Pedagogía. Esta muestra permite dar respuesta a los objetivos propuestos (Buendía, et al., 1998).

4.3.Instrumento

El instrumento empleado en esta investigación se trata de un cuestionario ya validado (García-Valcárcel, et al., 2019), pues fue sometido a discusión por pares y valoración de expertos. Por tanto, el cuestionario está conformado por un total de 16 ítems, de los cuales 6 hacen referencia a conocimientos y 10 a habilidades. De igual modo, todos ellos miden 4 subáreas dentro del área de la seguridad digital, a saber:

a. Protección de dispositivos (ítems 1-4)

b. Protección de datos personales (ítems 5-8)

c. Protección de la salud (ítems 9-12)

d. Protección del medio ambiente (ítems 13-16)

Las preguntas están configuradas de la siguiente manera: la suma de los ítems sobre conocimientos y habilidades, que son un total de 16, son tipo prueba objetiva con 4 alternativas de respuesta, donde solamente una es correcta. En este caso, las respuestas han sido codificadas de forma dicotómica:

- 0 = ha elegido la respuesta correcta
- 1= ha elegido la respuesta incorrecta

Esto conlleva que la puntuación máxima de la prueba sea de 16 puntos.

4.4.Procedimiento

El estudio completo se realizó en etapas diferenciadas. En la primera etapa se llevó a cabo una revisión de la literatura sobre la temática para la confección del marco teórico. En una segunda fase se llevó a cabo un estudio bibliométrico sobre el ciberacoso o ciberbullying como una de las temáticas principales dentro de la seguridad digital. Como tercer paso, se realizó una revisión sistemática donde se analizó la literatura existente sobre seguridad digital en la etapa de Educación Superior. El cuarto paso es realizar un metaanálisis de esta temática el cual pretende combinar los resultados de los estudios obtenidos para obtener parámetros de medidas globales.

En la última fase se lleva a cabo un estudio empírico a través de un cuestionario ya validado. La aplicación del cuestionario se llevó a cabo de forma individual y en línea. Los datos obtenidos se analizaron a través de los programas Excel y SPSS en su versión 25, a partir de aquí se procede a su análisis estadístico para poder alcanzar los objetivos de la investigación.

Una vez analizados los resultados, se comprueba como el área de la seguridad digital dentro de la etapa de Educación Superior y, concretamente, en los estudiantes de educación, es todavía un área con un déficit formativo reseñable que varía dependiendo de la subárea que se tenga en cuenta. Del mismo modo, las diferencias entre la formación de los diferentes sexos es también un elemento reseñable.

4.5.Análisis de datos

A partir de los datos extraídos se calcularon estadísticas descriptivas para cada variable. Antes de realizar cualquier análisis estadístico paramétrico, se comprobaron los supuestos de normalidad y homocedasticidad con las pruebas de Kolmogorov-Smirnov y Levene, respectivamente. Para determinar las diferencias entre hombres y mujeres se utilizó una prueba t de muestras emparejadas. La d de Cohen fue el indicador del tamaño del efecto. Para interpretar la magnitud del tamaño del efecto, se adoptaron los siguientes criterios: $d \leq 0,20$, pequeño; $d \leq 0,50$, mediano; y $d \leq 0,80$, grande.

Se utilizó el coeficiente de correlación r de Pearson para examinar la relación entre la edad y la puntuación global. Para interpretar la magnitud de estas correlaciones, se adoptó el siguiente criterio: Trivial: $\leq 0,10$; pequeña: 0,10 a 0,29; moderada: 0,30 a 0,49; grande: 0,50 a 0,69; muy grande: 0,70 a 0,89; casi perfecta: $\geq 0,90$.

Asimismo, se utilizó el coeficiente de correlación r de Pearson para examinar la relación entre cada una de las cuatro áreas del área de seguridad (Subárea 1 (S1): Protección de Dispositivos; Subárea 2 (S2): Protección de datos personales y privacidad; Subárea 3 (S3): Protección de la salud y el bienestar; Subárea 4 (S4): Protección del Medio Ambiente). Al igual que antes, para interpretar la magnitud de estas correlaciones se adoptó el siguiente criterio: Trivial: $\leq 0,10$; pequeña: 0,10 a 0,29; moderada: 0,30 a 0,49; grande: 0,50 a 0,69; muy grande: 0,70 a 0,89; casi perfecta: $\geq 0,90$.

Se utilizó el análisis de regresión múltiple para modelizar la predicción del nivel de competencia en seguridad digital de los estudiantes de educación a partir del resto de variables del área de seguridad. En este análisis de regresión, todas las variables se examinaron por separado. Los datos se analizaron utilizando Statistica (versión 13.3).

5. TRABAJOS PUBLICADOS E INDICIOS DE CALIDAD

Es este epígrafe se muestran las publicaciones que conforman el compendio, así como sus indicios de calidad de las revistas donde se han publicado:

1- La seguridad dentro de la competencia digital. Formación docente en esta área.

Rodríguez-Jiménez, C., Trujillo-Torres, J. M., Berral-Ortiz, B., y De la Cruz-Campos, J. C. (2022). La seguridad dentro de la competencia digital: formación docente en esta área. C. Hervás-Gómez, A. Luque de la Rosa, J.C. de la Cruz-Campos, M.A. Domínguez-González (ed.), *Espacios de aprendizaje e implicaciones prácticas* (pp. 69-79). Dykinson. ISBN 978-84-1122-697-4

2- Educación en Seguridad Digital: Estudio Bibliométrico sobre el Cyberbullying en Web of Science

Rodríguez-Jiménez, C., Trujillo-Torres, J. M., Moreno-Guerrero, A. J, y Alonso-García, S. (2020). Educación en seguridad digital: estudio bibliométrico sobre el cyberbullying en web of science. *Texto Livre: Linguagem e Tecnologia*, *13*(3), 140-160. https://doi.org/10.35699/1983-3652.2020.25110

3- Revisión Sistemática de la literatura sobre la Seguridad Digital en estudiantes de Educación Superior

Trujillo-Torres, J.M., Rodríguez-Jiménez, C., Alonso-García, S., y Berral-Ortiz, B. (2024). Revisión sistemática de la literatura sobre la Seguridad Digital en estudiantes de Educación Superior. *Información Tecnológica*, En Prensa.

4- Metaanálisis sobre la Seguridad Digital en estudiantes de Educación Superior

Rodríguez-Jiménez, C., Trujillo-Torres, J.M., Alonso-García, S., y Martínez-Domingo, J.A. (2025). Metaanálisis sobre la Seguridad Digital en Estudiantes de Educación Superior [Metaanalysis on Digital Safety in Higher Education Students]. *Pixel-Bit. Revista de Medios y Educación*, *72*, En Prensa.

5- Evaluación de las Competencias en Seguridad Digital de los Estudiantes de Educación Superior de la Universidad de Granada

Rodríguez-Jiménez. C., Trujillo-Torres, J.M., Alonso-García, S., y Martínez-Domingo, J.A. (2023). Evaluación de las Competencias en Seguridad Digital de los Estudiantes de Educación Superior de la Universidad de Granada. En (Coords. G. Estuardo Ceballos Uve,

M.J. Santos Villalba, M.J. Alcalá del Olmo Fernández y D. Álvarez Ferrándiz) *Educación integral con perspectivas innovadoras para el desarrollo educativo* (pp. 43-53). Dykinson. ISBN 978-84-1170-706-0.

5.1.Primera publicación

La seguridad dentro de la competencia digital. Formación docente en esta área.

Este trabajo ha sido publicado como capítulo del libro de la editorial Dykinson, que lleva por título Espacios de Aprendizaje e Implicaciones Prácticas (ISBN 978-84-1122-697-4). Esta editorial independiente publica mayoritariamente literatura especializada para profesionales de diferentes áreas, destacando las relativas a la Educación y a la Psicología. Esta se haya entre las seis 6 editoriales españolas, obteniendo también el puesto 14 de 272 en Scholarly Publishers Indicators (SPI) "In Humanities and Social Sciences" de todas las editoriales españolas con un indicador de prestigio (ICEE) de 20.763 del general de 504 editoriales. En lo relativo al área de Educación se haya en la posición 16 de 94 de un total de 156 editoriales con un ICEE de 0.954 (cuartil Q1).

Referencia bibliográfica:

Rodríguez-Jiménez, C., Trujillo-Torres, J. M., Berral-Ortiz, B., y De la Cruz-Campos, J. C. (2022). La seguridad dentro de la competencia digital: formación docente en esta área. C. Hervás-Gómez, A. Luque de la Rosa, J.C. de la Cruz-Campos, M.A. Domínguez-González (ed.), *Espacios de aprendizaje e implicaciones prácticas* (pp. 69-79). Dykinson. ISBN 978-84-1122-697-4

La seguridad dentro de la competencia digital: formación docente en esta área

Carmen Rodríguez Jiménez[1], Juan Manuel Trujillo Torres[1], Blanca Berral Ortiz[1] y Juan Carlos de la Cruz-Campos[1]

[1]Universidad de Granada

1. INTRODUCCIÓN

Desde hace ya varias décadas, en la sociedad actual, son varios los elementos o las áreas que movilizan todas las demás y caracterizan a la sociedad presente. Indudablemente, uno de los elementos que más cambios genera y más influye en todas las personas es la tecnología.

La tecnología en el presente tiene el poder de modificar a una velocidad de vértigo todos los sectores sociales y hace que el mundo globalizado del siglo XXI no pare de cambiar constantemente, lo que provoca que todo el mundo tenga que estar continuamente actualizándose.

Para adaptarse a esta tendencia creciente en los últimos años y que no tiene previsión de terminar, campos como el de la educación han tenido que hacer diversos y profundos cambios para no quedarse atrás. estos cambios han afectado a todos los elementos y miembros presentes tanto en la comunidad educativa como en los procesos de enseñanza-aprendizaje (a partir de ahora e-a), esto incluye materiales, herramientas, recursos, metodologías, formación docente, formación dicente, entre otros muchos aspectos.

Estas modificaciones siguen en la actualidad y no van a cesar pues los avances tecnológicos tampoco lo hacen. así pues, a través de los años se ha ido reflejando en diferentes documentos oficiales la importancia de este elemento tecnológico y digital.

Esta plasmación de estos elementos, que llega hasta hoy, es cada vez más específica y se da tanto en documentos internacionales como nacionales.

Así surge la competencia digital, un concepto novedoso que abarca diferentes saberes y desempeños que versan sobre la utilización eficaz y eficiente de todo lo concerniente a lo digital.

Sin embargo, con el paso de los años, la competencia digital ha ido desgranándose y dando a conocer todas las partes que la componen, áreas y subáreas, que suponen una mejor comprensión de qué es ser digitalmente competente.

Dentro de estas áreas se encuentra el área de seguridad digital que es de vital importancia hoy en día, pues los problemas derivados de un desconocimiento de esta área o de un mal uso de la competencia digital son cada vez más comunes entre la población.

De este modo, a través de este trabajo se pretende mostrar qué es la seguridad digital y en qué marco teórico y legislativo se encuentra inmersa. Del mismo modo, qué caracteriza este término y cómo se puede trabajar desde el área educativa.

2. LA COMPETENCIA DIGITAL

Hay que remontarse al año 2008 cuando se establecieron las competencias clave para encontrar el término competencia digital (a partir de ahora CD). Esta es una de las competencias clave por la relevancia e importancia que ya en aquellos años tomaba el concepto.

Estas competencias clave son una "combinación de conocimientos, capacidades y actitudes" (Consejo de la Unión Europea, 2018). Se entiende, por tanto, que las competencias deben estar conformadas por conceptos e ideas, a la misma vez que habilidades para el desarrollo en la práctica de esas ideas y una mentalidad a la hora de actuar para con esas ideas. Es decir, las competencias están compuestas por el saber, el saber hacer y el saber ser.

Por lo tanto, las competencias se enmarcan en un aprendizaje permanente desde la infancia y que no cesa nunca.

Las competencias clave son las siguientes:

- Competencia en comunicación lingüística (CLL).
- Competencia matemática y competencias básicas en ciencia y tecnología (CMCT).
- Competencia digital (CD).
- Aprender a aprender (CAA).
- Competencias sociales y cívicas (CSC).
- Sentido de la iniciativa y espíritu emprendedor (SIEP).
- Conciencia y expresiones culturales (CEC).

La CD es la que supone para el aprendiz el empleo de las Tecnologías de la Información y la Comunicación (a partir de ahora TIC) de una manera creativa, crítica y segura, todo esto con la finalidad de conseguir los objetivos propuestos.

Todo esto conlleva una serie de conocimientos relacionados necesarios para poder desarrollarla correctamente:

- Conocimiento de lenguaje específico básico.
- Conocimiento de pautas de decodificación y transferencia.
- Conocimiento de aplicaciones informáticas básicas.

- Conocimiento sobre el acceso a fuentes de información seguras y su tratamiento.
- Conocimiento de derechos y deberes de los usuarios en el mundo digital.

La CD, si se acude de nuevo a la definición de competencia clave, requiere de un saber, un saber hacer y un saber ser. Esto es, unos conocimientos, unas habilidades y unas actitudes. Estas se resumen en las siguientes (educagob, 2019):

Conocimientos (saber):

- Derechos y riesgos relacionados con lo digital.
- Fuentes de información.
- Elementos textuales, visuales, gráficos, etcétera, que aparecen el mundo digital.
- Aplicaciones informáticas variadas.

Habilidades (saber hacer):

- Emplear y tratar la información de manera crítica.
- Búsqueda, obtención y tratamiento de la información.
- Uso de diversos recursos tecnológicos.
- Creación de contenidos.

Actitudes (saber ser):

- Tener una actitud crítica y realista con los recursos tecnológicos.
- Conocer las ventajas y desventadas de los recursos tecnológicos.
- Tener motivación por el aprendizaje relacionado con la tecnología.
- Tener ética a la hora de usar la tecnología.

Dentro de la CD es importante destacar que existen diferentes áreas, las cuales serán abordadas más adelante, pero que abordan los siguientes ámbitos:

- Información.
- Comunicación.
- Creación de contenidos.

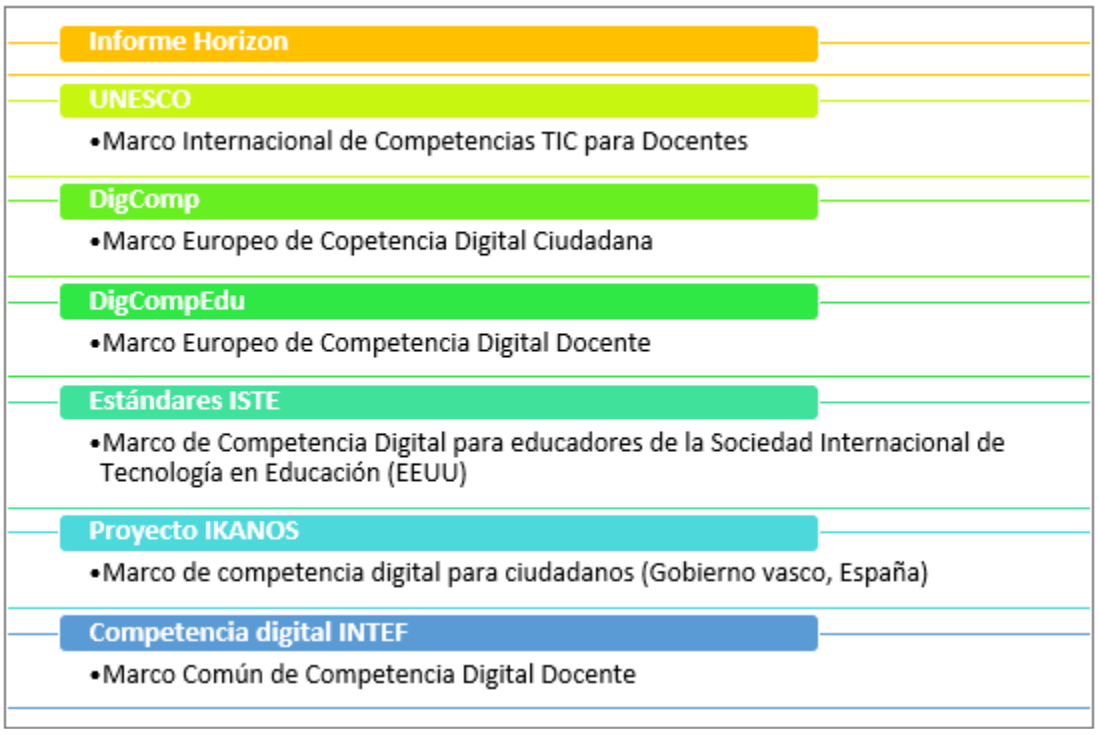
- Seguridad.
- Resolución de problemas.

Como se puede observar, la seguridad, en este caso digital, es una de las áreas principales de la CD, lo que supone reconocer la importancia de esta materia dentro de toda la formación digital.

3. MARCO DE REFERENCIA DE LA COMPETENCIA DIGITAL

En este epígrafe se van a abordar los diferentes marcos de referencia y documentos oficiales existentes sobre la CD. Estos marcos se han ido publicando a través de los años y se actualizan con frecuencia para mantenerlos al día de todas las novedades y cambios que van sucediendo en el área.

A continuación, se muestra de manera esquemática los diferentes informes desarrollados sobre



CD y que se van a abordar más adelante.

Figura 1. Marcos de referencia sobre competencia digital (elaboración propia).

De este modo, a nivel internacional se encuentra el Informe Horizon (Horizon Report) (Pelletier, 2021). Este informe está siendo publicado desde el año 2004 y es realizado por las entidades New Media Consortium (NMC) y EDUCASE Learning Initiative (ELI). Lo que pretende este informe desde su creación hasta la actualidad es establecer y desarrollar aquellas tecnologías que tendrán un impacto en el área educativa (Salvat y Fructuoso, 2015). Con este

informe se realizan una serie de estimaciones para un máximo de cinco años sobre los siguientes apartados (Adams Becker, et al., 2017):

- Tecnologías de gran impacto en una etapa educativa determinada
- Tendencias tecnológicas a implantar en los próximos años
    - A corto plazo.
    - A medio plazo.
    - A largo plazo.
- Desafíos educativos relevantes necesarios de abordar
    - Fáciles.
    - Difíciles.
    - Muy difíciles.

Este informe, no solo hace referencia a las tecnologías que tendrán una influencia en la educación, si no que le presta atención a aquellas que lo harán en la sociedad, pues esto supondrá también que lo hagan en la educación ya que van relacionadas. A la vez, es un ejemplo de diferentes retos a asumir por parte de los diferentes usuarios de las tecnologías y de los agentes implicados en la educación para estar preparados para un futuro próximo y sacar, por tanto, el máximo partido de las tecnologías cuando toque emplearlas.

Por otro lado, se encuentra el Marco Internacional de Competencias TIC para Docentes. Este documento pretende ayudar a os diferentes países para que estos desarrollen e implementen normativas en materia TIC para los docentes, llevando así el uso de las TIC a la educación (UNESCO, 2021).

Este marco resalta el papel de la tecnología como elemento de apoyo a seis aspectos principales de la labor pedagógica; además, detalla el nivel de implementación o adquisición de estos aspectos en las tres etapas sucesivas de la adquisición de conocimientos (Cabero-Almenara, et al., 2020).

A continuación, se detalla cómo las TIC ayudan al desarrollo de estos aspectos y etapas (tabla 1).

ETAPAS DE CONOCIMIENTO / ASPECTOS DE LA LABOR PEDAGÓGICA	Adquisición de conocimientos	Profundización de conocimientos	Creación de conocimientos
Comprensión del papel de las TIC en la educación	Conocimiento de las políticas	Aplicación de las políticas	Innovación política
Currículo y evaluación	Conocimientos básicos	Aplicación de los conocimientos	Competencias de la sociedad del conocimiento
Pedagogía	Enseñanza potenciada por las TIC	Resolución de problemas complejos	Autogestión
Aplicación de competencias digitales	Aplicación	Infusión	Transformación
Organización y administración	Aula estándar	Grupos de colaboración	Organizaciones del aprendizaje
Aprendizaje profesional de los docentes	Alfabetización digital	Trabajo en redes	El docente como innovador

Tabla 1. Marco Internacional de Competencias TIC para Docentes (adaptado de UNESCO (2021).

Siguiendo con otros marcos de referencia a nivel internacional, encontramos el DigComp y el DigComp 2.0 a nivel europeo. El DigComp (Comisión Europea, 2013) tiene como objetivo contribuir a un mejor entendimiento y desarrollo de esta competencia en el contexto europeo. Este documento pretende por un lado identificar los componentes de la competencia, (conocimientos, habilidades y actitudes) los cuales sirven para detectar a la persona que es digitalmente competente; por otro lado, desarrollar un marco conceptual para esta competencia y proponer descriptores de la competencia para todos los niveles de aprendizaje. Más tarde, en el año 2016, surgió una nueva versión del DigComp, ahora llamado DigComp 2.0. (Comisión Europea, 2016). Este documento contiene los mismos objetivos y finalidades, actualizando únicamente el vocabulario y los descriptores que incluye.

De manera más concreta, siguiendo esta misma estela, dentro del marco europeo está el DigCompEdu (Digital Competence for Educators). Un documento de referencia que es a la vez

una herramienta de autoevaluación para los docentes y un modelo para las políticas sobre competencia digital y programas de capacitación a este respecto (European Comission, 2017).

Por otro lado, también a nivel internacional se encuentran los estándares ISTE. Estos conforman un Marco de referencia dentro de la CD desarrollados por la Sociedad Internacional para la Tecnología en la Educación (ISTE) fundada en EE. UU.

Estos estándares ofrecen las competencias para aprender, enseñar y liderar en la era digital en la que estamos sumergidos. De igual modo, diseñan una "hoja de ruta integral para el uso efectivo de la tecnología en las escuelas de todo el mundo" (ISTE, 2022). Además, estos estándares están divididos por grupos, especializándose así a los usuarios que accedan a ellos. Se encuentran así estándares para:

- Estudiantes
- Docentes
- Líderes eductivos
- Mentores

También ofrecen para los educadores una serie de competencias para desarrollar el pensamiento computacional en todas las áreas de conocimiento y con discentes de todas las etapas educativas.

Concretando ya a nivel nacional, en España se encuentra el Marco Común de Competencia Digital Docente (INTEF, 2017). Este documento es una adaptación del DigComp y del DigCompEdu al contexto español.

En él se describen detalladamente las competencias y los diversos niveles en que pueden darse. Este proyecto es una herramienta útil para detectar las necesidades formativas de los docentes en materia de competencia digital. Está formado por cinco áreas competenciales que incluyen veintiuna competencias, y en cada una se establecen seis niveles que se refieren tanto a conocimientos, como a capacidades y actitudes (Figura 2).

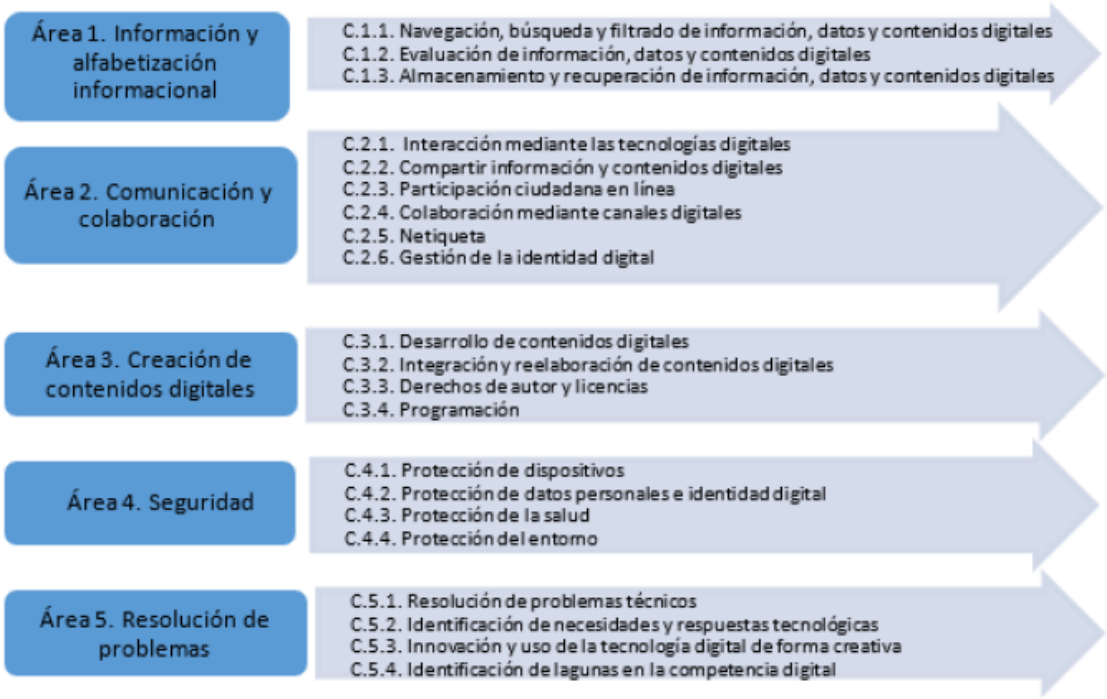


Figura 2. Áreas y subáreas del Marco Común de Competencia Digital Docente (elaboración propia).

Sin embargo, a principios del presente, el INTEF publicó una actualización del Marco Común de Competencia Digital, pasando a llamarse ahora Marco de Referencia de la Competencia Digital Docente (INTEF, 2022). Se trata de una propuesta que aún está en borrador esperando a ser aprobado.

En este caso, de nuevo se parte del DigCompEdu y se adapta al contexto educativo español, modificándolo para su adaptación a las diferentes fases de desarrollo profesional de los docentes, desde la formación inicial y la incorporación al sistema educativo hasta la consecución como expertos de un uso crítico y creativo de la labor docente donde "las tecnologías digitales no son un fin, sino un medio más para que todo el alumnado mejore sus aprendizajes" (INTEF, 2022).

A continuación, se enuncian las áreas de la CD que han sido renombradas y modificadas, así como sus subáreas (INTEF, 2022):

1) ÁREA 1: compromiso profesional.

    4.1.Comunicación organizativa.

    4.2.Participación, colaboración y coordinación profesional.

    4.3.Práctica reflexiva.

4.4.Desarrollo profesional digital continuo.

4.5.Protección de datos personales, privacidad, seguridad y bienestar digital.

2) ÁREA 2: Contenidos digitales.

2.1.Búsqueda y selección de contenidos digitales.

2.2.Creación y modificación de contenidos digitales.

2.3.Protección, gestión y compartición de contenidos digitales.

3) ÁREA 3: Enseñanza y aprendizaje.

3.1.Enseñanza.

3.2.Orientación y apoyo en el aprendizaje.

3.3.Aprendizaje entre iguales.

3.4.Aprendizaje autorregulado.

4) ÁREA 4: Evaluación y retroalimentación.

4.1.Estrategias de evaluación.

4.2.Analíticas y evidencias de aprendizaje.

4.3.Retroalimentación y toma de decisiones.

5) ÁREA 5: Empoderamiento del alumnado.

5.1.Accesibilidad e inclusión.

5.2.Atención a las diferencias personales en el aprendizaje.

5.3.Compromiso activo del alumnado con su propio aprendizaje.

6) ÁREA 6: Desarrollo de la competencia digital del alumnado.

6.1.Alfabetización mediática y en el tratamiento de la información y de los datos.

6.2.Comunicación, colaboración y ciudadanía digital.

6.3.Creación de contenidos digitales.

6.4.Uso responsable y bienestar digital.

6.5.Resolución de problemas.

Se puede observar que el principal cambio es la creación de una nueva área, así como el cambio de nombre de todas ellas y sus subáreas.

De una manera más concreta, dentro del contexto español, el gobierno vasco ha creado la iniciativa Ikanos, mediante la cual proponen una metodología para el correcto desarrollo de la CD. Esta iniciativa pretende sensibilizar, acompañar e innovar en todo lo referente a la formación en CD para profesionales, organizaciones y stakeholders o promotores.

Dentro de esta iniciativa se encuentra el Test Ikanos (Gobierno Vasco, 2019). Esta prueba proporciona una vez realizada un perfil digital que, nuevamente, se basa en el DigComp. Hay dos tipologías principales de este test: el test individual y para colectivos. Dentro de estas dos tipologías el test se especifica dependiendo del área profesional a la que se pertenezca.

Test Ikanos individual:

- General.
- Para educación.

Test Ikanos para colectivos:

- Industria avanzada.
- Profesionales de la economía.
- Profesionales del ámbito de la salud y la medicina.

4. EL PAPEL DE LA SEGURIDAD DIGITAL DENTRO DE LA COMPETENCIA DIGITAL

Como se ha podido comprobar a lo largo de todo este documento, la importancia de la cd es supina en la actualidad. dentro de esta, como ya se ha visto, se encuentra el área de seguridad. la seguridad digital, por tanto, debe ser trabajada a la par que el resto de las áreas.

La seguridad digital incluye los riesgos, las estrategias y las adicciones asociadas al uso de los dispositivos tecnológicos. aunque estos conceptos están extendidos en toda la sociedad y entre los usuarios de las TIC, son ideas difusas las cuales deben ser comprendidas para eliminar así los climas de indefensión que pueden generarse con el uso de la tecnología.

Tras la actualización del marco común de competencia digital docente, todo se aúna en la protección de datos personales, privacidad, seguridad y bienestar digital. esto incluye la protección de los datos personales, así como de las diferentes comunicaciones que se tienen con otros usuarios a través de diferentes dispositivos. todo esto con la finalidad de evitar o minimizar los riesgos y amenazas digitales. se pretende que la tecnología se use con responsabilidad, de una manera segura y saludable, eliminando así riesgos personales, laborales y contextuales, garantizando un bienestar psíquico, físico y social (INTEF, 2022).

Siguiendo este mismo documento, son cuatro los ejes que se tienen que seguir para que los docentes estén comprometidos con la seguridad digital. los ejes son los siguientes:

1. la protección de datos personales, de la privacidad y de los derechos digitales.
2. la seguridad en el acceso a los dispositivos, sistemas y redes.
3. el uso responsable y sostenible de los recursos digitales desde el punto de vista medioambiental.
4. las medidas orientadas a garantizar la salud física y mental.

Esta competencia que es la seguridad digital debe trabajar unos contenidos por sí misma, los cuales son específicos y concretos pero que a la vez se interrelacionan con el resto de áreas y subáreas de la CD. Así, deben trabajarse las legislaciones existentes sobre derechos y deberes en el ámbito digital y en el ámbito digital educativo; la seguridad a la hora de acceder, crear, modificar, almacenar y recuperar información, contenidos, materiales, herramientas u otros elementos digitales; y los conceptos de bienestar digital y cómo lograrlo, así como qué es usar de manera responsable, saludable y sostenible los recursos digitales

5. CONCLUSIONES

Tras todo lo expuesto en este documento queda patente que la CD es primordial en el área educativa en el presente y va a seguir siéndolo pues cambia y se actualiza constantemente.
Conocer los diferentes marcos de referencia que abalan su importancia, su vigencia y que ayudan a una formación adecuada a este respecto tiene que ser un elemento más dentro de los sistemas educativos y dentro de la formación docente.

La competencia digital tiene además que ser trabajada de manera global, desarrollando al máximo todas y cada una de sus áreas y subáreas, para poder ser ciudadanos y usuarios digitalmente competentes.

En lo referente al área de seguridad digital, considero que no debe dejarse atrás o sobreentender que va de la mano del resto de áreas cuando estás son trabajadas. Esto es cierto, pero debe haber un espacio concreto donde se trabaje de manera específica todo lo que conlleva la seguridad digital, pues no son pocos os inconvenientes, riesgos y amenazas derivadas de un mal uso de la CD por desconocimiento de la seguridad digital y todos sus elementos.

Siguiendo en esta misma línea, creo que es importante resaltar los cambios tan evidentes y sustanciales sufridos por el Marco Común de Competencia Digital Docente en el contexto español, pues el área de Seguridad como tal desaparece, diluyéndose en las otras áreas a modo de subárea. Considero que esto podría restarle importancia a la seguridad digital como elemento fundamental dentro del tratamiento de la CD. Sin embargo, el borrador que se presenta en todos los demás aspectos es mucho más específico en cuanto a la labor docente y su aprendizaje dentro del mundo digital. Además, se le da un papel claro al estudiante y cómo el docente tiene que llevar a cabo el proceso de E-A a través de las tecnologías para la consecución de todos los objetivos.

Finalmente, creo que dar a conocer a nivel teórico todo lo relativo a la CD y sus áreas de manera periódica es un modo de actualización de los conocimientos rápido, para poder así a continuación ponerlos en práctica en la realidad educativa.

REFERENCIAS BIBLIOGRÁFICAS

Adams Becker, S., Cummins, M., Davis, A., Freeman, A., Hall Giesinger, C., y Ananthanarayanan, V. (2017). *NMC Informe Horizon 2017 Edición Superior de Educación.* Austin, Texas: El New Media Consortium.

Cabero-Almenara, J., Barroso-Osuna, J., Rodríguez, A. P., y Llorente-Cejudo, C. (2020). Marcos de Competencias Digitales para docentes universitarios: su evaluación a través del coeficiente competencia experta. *Revista electrónica interuniversitaria de formación del profesorado, 23(*3). https://doi.org/10.6018/reifop.414501

Comisión Europea. (2013). *DigComp. Digitally Competent Educational Organisations.* https://ec.europa.eu/jrc/en/digcomp

Comisión Europea. (2016). *DigCompOrg. Digitally Competent Educational Organisations.* https://ec.europa.eu/jrc/en/digcomporg

Consejo de la Unión Europea. (2018). *RECOMENDACIÓN DEL CONSEJO de 22 de mayo de 2018 relativa a las competencias clave para el aprendizaje permanente.* https://eurlex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018H0604(01)&from=SV

Educagob. *Portal del sistema educativo español. (2019). Competencias clave.* https://educagob.educacionyfp.gob.es/curriculo/curriculo-actual/competencias-clave.html

European Comission. (2017). *DigCompEdu. Digital Competence for Educators.* https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-researchreports/european-framework-digital-competence-educators-digcompedu

Gobierno Vasco. (2019). *Test Ikanos de competencias digitales.* https://test.ikanos.eus/index.php/566697?lang=en

INTEF. (2017). *Marco Común de Competencia Digital Docente.* http://aprende.intef.es/sites/default/files/2018-05/2017_1020_Marco-Com%C3%BAn-deCompetencia-Digital-Docente.pdf

INTEF. (2022). *Marco de Referencia de la Competencia Digital Docente (borrador).* https://intef.es/wp-content/uploads/2022/03/MRCDD_V06B_GTTA.pdf

ISTE. (2022). *Estándares ISTE.* https://www.iste.org/es/iste-standards

Pelletier, K., Brown, M., Brooks, D. C., McCormack, M., Reeves, J., Arbino, N., ... y Mondelli, V. (2021*). 2021 EDUCAUSE Horizon Report Teaching and Learning Edition*. EDU, Boulder, CO.

Salvat, B. G., y Fructuoso, I. N. (2015). Mirando el futuro: Evolución de las tendencias tecnopedagógicas en educación superior. *Campus Virtuales*, *2*(2), 130-140.

UNESCO. (2021). Marco de Competencias de los Docentes en materia de TIC. https://es.unesco.org/themes/tic-educacion/marco-competencias-docentes

5.2.Segunda publicación

Educación en Seguridad Digital: Estudio Bibliométrico sobre el Cyberbullying en Web of Science

Este artículo ha sido publicado en la revista Texto Livre: Linguagem e Tecnología (ISSN 1983-3652). Se trata de una revista internacional que publica artículos científicos, relatos de experiencias, ensayos, reseñas críticas, entrevistas y dossiers, que abordan la transdisciplinariedad en las líneas de lingüística, semiótica, educación, comunicación, las TIC, la traducción, la robótica y la cultura libre relacionadas siempre con las tecnologías. En cuanto al área educativa los temas de interés para la revista son: el uso de tecnologías de enseñanza-aprendizaje, recursos educativos abiertos, inclusión digital, alfabetización digital, y cualquier otro tema relacionado con las tecnologías.

Se encuentra en el cuartil Q2 2022 SJR 0.2

En el Indicador de citas de revistas (JCI) de 2021 obtuvo una puntuación de 0,50, Cuartil: Q2

En la Clasificación del Journal Citation Indicatos (JCI) obtuvo la posición 182 de 370.

Esta revista está indexada en las bases de datos: DOAJ, ERIHPLUS, LATINDEX, MIAR, SCOPUS, REDIB, Redalyc, EBSCO, Dialnet, Cariniana, Diadorim.

Referencia bibliográfica:

Rodríguez-Jiménez, C., Trujillo-Torres, J. M., Moreno-Guerrero, A. J, y Alonso-García, S. (2020). Educación en seguridad digital: estudio bibliométrico sobre el cyberbullying en web of science. Texto Livre: Linguagem e Tecnologia, 13(3), 140-160. https://doi.org/10.35699/1983-3652.2020.25110

EDUCACIÓN EN SEGURIDAD DIGITAL: ESTUDIO BIBLIOMÉTRICO SOBRE EL CYBERBULLYING EN WEB OF SCIENCE

DIGITAL SECURITY EDUCATION: BIBLIOMETRIC STUDY ON CYBERBULLYING IN WEB OF SCIENCE

EDUCAÇÃO EM SEGURANÇA DIGITAL: ESTUDO BIBLIOMÉTRICO SOBRE CYBERBULLYING NA WEB OF SCIENCE

Carmen Rodríguez Jiménez[1], Juan Manuel Trujillo Torres[1], Antonio José Moreno Guerrero[1], Santiago Alonso García[1]

[1]Universidad de Granada

RESUMEN: La manera en la que la sociedad se comunica en la actualidad ha cambiado y esto afecta también a la educación. Las Tecnologías de la Información y Comunicación (TIC), las redes sociales y los diferentes dispositivos multimedia suponen un papel fundamental en el ámbito educativo, sin embargo, no siempre este uso reporta beneficios, presentándose entre las posibles desventajas el cyberbullying. Esta investigación tiene como objetivo analizar la situación de la literatura científica existente en la base de datos Web of Science sobre cyberbullying. A nivel metodológico se ha llevado a cabo un estudio bibliométrico donde se analiza el desarrollo estructural y dinámico del término de estudio. Los resultados reflejan que la producción científica sobre esta temática es escasa e irregular, donde la mayoría de textos científicos son artículos y el inglés es su principal idioma. Se concluye que la temática aboga principalmente por la intervención y prevención.

PALABRAS CLAVE: Cyberbullying. Investigación educativa. Bibliométrico.

ABSTRACT: The way society communicates today has changed and this affects education as well. The information and communication technologies (ICT), social networks and different multimedia devices play a fundamental role in the educational field, however, this use does not always bring benefits, and one of the disadvantages is cyberbullying. This research aims to analyse the situation of the existing scientific literature in the Web of Science database on cyberbullying. On a methodological level, a bibliometric study has been carried out where the structural and dynamic development of the study term is analysed. The results reflect that the scientific production on this subject is low and irregular, where most of the scientific texts are articles and English is their main language. It is concluded that the theme advocates mainly intervention and prevention.

KEYWORDS: Cyberbullying. Educational research. Bibliometrics.

RESUMO: A forma como a sociedade se comunica hoje mudou e isso também afeta a educação. As Tecnologias da Informação e Comunicação (TIC), as redes sociais e os diversos dispositivos multimídia desempenham um papel fundamental no campo educacional; porém, esse uso nem sempre traz benefícios, estando o cyberbullying entre as possíveis desvantagens. Esta pesquisa tem como objetivo analisar a situação da produção científica na base de dados Web of Science sobre cyberbullying. Em termos metodológico, realiza-se um estudo bibliométrico para se analisar o desenvolvimento estrutural e dinâmico do termo de estudo. Os resultados refletem que a produção científica sobre o assunto é escassa e irregular, sendo a

maioria dos textos científicos artigos e o inglês o idioma principal. Conclui-se que o tema preconiza principalmente intervenção e prevenção.

PALAVRAS-CHAVE: Cyberbullying. Investigação educacional. Bibliometria.

1 Marco Teórico

El uso de los medios de comunicación, los diferentes dispositivos multimedia, las redes sociales e internet para compartir información, han supuesto en las últimas décadas una potenciación del aprendizaje y una interconexión entre diferentes personas y comunidades (SWEET et al., 2020). A medida que esta forma de comunicarse ha logrado erigirse como una de las herramientas más comunes para el aprendizaje tanto formal como informal, surge la necesidad de entender cómo se gestiona su uso (KOKKINOS; ANTONIADOU; MARKOS, 2014). Este rápido crecimiento ha traído consigo ventajas, pero también elementos negativos (MONTIEL; AGUSTINA, 2019), como consecuencia de un mal uso y gestión que pueden derivar en diferentes fenómenos, entre los que destaca el cyberbullying (AZNAR-DÍAZ et al., 2019; MÉNDEZ-MATEO et al., 2019; RUIZ-PALMERO; SÁNCHEZ-RODRÍGUEZ; TRUJILLO-TORRES, 2016).

La violencia dentro de las aulas sigue siendo un reto a superar por parte de todos los agentes implicados en ese proceso. Así, del mismo modo que cambian todos los elementos que juegan un papel en los procesos de enseñanza-aprendizaje (E-A) cambian también las formas de violencia que se dan.

El bullying tradicional es ya un fenómeno ampliamente estudiado (ENRIQUEZVILLOTA; GARZÓN-VELASQUEZ, 2015; MENESINI; SALMIVALLI, 2017; OLWEUS, 1983) y del cual se ha abordado tanto el propio concepto (OLWEUS, 1993), como las causas (MISHNA et al., 2010; REIJNTJES et al., 2016), consecuencias (SMITH, 2014) y características (SWEARER; HYMEL, 2015; WAASDORP; BRADSHAW, 2015), y se ha visto complementado por este otro fenómeno del cyberbullying, aunque no sustituido.

Los ataques violentos a través de las tecnologías son conocidos como cyberbullying o ciberacoso (LANDAZABAL; LARRAIN, 2020). Este fenómeno es una derivación del bullying o acoso tradicional. Por lo que, en la mayoría de las ocasiones, los elementos, implicaciones y características son comunes.

El fenómeno del cyberbullying se basa en el empleo de diferentes dispositivos multimedia y de internet para acosar a otras personas. Este acoso puede ser, directo o indirecto, anónimo o

expreso (SARWAR et al., 2019). Las características del cyberbullying son (RUBIO-HERNÁNDEZ; DIAZ-LÓPEZ; CEREZO-RAMÍREZ, 2019):

- Incursión constante en la vida de la víctima.
- Repercusión y difusión mayor que en el bullying, pues las redes sociales facilitan este factor.
- Mayor facilidad a la hora de perpetrar el acoso.
- Si el acoso se anónimo, se pierde la percepción de sensación de culpa por parte del agresor.
- Se puede producir independientemente del contexto espacio-temporal.

En el cyberbullying un solo acto que suponga un elemento de violencia o intromisión en la privacidad de la otra persona a través de, por ejemplo, las redes sociales, aunque no sea continuado, ya puede ser considerado como tal (GONZALEZ CALATAYUD; PRENDES ESPINOSA, 2018). Del mismo modo, en este fenómeno, la persona que lo perpetra no tiene por qué ser, como en otros actos de acoso, alguien influyente o notable en un grupo determinado (PABIAN; VANDEBOSCH, 2016).

Dentro de las posibles agresiones que se sufren a través del cyberbullying, las más comunes son las agresiones por escrito (insultos, ofensas, amenazas…), del mismo modo que la divulgación de información personales, rumores o bulos (KOKKINOS; ANTONIADOU; MARKOS, 2014).

Las personas que sufren estos actos o víctimas, de manera generalizada cumplen una serie de características. Así, estas personas pueden padecer problemas o dificultades a nivel psicológico o físico, y son propensas a albergar dificultades interpersonales o intrapersonales, o mostrar una percepción general de una inseguridad manifiesta (JIMÉNEZ, 2019; MCLOUGHLIN et al., 2019).

Las consecuencias de esta situación en diferentes contextos, entre los que se encuentra el escolar se pueden agrupar en tres categorías. Por un lado, se encontrarían las consecuencias emocionales; por otro, las consecuencias académicas; por último, las consecuencias sociales. En estos tres grupos, estas consecuencias no son solo para la víctima, sino también para el agresor (MÉNDEZ-MATEO et al., 2019).

En las consecuencias emocionales resalta en ambos casos la ausencia total de empatía y sentimiento de culpa por parte del agresor (ESTÉVEZ; JIMÉNEZ; MORENO, 2018), y un incremento de trastornos y problemas emocionales y físicos como ansiedad o depresión, entre otros (SÁNCHEZ-LACASA; CEREZO-RAMÍREZ, 2018). Con respecto a las académicas es importante señalar que sí coinciden en ambos grupos, víctimas y agresores, las consecuencias pues se da fracaso escolar (O'CONNOR et al., 2018). Los problemas sociales que acarrea este fenómeno son una ausencia total de acatamiento de las normas a nivel general por parte del agresor y una sensación de soledad y abandono por parte de la víctima (GARAIGORDOBIL; MARTÍNEZ, 2014).

Centrando la temática en la educación, son muchas las investigaciones (BEER et al., 2019; CEREZO; RUBIO, 2017; THOMAS et al., 2019) que han puesto de manifiesto cómo los programas existentes y la formación proporcionada (TOMCZYK, 2019) a los diferentes agentes de los contextos escolares no son suficientes para la prevención e intervención ante estas situaciones. Algunos de estos programas o planes son el Plan Estratégico de Convivencia Escolar (MINISTERIOS DE EDUCACIÓN, CULTURA Y DEPORTE, 2016), el Plan "Asegúrate" (DEL REY et al., 2018) y Cyberprogram 2.0 (GARAIGORDOBIL; MARTÍNEZ-VALDERREY, 2014).

Debido a que estamos en una época en la que este fenómeno está adquiriendo mayor importancia en el ámbito educativo, donde la formación innovadora y renovada pasa por la tecnología, y siguiendo la línea establecida por otros estudios donde se trata de mostrar todos aspectos relevantes en el campo de investigación (ANDERSSON et al.; 2017; MARÍN-MARÍN et al., 2019), se considera necesario la realización de este análisis bibliométrico, pues no solo se ofrece una visión general de la cuestión, sino que se revelan las tendencias de la misma y de su producción científica.

2 Justificación y objetivos

Esta investigación tiene como finalidad el análisis, abordado desde un enfoque analítico, del recorrido e importancia del término "cyberbullying" tanto de manera general en el área de educación, como en la literatura científica relevante extraída de la base de datos Web of Science (WoS), con el objetivo de dar a conocer el estado de la cuestión acerca de cómo se encuentra todo lo relativo a la investigación de esta temática.

Los aspectos novedosos que presenta esta investigación, frente a otros del mismo corte (GÓMEZ-GARCÍA; RODRÍGUEZ-JIMÉNEZ; RAMOS, 2019; RODRÍGUEZ-GARCÍA; TRUJLLO; SÁNCHEZ, 2019), es la técnica de análisis bibliométrico que se ha empleado. Así, esta no se basa en la cuantificación de indicadores bibliométricos del tema de estudio, sino que también se realiza el desarrollo dinámico y estructural de los constructos delimitados, tal y como muestran otras investigaciones (HINOJO-LUCENA et al., 2020; RODRÍGUEZ-GARCÍA; FERNÁNDEZ; MORENO-GUERRERO, 2019). Por lo que esta investigación supone un aporte nuevo en lo que respecta a la literatura sobre este tema, pues no se ha encontrado ningún estudio realizado que contenga las mismas características que se exponen en este documento.

Los objetivos de esta investigación son los siguientes: a) Exponer el rendimiento y producción de la literatura científica sobre "cyberbullying"; b) Precisar la evolución científica del concepto de estudio; c) Determinar las temáticas más relevantes en el campo de estudio sobre el concepto; d) Establecer los autores más notables en la literatura sorbe el término que se estudia.

3 Materiales y método

3.1 Diseño de investigación

Este estudio ha empleado una metodología que se basa en la bibliometría, atendiendo a otros estudios previos extraídos de la literatura de impacto (HINOJOLUCENA et al., 2020; MORENO-GUERRERO, 2019). La utilización de esta técnica de investigación queda respaldada al conocer las potencialidades que supone la cienciometría en todo lo relativo a la cuantificación, evaluación y estimación de la evolución científica en el área concreta de estudio que se trabaja (FUENTES-CABRERA et al., 2019).

En el presente trabajo, de manera principal, se analizan dos elementos. Por un lado, el desarrollo estructural y, por otro, el desarrollo dinámico de todo lo relativo al "cyberbullying" a través de un análisis de co-palabras (HIRSCH, 2005). La manera en la que se ha llevado esto a cabo, radica en tomar el índice h y el volumen de citas a modo de indicadores de referencia (COBO et al., 2011) con el objetivo de realizar mapas científicos de mapas científicos en los cuales se examinen variables como el rendimiento y la localización y establecimiento de subdominios conceptuales, con el objetivo de determinar cómo se ha desarrollado la temática de estudio (LÓPEZ-ROBLES et al., 2019). Del mismo modo, se han tenido en cuenta otros

parámetros como el índice-g, el índice-hg y el índice-q2 para dotar de mayor información sobre la medida de las diferentes temáticas.

Este estudio ha respetado el protocolo de análisis de la matriz PRISMA-P, realizándose de igual manera diferentes técnicas de rastreo analítico y cálculo de documentos a través de la conformación de variables controladoras a nivel literario.

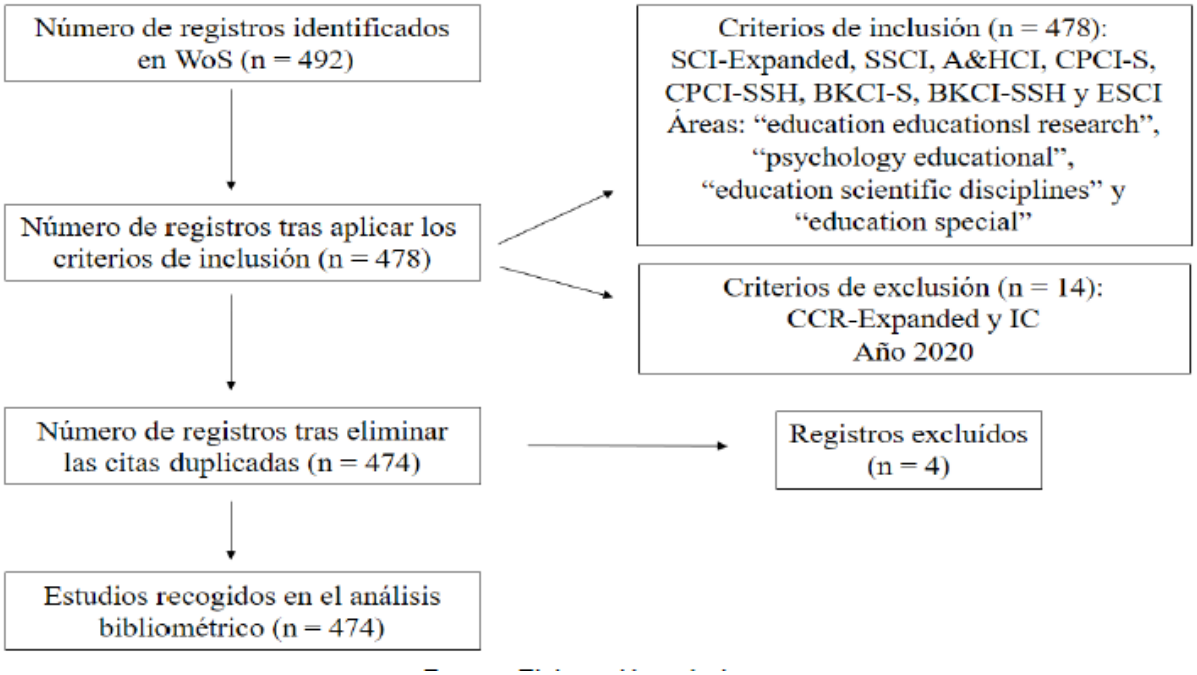
3.2 Procedimiento y análisis de datos

Este estudio se realizó en varias fases. En primer lugar, se escogió la base de datos de la cual se extrae la literatura científica. En este caso, la base de datos elegida fue WoS por ser un repositorio en el que se encuentra un gran volumen de producción literaria de impacto. En segundo lugar, se escogieron las palabras clave que se introducen en la herramienta de búsqueda de la base de datos. Así, se tuvo en cuenta la información proporcionada por los editores del número especial "Tecnologías del aprendizaje" de la revista Texto Livre. Del mismo modo, se realizó una búsqueda en el tesauro ERIC, con la finalidad de emplear términos recogidos por tesauros estandarizados y utilizados por la Comunidad científica. De esta búsqueda, se deriva la elección de la palabra "cyberbullying".

Tras todo este proceso, se procedió a realizar la búsqueda en WoS con la palabra clave "cyberbullying" donde se utilizó la siguiente ecuación de búsqueda: [TEMA] "cyberbullying". A través de esta búsqueda se identifica esta palabra tanto en el título, abstract y palabras clave de los diferentes documentos, esto es, si aparece en uno o varios de estos elementos ya se contabiliza como documento localizado. La búsqueda obtuvo un total de 2291 documentos, de los cuales una gran cantidad de ellos no hacían referencia a los objetivos propuestos, por lo que se realizó una nueva ecuación de búsqueda diferente a la presentada anteriormente: [TEMA] "cyberbullying" en las categorías "education educationsl research", "psychology educational", "education scientific disciplines" y "education special". En esta nueva ecuación la atención se pone sobre el ámbito educativo, obteniendo así un total de 492 artículos relacionados con los objetivos del estudio.

La búsqueda se ha realizado durante el mes de marzo de 2020 y para el análisis de ha aplicado un protocolo PRISMA que se detalla en la Figura 1. Así, la muestra final obtenida es de 474 publicaciones científicas.

Figura 1: Diagrama de flujo según la Declaración PRISMA



Fuente: Elaboración propia

Para el análisis de datos se han utilizado diferentes herramientas. En primer lugar, para la identificación del año, tipo de documento, institución, autores, medio de difusión, país, idioma y documentos más citados se han empleado el Analyze Results y Creation Citation Report, estas dos herramientas perteneces a la plataforma WoS. El desarrollo estructural y el dinamismo longitudinal del volumen científico se ha estudiado y realizado a través de SciMAT, siguiendo así lo establecido por Cobo et al., (2012). Con este software se han podido realizar las siguientes tareas:

- Reconocimiento: análisis de las palabras clave de la totalidad de la producción científica (n = 1248) y la creación de un mapa de co-currencia mediante nodos, originando así una red normaliazda de co-palabras. Así, se obtienen las palabras clave importantes (n = 1163) y a través de un algoritmo de clustering quedan definidos los temas, del mismo modo que los conceptos con un elevado nivel de atracción entre ellos.

- Reproducción: se realizó por medio de la elaboración de un diagrama estratégico y red temática fundamentada en dos principios, centralidad y densidad. Esta reproducción se representa de manera gráfica con la configuración de cuatro sectores diferenciados: 1) Superior-derecho=aglutina temas motores y relevantes; 2) Superior-izquierdo=temas consolidados pero aislados; 3) Inferiorizquierdo=temas en desarrollo o en desaparición; 4) Inferior-derecho: temas transversales y con escaso desarrollo.

- Determinación: se realizó a través de un estudio sobre la evolución de los nodos en intervalos temporales. Exactamente son tres estos intervalos (I1=2006-2013; I2=2014-2016; I3=2017-2019) para la clasificación y análisis de los documentos reportados. Por otro lado, con los autores se ha diseñado un único intervalo (IX=2006-2019) que aborda la totalidad de la producción. La fuerza de asociación se establece mediante el volumen de palabras clave que tienen en común los intervalos.

- Rendimiento: se extrajo a través de conexiones encontradas entre las palabras clave y otros conceptos tendentes del nodo. Para esto, se estudió la unidad de análisis que determina la unidad de valoración que contiene las palabras clave determinadas por los autores en las diferentes publicaciones. Otro indicador es el umbral de frecuencia, este se empleó para la determinación de la frecuencia mínima de los intervalos, siendo n = 2 para el primero, segundo y tercer intervalo y n = 3 para el intervalo X. Una red de este tipo hizo posible la realización de una red de co-ocurrencia de palabras clave y autores (co-words – co-authors). El valor de unión de coincidencia hizo posible articular los intervalos establecidos (cuatro para las palabras clave y uno para los autores). La medida de normalización determinó el umbral de unión, revelando la conexión mínima de la ocurrencia (palabras clave = I1 ≥ 1; I2 ≥ ; I3 ≥ 2; autores = IX ≥ 2). Para normalizar las conexiones se efectuó el índice de equivalencia eij = cij2/Root (ci - cj). El algoritmo de clustering, mediante centros simples, se utilizó para confeccionar el mapa de temas y subredes relacionadas. La evolución temática, a través del Jaccard Index, sirvió para determinar la medida de similitud que elabora el mapa de evolución y el mapa de transición mediante la ratio de inclusión (Tabla 1).

Tabla 1: Indicadores de producción y criterios de inclusión.

Configuración	Valores
Unidad de análisis	Palabras clave de autores, palabras clave de WoS Palabras clave: I_1 = (2), I_2 = (2), I_3 = (2)
Umbral de frecuencia	Aurtores: IX = (3)
Tipo de red	Co-ocurrencia
Umbral de valor de unión de co-ocurrencia	Palabras clave: I_1 = (1), I_2 = (1), I_3 = (2) Autores: IX = (2)
Medida de normalización	Índice de equivalencia
Algoritmo de agrupación	Tamaño máximo: ; Tamaño mínimo: 3
Medida evolutiva	Índice Jaccard
Medida superpuesta	Tasa de inclusión

Nota: I1: El periodo desde 2006 hasta 2013; I2: el periodo desde 2014 a 2016; I3: el periodo desde 2017 a 2019; Ix: 2006-2009.

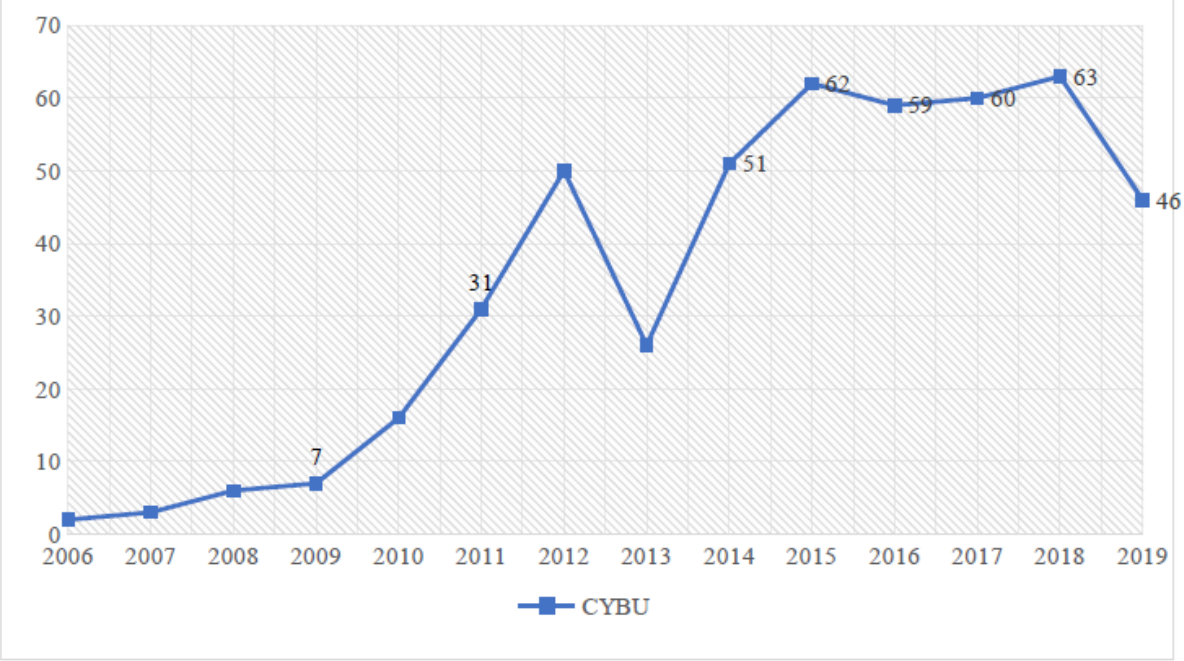
Fuente: Elaboración própria.

4 Resultados

4.1 Rendimiento y producción científica

La evolución de la producción científica se remonta del año 2006 hasta la actualidad, aunque su desarrollo ha sido desigual. Se observa una evolución de la producción desde el año 2006 hasta el año 2009 constante y escasa, pero desde el año 2010 hasta el 2012, la producción evoluciona de forma considerable. En el año 2013 hay un descenso considerable de la producción, pero en el año 2014 crece hasta mantenerse constante en el tiempo hasta el año 2018. En el año 2019 vuelve a descender la producción científica, volviendo a niveles del año 2014 (Figura 2).

Figura 2: Evolución de la producción científica.



Fuente: Elaboración propia.

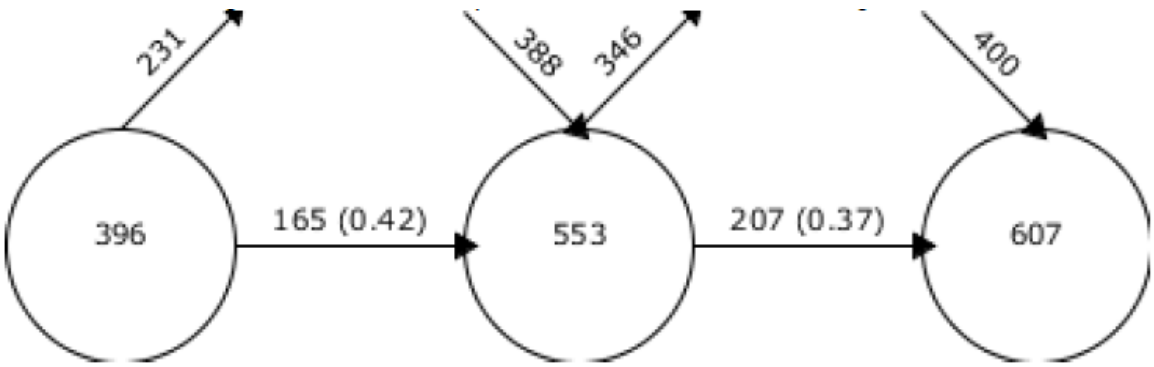
El idioma usado principalmente por parte de la comunidad educativa para presentar sus resultados es el inglés (n=412), seguido muy de lejos por el español (n=50) (https://bit.ly/33RXpi0). El área de conocimiento donde se recogen los estudios desarrollados sobre cyberbulling en el ámbito educativo es "education educational research" (n=366), seguido de lejos por "psychology educational" (n=148) (https://bit.ly/2WKdAg1). El principal

medio para mostrar los resultados de las investigaciones son los artículos (n=384), seguido muy de lejos por las comunicaciones (n=60) (https://bit.ly/2UE0sqc). La institución que más investiga sobre la temática de estudio planteado es "Queensland University of Technology QuT" (n=16), seguido muy de cerca de las instituciones "Universidad de Córdoba" (n=13), "Universidad de Londres" (n=13) y "Universidad de Sevilla" (n=13) (https://bit.ly/39kHHND). El autor con más producción sobre cyberbullying en el ámbito educativo es Campbell, M. (n=13), seguido a corta distancia de Cross, D. (n=11), Ortega-Ruiz, R. (n=10) y Smith, P.K. (n=10) (https://bit.ly/33Om72S). La principal fuente de publicación sobre este tipo de estudios es Journal of School Violence (n=26), seguido a una distancia considerable por School Psychology International (n=19) (https://bit.ly/3dB4U1h). El país con más contribuciones al campo de estudio establecido es Estados Unidos (n=102), seguido de España (n=89) (https://bit.ly/2WYTbUL). Sobre las publicaciones más citadas en el campo de CYBU encontramos las de Juvonen y Gross (2008), con 522 citas, y la de Li (2006), con 386 citas (https://bit.ly/3apMXAS).

4.2 Desarrollo estructural y temático

El desarrollo de palabras clave muestra datos sobre las palabras clave que salen o se incluyen en un determinado periodo temporal. También muestra la coincidencia entre los intervalos temporales establecidos. Analizando la Figura 3, se muestra como hay un alto índice de coincidencia entre los periodos establecidos, sobre todo entre el periodo primero y el periodo segundo. En este caso, se puede determinar que los estudios por parte de la comunidad científica tienen una base común, sobre todo entre el primer y segundo periodo, pero se vislumbra nuevos estudios entre el segundo y tercer periodo, dedo que el índice de coincidencia desciende ligeramente.

Figura 3: Continuidad de palabras clave entre intervalos contiguos.



Fuente: Elaboración propia

El rendimiento académico en cada uno de los intervalos temporales establecidos muestra las principales temáticas obtenidas del análisis estadístico, con sus respectivos indicadores estadísticos (índice h, índice g, índice hg e índice q2). Según se establece en la Tabla 2, en el primer intervalo (2006-2013) la temática "adolescents" es la que presenta mayor indicador bibliométrico, seguida de "intervention". En el segundo periodo (2014- 2016), la temática "cuberbullying" es la que presenta mayor indicador bibliométrico, le sigue, a una distancia considerable "prevalence". En el último intervalo temporal (2017- 2019), la temática "cyberbullying" vuelve a ser la que presenta mayor indicador bibliométrico.

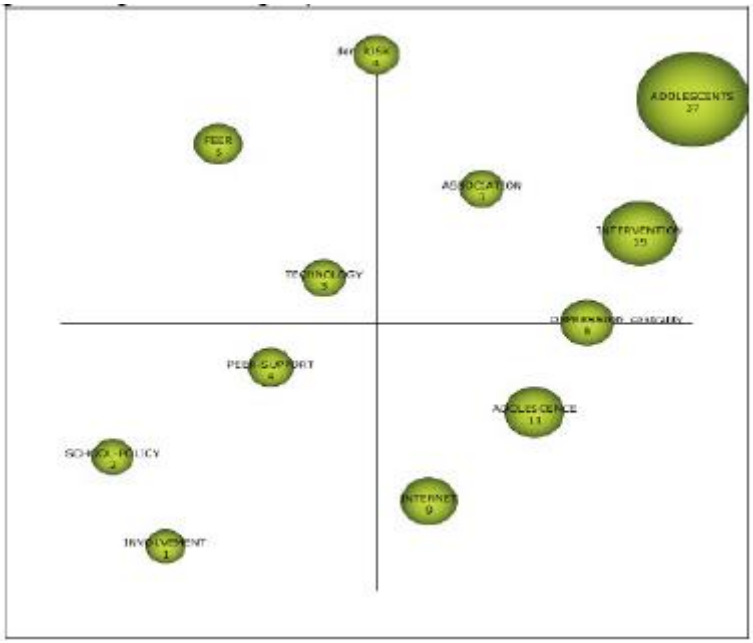
Tabla 2: Rendimiento temático en CYBU.

Intervalo 2006-2013						
Denominación	**Obras**	**Índice-h**	**Índice-g**	**Índice-hg**	**Índice-q2**	**Citas**
Adolescents	78	37	61	47.51	48.66	3807
Peer	5	5	5	5	15.81	230
Association	4	3	3	3	11.36	109
Intervention	24	19	23	20.9	31.43	1097
Risk	6	4	4	4	10.77	117
Technology	4	3	3	3	10.68	161
Peer-support	4	4	4	4	8.25	255
Adolescence	13	11	13	11.96	23.45	546
Depression	8	8	8	8	22.98	603
Internet	13	9	12	10.39	24	979
School-policy	2	2	2	2	9.49	57
Involvement	2	1	1	1	6.08	37
Intervalo 2014-2016						
Denominación	**Obras**	**Índice-h**	**Índice-g**	**Índice-hg**	**Índice-q2**	**Citas**
Social-Relationships	2	2	2	2	7.35	35
High-school	5	4	4	4	5.66	59
Gender-differences	5	4	5	4.47	8	52
Cyberbullying	104	24	31	27.28	28.14	1378
Mobile-phone	4	4	4	4	9.38	81
Facebook	4	2	3	2.45	8.49	46
Questionnaire	8	7	8	7.48	14.25	258
Help-seeking	3	3	3	3	8.12	57
Peer	6	5	6	5.48	11.4	151
Prevalence	34	13	21	16.52	18.73	498
Self-efficacy	8	7	8	7.48	10.58	136
Participant-roles	5	4	4	4	6.93	62
Internet	13	6	10	7.75	13.86	150
Risk	8	7	8	7.48	13.49	166
Depression	6	6	6	6	9.8	126
Emotions	4	4	4	4	11.31	113
Prevention	3	2	2	2	7.87	40
University-students	2	1	1	1	1.73	3
Programs	2	1	1	1	6.48	42
Intervalo 2017-2019						
Denominación	**Obras**	**Índice-h**	**Índice-g**	**Índice-hg**	**Índice-q2**	**Citas**
Cyberbullying	113	9	10	9.49	9.95	279
Mental-health	10	4	6	4.9	6.63	50
Children	15	3	3	3	3.46	23
Perceptions	11	4	6	4.9	6.63	39
Cybervictimization	16	6	8	6.93	8.12	76
Youth	11	4	6	4.9	5.66	39
Peer-victimization	12	3	4	3.46	3.87	18
Metaanalysis	9	3	5	3.87	3.87	26
Bystanders	3	2	2	2	3.74	9
Mobile-phone	4	2	3	2.45	3.46	9
Anonymity	2	2	2	2	2.83	7
Sites	3	1	1	1	1.41	4
Online	4	3	4	3.46	4.58	26

Fuente: Elaboración propia

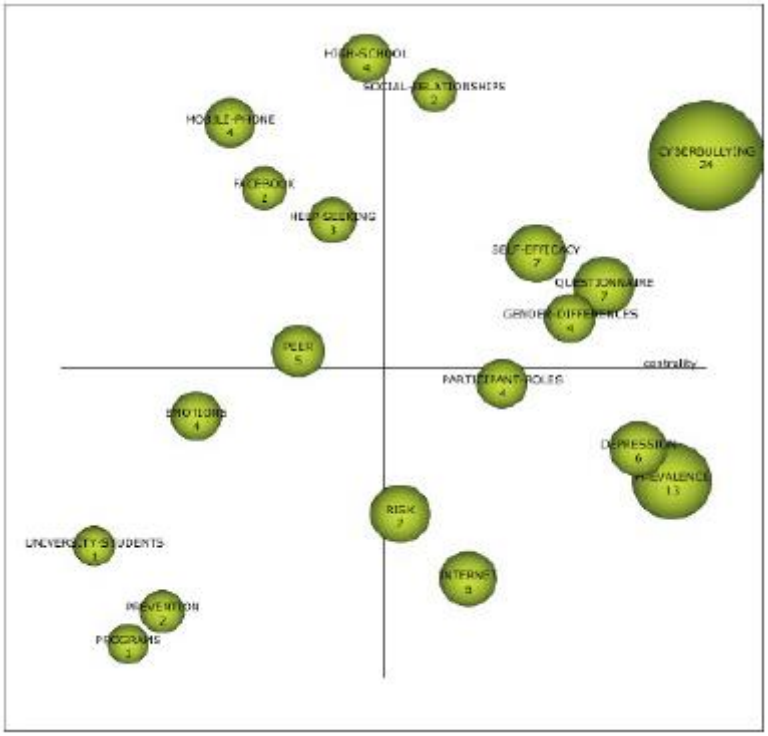
Los diagramas de intervalos generados muestra datos sobre la importancia de cada una de las temáticas, mediante un proceso de agrupación, según el indicador de Callon, que refleja el grado de interacción de una red con respecto a otras redes temáticas, pero desde dos ópticas: la centralidad, que mide la fuerza de los vínculos externos con otros temas, siendo la medida de la importancia de un tema en el desarrollo de un determinado campo de investigación; y la densidad, que analiza la fuerza interna de la red, identificando los vínculos internos entre todas las palabras clave que se agrupan alrededor de una temática concreta, ofreciendo así el grado de desarrollo del campo de estudio analizado. En el primer periodo (2006-2013), los temas motores son “adolescents”, que centran su estudio sobre el “bullying”, “victimization”, “prevalence”, “behavior”, “children”, “experiences”, “gender-differences” y “cyberbullying”; “association”, que centran sus estudios en “friendship”, “age-trends”, “friends”, “parents”, “predictors”, “teachers”, “self-esteem” y “schoold students”; e “intervention”, que se centran en “gender”, “anonymity”, “information and communication”, “impact”, “middle school”, “school”, “victims” y “prevention”. En el segundo periodo lo temas motores son “social relationships”, que centra sus estudios en “ICT-Use”, “research”, “popularity”, “elementaryschool”, “metaanalysis”, “social-competence”, “ support” y “friendship”; “cyberbullying”, que se centra en “bullying”, “victimization”, “cybervictimization”, “adolescents”, “children”, “ school”, “victims”, “aggression”; “self-efficacy”, que se centra en “health”, “competence”, “qualitative methods”, “peer victimization”, “loneliness”, “moral disengagement”, “secondary-education” y “social-support”; “questionnaire”, que se centra en “traditional bullying”, “evaluation”, “cognitive empathy”, “definition”, “scale”, “students”, “framework” y “emotional impact”; y “gender-differences” que se centra en “trends”, “perceived social support”, “ academic performance”, “cyber aggression”, “anxiety”, “youth”, “ bullying behaviors” y “high school students”. En el último periodo (2017-2019), lo temas motores son “cyberbullying”, que se centra en “bullying”, “victimization”, “prevalence”, “adolescents”, “behavior”, “school”, “victims” y “students”; “children” que se centra en “traditional-bullying”, “coping”, “special education”, “autism spectrum disorder”, “experiences”, “parents” y “safety”; y “cybervictimization” que se centra en “social support”, “gender”, “risk factors”, “intervention”, “questionnaire”, “aggresion”, “cyber aggression” y “self esteem”. En este periodo, además, se debe tener presente las temáticas “mobilephone” y “on-line”, debido a que son consideradas incógnitas, dado que pueden ser relevante en los próximos años o desaparecer (Figuras 4, 5 y 6).

Figura 4: Diagrama estratégico por índice-h de CYBU. Intervalo 2006-2013



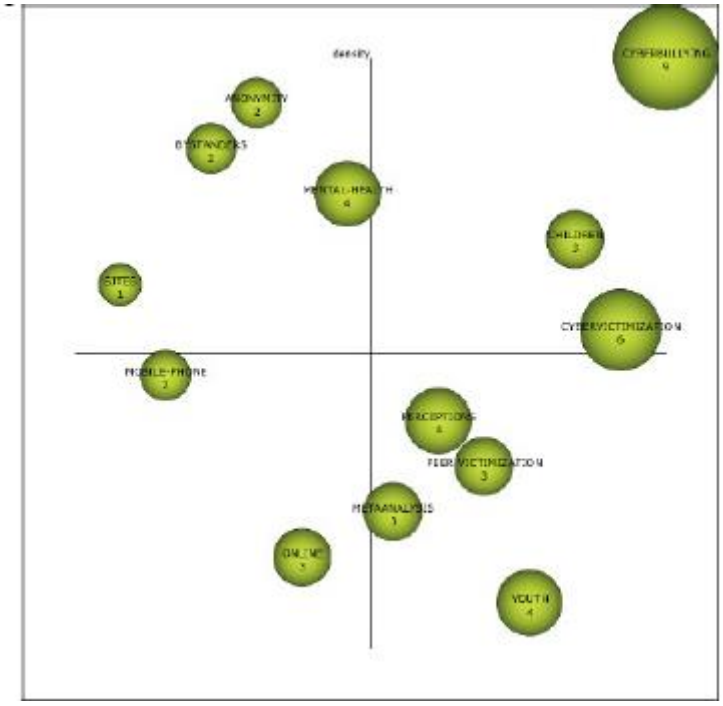
Fuente: de los autores.

Figura 5: Diagrama estratégico por índice-h de CYBU. Intervalo 2014-2016.



Fuente: de los autores.

Figura 6: Diagrama estratégico por índice-h de CYBU. Intervalo 2017-2019



Fuente: de los autores.

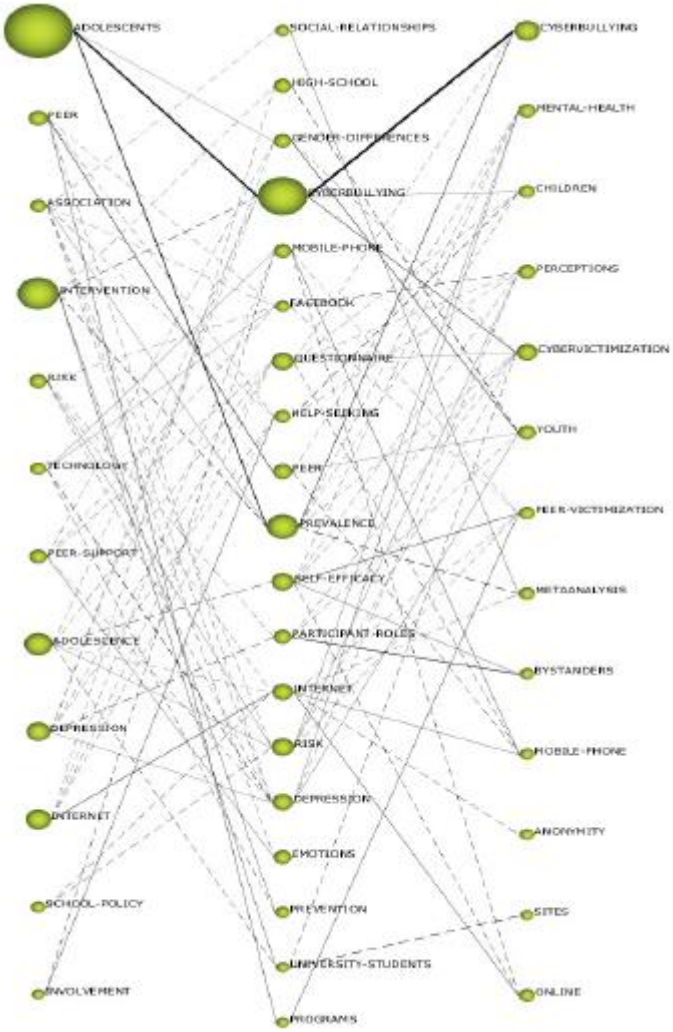
4.3 Evolución temática de los términos

La evolución temática representa la fuerza de relación establecida entre las temáticas de los diversos intervalos generados teniendo presente el índice Jaccard. La evolución se produce si un tema de un determinado intervalo comparte palabras clave con los intervalos previos o contiguos. Cuantas más palabras clave tengan en relación ambas temáticas de intervalos consecutivos, más sólida será su evolución. Los dos tipos de conexiones que se pueden producir son: línea continua, donde su conexión es temática; y línea discontinua, cuya conexión es mediante palabras clave. El grosor de las líneas muestra la fuerza de relación entre las temáticas.

Teniendo presente los datos conseguidos se puede establecer que existe una brecha conceptual en CYBU, dado que no hay una palabra clave que se repita en los tres periodos. Entre el primer y segundo periodo hay menos temáticas comunes que entre el segundo y el tercer periodo. A pesar de existir una brecha conceptual, hay una línea temática de investigación que destaca sobre las demás, que es la que se establece entre “adolescents-cyberbullying-cyberbullying”. Las demás temáticas, aunque puedan tener conexión temática, no presentan una fuerza de relación alta. Las conexiones entre los periodos son principalmente temáticas. En el primer periodo, las temáticas hacen referencia a los adolescentes, las tecnologías y las intervenciones,

mientras que en el segundo y tercer periodo las temáticas se orientan hacia las distintas etapas educativas, en distintos dispositivos tecnológicos y en las víctimas (Figura 7).

Figura 7: Evolución temátinunca ca por índice-h.

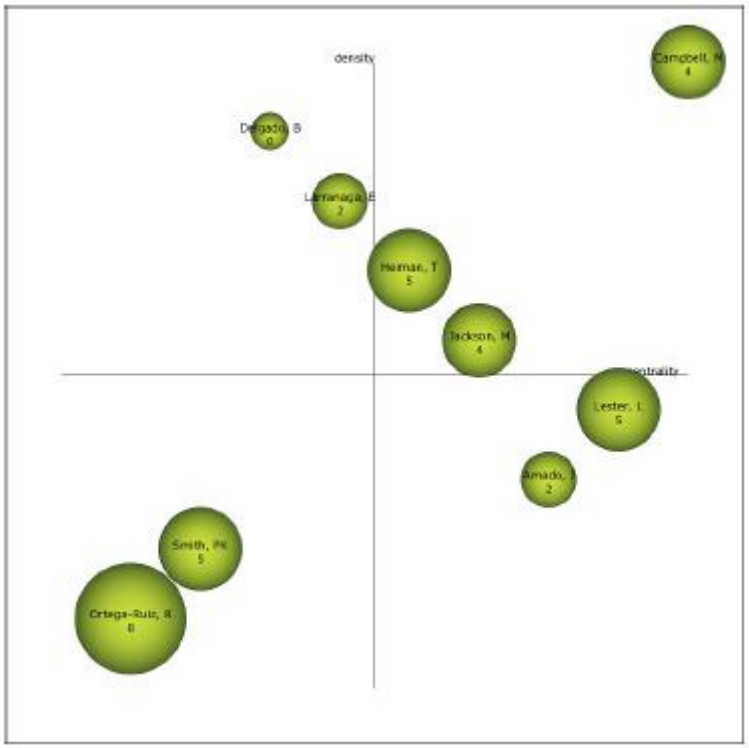


Fuente: de los autores

4.4 Autores con mayor índice de relevancia

Según los datos arrojados sobre los autores, se muestra como Campbell, M., Jackson, M., y Heiman, T., que son los autores motores sobre la temática. Se debe tener presente a los autores Ortega-Ruiz, R., y Smith, P. K., debido a que su ubicación en el diagrama los sitúa como autores incógnita, los cuales puede ser relevantes en el futuro o tender a desaparecer (Figura 8).

Figura 8: Diagrama estratégico de autores de toda la producción.



Fuente: de los autores.

5 Discusión y conclusiones

En la presentación de los resultados se ha mostrado los datos que se han obtenido a través de los objetivos planteados al inicio del estudio. Así, la producción científica a este respecto es bastante específica, ya que en la gran parte de esta todos los documentos atienden concretamente al tema de estudio siendo, por tanto, el cyberbullying el centro de las investigaciones.

Dentro de las investigaciones estudiadas, existen una gran cantidad de ellas de ámbito nacional (ORTEGA-RUIZ; ZYCH, 2016) y otras de ámbito internacional (HO; CHEN; NG; 2017; NOCENTINI et al., 2010).

El cyberbullying en los últimos años es considerado un elemento de gran incidencia en el ámbito educativo (RUBIO-HERNÁNDEZ; DIAZ-LÓPEZ; CEREZO-RAMÍREZ, 2019), tal y como se puede percibir tras observar las áreas de investigación donde se encuentra la literatura científica. Este fenómeno, por tanto, ha supuesto un incremento de la violencia a través de las nuevas formas de comunicación entre los estudiantes (MÉNDEZMATEO et al., 2019; MONTIEL; AGUSTINA, 2019).

La investigación a este respecto se hace necesaria, pues como se ha podido contrastar las palabras clave entre los diferentes periodos van cambiando, disminuyendo la coincidencia entre ellas, lo que podría suponer un cambio de tendencia a la hora de darse este fenómeno (SARWAR et al., 2019).

La evolución que se percibe el campo de estudio sobre la temática de cyberbullying por parte de la comunidad científica ha sido discontinua, dado que inició un crecimiento vertiginoso, en lo que a aportaciones se refiere, en el año 2009 y dura hasta el año 2012. Es a partir de ese momento, en el año 2013, donde se percibe un descenso considerable de la producción científica, volviendo a subir y manteniéndose estable hasta el año 2018. En el año 2019, de nuevo hay un descenso en la producción. Esto hace prever que posiblemente vuelva a repuntar la producción científica sobre este campo de estudio si se tiene en cuenta la evolución de toda la producción.

La radiografía del campo científico que puede obtenerse de este tipo de estudios, teniendo presente la base de datos Web of Science, es que suelen estar escritos en artículos de investigación e inglés, siendo el país con más incidencia en la producción científica Estados Unidos, en la categoría "Education Educational Research", siendo la institución de referencia "Queensland University of Technology QuT", la revista que más produce "Journal of School Violence" y el autor más prolífico y con más relevancia en el campo científico es Campell, M. La obra más citada es la de Juvonen y Gross (2008) con un total de 522 citas.

El desarrollo de palabras clave a lo largo de los tres periodos establecidos nos muestra que desde el año 2014 hasta la actualidad hay un cambio de tendencia en las investigaciones, dado que se reduce de forma considerable el porcentaje de palabras clave comunes entre ambos tiempos. Es reseñable indicar que desde los inicios de la producción científica hasta el año 2014, las tendencias de la comunidad educativa eran más concretas, dado que el nivel de coincidencia de palabras clave es elevado. Se puede determinar que hay un punto de inflexión desde el año 2016 hasta la actualidad. Además, este hecho se confirma con la evolución de temáticas, dado que solamente hay una línea de investigación asentada en el tiempo, que es "adolescents-cyberbullying-cyberbullying". El resto de temáticas varían y no tienen conexiones consistentes ni persistentes en el tiempo.

Los indicadores de palabras clave nos muestran que, en el primer periodo de la producción, la temática más relevante era "adolescent", para pasar luego, en los dos periodos restantes a ser

"cyberbullying". Es decir, se pasa de centrar los estudios en las personas a estudiar los aspectos relacionados con las acciones que generan y provoca el cyberbullying.

Si se atiende a los temas motores más relevantes de los tres periodos, se puede ver con más nitidez la prevalencia de estudio. En el primer periodo, la temática más relevante es "adolescents", junto a "association" e "intervention", lo que muestra que la incidencia se centraba en los adolescentes y en la intervención a realizar cuando se daban los casos de cyberbullying. En el segundo periodo, los temas motores varian de forma drástica, pasando a ser "cyberbullying", "self-efficacy", "questionnaire" y "genderdifference", lo que muestra que los estudios se focalizan en el desarrollo de instrumentos que permitan identificar los casos de "cyberbullying", además de analizar las posibles diferencias existentes a nivel de género. En el tercer periodo, los temas motores son "cyberbullying", "cybervictimization" y "children", lo que determina que una tendencia sobre el estudio del término, pero focalizando el estudio en las criminalizaciones de dichas acciones. En este caso, se puede vislumbrar que la edad de incidencia del "cyberbullying" está descendiendo, debido a que los estudios empiezan a focalizarse en los niños.

Se puede concluir, que el cyberbullying es una temática de investigación joven, dado que sus inicios datan de 2006, no ha tenido una evolución contante, ni en el nivel de producción científica, la cual es irregular, ni en la línea de investigación marcada por la comunidad educativa, pasando de analizar las incidencias en los adolescentes a pasar a investigar sobre las intervenciones y actuaciones desarrolladas para identificar y tratar el ciberbullying.

La prospectiva de este estudio es proporcionar a los investigadores una visión de las últimas tendencias acerca de las temáticas de mayor relevancia e interés dentro de la comunidad científica. Del mismo modo, se pretende indicar aquellos aspectos en los que los últimos estudios se han basado, para así tener unos fundamentos sobre los que comenzar, desarrollar y enfocar sus investigaciones.

Las limitaciones que se han dado en esta investigación son varias. En un primer momento, está la depuración de los datos extraídos de WoS, donde existen documentos repetidos o que no se ajustan a la temática abordada. En segundo lugar, la equidad en lo que respecta al número de documentos por intervalo, que en todo momento ha sido prioridad para los investigadores el intentar alcanzarla. Por último, los parámetros establecidos en esta investigación han sido marcados a través de criterios de los investigadores, que han intentado presentar unos resultados que se asemejen en tamaño y relevancia. Por ello, los datos que aquí se presentan se

deben tomar con precaución pues el cambio de los parámetros que se establecen puede hacer que cambien tanto las cantidades como las diferentes conexiones. Las futuras líneas de investigación plantean el desarrollo de actuaciones pedagógicas dentro del ámbito educativo que tengan como elemento central el cyberbullying.

Referencias

ANDERSSON, C.; ANTELIUS, J.; MÅNSSON, J.; SUND, K. Technical efficiency and productivity for higher education institutions in Sweden. *Scandinavian journal of educational research*, v. 61, n. 2, p. 205-223, 2017.

AZNAR-DÍAZ, I.; KOPECKY, K.; ROMERO, J. M.; CÁCERES, M. P.; TRUJILLO-TORRES, J. M. Patologías asociadas al uso problemático de Internet. Una revisión sistemática y meta-análisis en WOS y Scopus. *Revista Bibliotecológica: archivonomía, bibliotecología e información*, v. 34, n. 82, p. 229-253, 2019.

BEER, P.; HAWKINS, C.; HEWITSON, D.; HALLETT, F. Perpetrators, victims, bystanders and upstanders: cyberbullying in a special school context. Support for Learning, v. 34 n. 3, p. 340-356, 2019. CEREZO, F.; RUBIO, F.J. Medidas relativas al acoso escolar y ciberacoso en la normativa autonómica española. Un estudio comparativo. *Revista Electrónica Interuniversitaria de Formación del Profesorado,* v. 20, n. 1, p. 113, 2017. https://doi.org/10.6018/reifop/20.1.253391

COBO, M. J.; LÓPEZ-HERRERA, A. G.; HERRERA-VIEDMA, E.; HERRERA, F. Science mapping software tools: Review, analysis, and cooperative study among tools. *Journal of the American Society for information Science and Technology*, v. 62, n. 7, p. 1382-1402, 2011. https://doi.org/10.1002/asi.21525

COBO, M. J.; LÓPEZ-HERRERA, A. G.; HERRERA-VIEDMA, E.; HERRERA, F. SciMAT: A new science mapping analysis software tool. *Journal of the American Society for Information Science and Technology,* v. 63, n. 8, p. 1609-1630, 2012. https://doi.org/10.1002/asi.22688

COOPER, K.; QUAYLE, E.; JONSSON, L.; SVEDIN, C. G. Adolescents and self-taken sexual images: A review of the literature. *Computers in human behavior,* v. 55, p. 706-716, 2016.

DEL REY, R.; MORA-MECHÁN, J.: CASAS, J.: ORTEGA-RUIZ, R.; ELIPE, P. Programa «Asegúrate»: Efectos en ciberagresión y sus factores de riesgo. *Comunicar*, v. 56, n. 3, p. 39-48, 2018.

ENRIQUEZ-VILLOTA, M. F.; GARZÓN-VELASQUEZ, F. El acoso escolar. *Saber, Ciencia y Libertad*, v. 10, n. 1, p. 219-233, 2015. http://dx.doi.org/10.22525/sabcliber.2015v10n1.219234

ESTÉVEZ, E.; JIMÉNEZ, T. I.; MORENO, D. Aggressive behavior in adolescence as a predictor of personal, family, and school adjustment problems. *Psicothema*, v. 30, n. 1, p. 66-73, 2018.

FUENTES-CABRERA, A.; MORENO-GUERRERO, A. J.; POZO-SÁNCHEZ, J. S.; RODRÍGUEZ-GARCÍA, A. M. Bullying among Teens: Are Ethnicity and Race Risk Factors for Victimization? A Bibliometric Research. *Education Sciences*, v. 9, n. 3, p. 220, 2019. https://doi.org/10.3390/educsci9030220

GARAIGORDOBIL, M.; MARTÍNEZ-VALDERREY, V. Efecto del Cyberprogram 2.0 sobre la reducción de la victimización y la mejora de la competencia social en la adolescencia. *Revista de Psicodidáctica*, v. 19, n. 2, p. 289-305, 2014.

GÓMEZ-GARCÍA, G.; RODRÍGUEZ-JIMÉNEZ, C.; RAMOS, M. Virtual Reality in Physical Education area. *Journal of Sport and Health Research*, v. 11, n. Supl 1, p. 177-186, 2019.

GONZALEZ CALATAYUD, V.; PRENDES ESPINOSA, M. P. Cyberbullies: A quantitative research with secondary students. *PIXEL-BIT-REVISTA DE MEDIOS Y EDUCACION*, n. 53, p. 137-149, 2018.

HINOJO-LUCENA, F. J.; DÚO-TERRÓN, P.; RAMOS, M.; RODRÍGUEZ-JIMÉNEZ, C.; MORENO-GUERRERO, A. J. Scientific Performance and Mapping of the Term STEM in Education on the Web of Science. *Sustainability*, v. 12, n. 6, p. 1-20, 2020.

HIRSCH ADLER, A. Construcción de una escala de actitudes sobre ética profesional. *Revista electrónica de investigación educativa*, v. 7, n. 1, p. 01-14, 2005.

HO, S. S.; CHEN, L.; NG, A. P. Comparing cyberbullying perpetration on social media between primary and secondary school students. *Computers & Education*, v. 109, p. 74- 84, 2017. https://doi.org/10.1016/j.compedu.2017.02.004

JIMÉNEZ, R. Multiple Victimization (Bullying and Cyberbullying) in Primary Education in Spain from a Gender Perspective. *Multidisciplinary Journal of Educational Research*, v. 9, n. 2, p. 169-193, 2019. http://dx.doi.org/10.17583/remie.2019.4272

KOKKINOS, C. M., ANTONIADOU, N., Y MARKOS, A. Cyber-bullying: An investigation of the psychological profile of university student participants. *Journal of Applied Developmental Psychology*, v. 35, n. 3, p. 204-214, 2014. https://doi.org/10.1016/j.appdev.2014.04.001

LANDAZABAL, M. G.; LARRAIN, E. Acoso y ciberacoso en adolescentes LGTB: Prevalencia y efectos en la salud mental. *Comunicar: Revista científica iberoamericana de comunicación y educación*, n. 62, p. 79-90, 2020.

LÓPEZ-ROBLES, J. R.; GUALLAR, J.; OTEGI-OLASO, J. R.; GAMBOA-ROSALES, N. K. El profesional de la información (EPI): bibliometric and thematic analysis (2006-2017). *El profesional de la información*, v. 28, n. 4, p. e280417, 2019. https://doi.org/10.3145/epi.2019.jul.17

MARÍN-MARÍN, J. A.; LÓPEZ-BELMONTE, J.; FERNÁNDEZ-CAMPOY, J. M.; ROMERORODRÍGUEZ, J. M. Big Data in Education. A Bibliometric Review. *Social Sciences*, v. 8, n. 8, p. 223, 2019. https://doi.org/10.3390/socsci8080223

MCLOUGHLIN, L. T.; SPEARS, B. A.; TADDEO, C. M.; HERMENS, D. F. Remaining connected in the face of cyberbullying: Why social connectedness is important for mental health. *Psychology in the Schools*, v. 56, n. 6, p. 945-958, 2019. https://doi.org/10.1002/pits.22232

MÉNDEZ-MATEO, I.; RUIZ-ESTEBAN, C.; PEDRO-MARTINEZ, J.; CEREZO, F. Cyberbullying according to sociodemographic and academic characteristics among university students. *Revista Española de Pedagogía*, v. 77, n. 273, p. 261-276, 2019.

MENESINI, E.; SALMIVALLI, C. Bullying in schools: The state of knowledge and effective interventions. Psychology, *Health & Medicine*, v. 22, n. sup1, p. 240-253, 2017.

MINISTERIOS DE EDUCACIÓN, CULTURA Y DEPORTE. *Plan Estratégico de Convivencia Escolar*. 2016.

MISHNA, F.; COOK, C.; GADALLA, T.; DACIUK, J.; Y SOLOMON, S. Cyber bullying behaviors among middle and high school students. *American Journal of Orthopsychiatry*, v. 80, n. 3, p. 362-374, 2010.

MONTIEL, I.; AGUSTINA, J. R. Educational challenges of emerging risks in cyberspace: foundations of an appropriate strategy for preventing online child victimisation. *REVISTA ESPANOLA DE PEDAGOGIA*, v. 77, n. 273, p. 277-294, 2019.

MORENO-GUERRERO, A. J. Estudio bibliométrico de la producción científica en Web of Science: Formación Profesional y blended learning. *Píxel-Bit. Revista de Medios y Educación*, n. 56, p. 149-168, 2019.

NOCENTINI, A.; CALMAESTRA, J.; SCHULTZE-KRUMBHOLZ, A.; SCHEITHAUER, H.; ORTEGA, R.; MENESINI, E. Cyberbullying: Labels, behaviours and definition in three European countries. *Journal of Psychologists and Counsellors in Schools*, v. 20, n. 2, p. 129-142, 2010.

O'CONNOR, K.; DROUIN, M.; DAVIS, J.; THOMPSON, H. Cyberbullying, revenge porn and the mid-sized university: Victim characteristics, prevalence and students' knowledge of university policy and reporting procedures. *Higher Education Quarterly*, v. 72, n. 4, p. 344-359, 2018. https://doi.org/10.1111/hequ.12171

OLWEUS, D. *Bullying at school: What we know and what we can do*. Oxford: Blackwell, 1993.

OLWEUS, D.; LIMBER, S. P. Olweus bullying prevention program. En: *The Handbook of Bullying in Schools: An International Perspective*. Nueva York: Routledge, 1983. p. 37- 401.

ORTEGA-RUIZ, R.; ZYCH, I. La ciberconducta y la psicología educativa: retos y riesgos. *Psicología Educativa*, v. 22, n. 1, p. 1-4, 2016. http://doi.org/10.1016/j.pse.2016.04.001

PABIAN, S.; VANDEBOSCH, H. An investigation of short-term longitudinal associations between social anxiety and victimization and perpetration of traditional bullying and cyberbullying. *Journal of youth and adolescence*, v. 45, n. 2, p. 328-339, 2016.

REIJNTJES, A.; VERMANDE, M.; THOMAES, S.; GOOSSENS, F.; OLTHOF, T.; ALEVA, L.; VAN DER MEULEN, M. Narcissism, bullying, and social dominance in youth: A longitudinal analysis. *Journal of Abnormal Child Psychology*, v. 44, p. 63-74, 2016.

RODRÍGUEZ-GARCÍA, A. M.; FERNÁNDEZ, M. A.; MORENO-GUERRERO, A. J. Evolución científica de lenguas en el contexto universitario (1900-2019). *Texto Livre: Linguagem e Tecnologia*, v. 12, n. 2, p. 16-36, 2019.

RODRÍGUEZ-GARCÍA, A. M.; TRUJILLO, J. M.; SÁNCHEZ, J. Impacto de la productividad científica sobre competencia digital de los futuros docentes: aproximación bibliométrica en Scopus y Web of Science. *Revista Complutense de Educación*, v. 30, n. 2, p. 626-646, 2019.

RUBIO-HERNÁNDEZ, F. J.; DIAZ-LÓPEZ, A.; CEREZO-RAMÍREZ, F. Bullying and cyberbullying: The answer of the autonomous communities. *Revista Electrónica Interuniversitaria de Formación del Profesorado*, v. 22, n. 1, p. 145-157, 2019.

RUIZ-PALMERO, J.; SÁNCHEZ-RODRÍGUEZ, J.; TRUJILLO-TORRES, J. M. Utilización de internet y dependencia a teléfonos móviles en adolescentes. *Revista Latinoamericana de Ciencias Sociales, niñez y juventud*, v. 14, n. 2, p. 1357-1370, 2016.

SÁNCHEZ-LACASA, C.; CEREZO-RAMÍREZ, F. Consecuencias psicológicas, sociales y académicas del ciberbullying: una revisión teórica. En: GÁZQUEZ, J. J.; MOLERO, M. M.; PÉREZ-FUENTES, M. C.; MARTOS, A.; SIMÓN, M. M.; BARRAGÁN, A. B.; SISTO, M. (eds.), *La convivencia Escolar: Un Acercamiento Multidisciplinar*. Almería, España: ASUNIVEP, 2018. p. 19-24.

SARWAR, B.; ZULFIQAR, S.; AZIZ, S.; EJAZ CHANDIA, K. Usage of social media tools for collaborative learning: The effect on learning success with the moderating role of cyberbullying. *Journal of Educational Computing Research*, v. 57, n. 1, p. 246-279, 2019. https://doi.org/10.1177/0735633117748415

SMITH, P. K. *Understanding school bullying: Its nature and prevention strategies*. London: Sage, 2014.

SWEARER, S. M.; HYMEL, S. Understanding the psychology of bullying: Moving toward a social-ecological diathesis-stress model. *American Psychologist*, v. 70, p. 344-353, 2015.

SWEET, K. S., LEBLANC, J. K., STOUGH, L. M., Y SWEANY, N. W. Community building and knowledge sharing by individuals with disabilities using social media. *Journal of Computer Assisted Learning*, v. 36, n. 1, p. 1-11, 2020. https://doi.org/10.1111/jcal.12377

THOMAS, H. J.; SCOTT, J. G.; COATES, J. M.; CONNOR, J. P. Development and validation of the Bullying and Cyberbullying Scale for Adolescents: A multi-dimensional measurement model. *British Journal of Educational Psychology*, v. 89, n. 1, p. 75-94, 2019. https://doi.org/10.1111/bjep.12223

TOMCZYK, Ł. What Do Teachers Know About Digital Safety? *Computers in the Schools*, v. 36, n. 3, p. 167-187, 2019. https://doi.org/10.1080/07380569.2019.1642728

WAASDORP, T. E.; BRADSHAW, C. P. The overlap between cyberbullying and traditional bullying. *Journal of Adolescent Health*, v. 56, n. 5, p. 483-488, 2015.

5.3.Tercera publicación

Revisión Sistemática de la literatura sobre la Seguridad Digital en estudiantes de Educación Superior

Este artículo ha sido publicado en la revista *Información Tecnológica* (CIT) (ISNN 0718-0764). Es una revista internacional que admite trabajos de diferentes áreas como ciencia, ingeniería y tecnología. Los trabajos deben ser de investigación y que tengan un impacto relevante en el desarrollo de países de Iberoamérica. La revista se encuentra en un total de 12 índices internacionales.

Se haya en el cuartil Q2 2020, SJR 0.22

La revista se encuentra indexada en las siguientes bases de datos: Scielo, CIT, Chemicail Abstract, Engineering Village Compendex, Dialnet y Latindex.

Referencia bibliográfica:

Trujillo-Torres, J.M., Rodríguez-Jiménez, C., Alonso-García, S., y Berral-Ortiz, B. (2024). Revisión sistemática de la literatura sobre la Seguridad Digital en estudiantes de Educación Superior. *Información Tecnológica*, En Prensa.

Revisión sistemática de la literatura sobre la Seguridad Digital en estudiantes de Educación Superior

Juan Manuel Trujillo-Torres[1], Carmen Rodríguez-Jiménez[2], Santiago Alonso-García[1], Blanca Berral-Ortiz[1]

(1) Facultad de Ciencias de la Educación, Dpto. de Didáctica y Organización Escolar, Univ. de Granada, Prof. Vicente Callao - Fte Ciencias Educación, 18011, 18011, Granada

(correo-e: jttorres@ugr.es; salonsog@ugr.es; blancaberral@ugr.es)

(2) Facultad de Ciencias de la Educación y del Deporte, Dpto. Didáctica y Organización Escolar, Univ. de Granada, Ctra. Alfonso XIII, s/n, 52005 Melilla

(correo-e: carmenrj@ugr.es)

Resumen

La seguridad digital y la privacidad en línea son preocupaciones importantes en la sociedad actual, especialmente en el entorno educativo. Los estudiantes de Educación Superior por el simple hecho de emplear su competencia digital en su formación están en riesgo de ser víctimas de ciberdelitos, como el acoso en línea, el robo de identidad y la exposición a contenido inapropiado. Por lo tanto, es crucial que se implementen medidas de seguridad efectivas para proteger a los estudiantes y garantizar un entorno de aprendizaje seguro y saludable. La presente investigación tiene como objetivo analizar las prácticas actuales de seguridad digital y la percepción de riesgos de los estudiantes de Educación Superior en relación con su uso de las TIC. Para ello, se llevará a cabo una revisión sistemática de la literatura sobre seguridad digital, ciberseguridad, seguridad en Internet y seguridad en línea, así como sobre el uso de tecnologías digitales en la etapa nombrada. Con esta investigación se espera identificar las mejores prácticas y estrategias para mejorar la seguridad digital en la etapa de Educación Superior y reducir el riesgo de ciberdelitos en los estudiantes.

Palabras clave: seguridad digital; educación *superior****, competencia digital, TIC, revisión sistemática***

Systematic literature review on Digital Safety in Higher Education students

Abstract

Digital security and online privacy are important concerns today, especially in the educational environment. Secondary school students are at risk of falling victim to cybercrime, such as online bullying, identity theft and exposure to inappropriate content. Therefore, it is crucial that effective security measures are implemented to protect students and ensure a safe and healthy learning environment. The present research aims to analyze current digital safety practices and risk perceptions of secondary school students in relation to their use of digital technologies. To

this end, a systematic review of the literature on cybersecurity, Internet safety and online safety, as well as the use of digital technologies in secondary education will be carried out. This research is expected to identify best practices and strategies to improve digital safety in secondary education and reduce the risk of cybercrime among students.

Keywords: digital security; higher education, digital competence, ICT, systematic review

Introducción

La seguridad digital es un aspecto fundamental en el mundo actual, en el que el uso de tecnologías de la información y comunicación (TIC) se ha vuelto una herramienta esencial en todos los ámbitos, incluido el educativo. Los estudiantes de educación superior no son ajenos a este fenómeno, ya que cada vez más hacen uso de dispositivos electrónicos y plataformas en línea para acceder a información, comunicarse y realizar actividades académicas (Castillejos et al., 2016).

Sin embargo, el incremento en la utilización de estas tecnologías también ha generado una serie de riesgos y amenazas a la privacidad y seguridad de la información de los usuarios, como lo son el robo de identidad, ciberacoso, acceso no autorizado a datos personales, entre otros. En este contexto, es fundamental que los estudiantes de educación superior estén conscientes de estos riesgos y cuenten con las habilidades y conocimientos necesarios para protegerse en el entorno digital (Anderson, 2003).

A pesar de la importancia de la seguridad digital en la vida de los estudiantes de educación superior (Björk, et al., 2020), existe una escasa comprensión de cómo estos jóvenes enfrentan y abordan los riesgos relacionados con la seguridad en línea. Asimismo, se desconoce la efectividad de las estrategias y medidas de protección que se están implementando en las instituciones educativas para garantizar la seguridad digital de sus estudiantes. Esta falta de conocimiento impide el desarrollo de políticas y prácticas adecuadas para mejorar la seguridad digital en el entorno universitario.

Por lo tanto, es necesario llevar a cabo una revisión sistemática de la literatura sobre la seguridad digital en estudiantes de educación superior, con el objetivo de identificar y analizar los principales riesgos y amenazas a los que están expuestos, así como las estrategias de prevención y protección que se han propuesto e implementado en este ámbito. Dicha investigación permitirá obtener una panorámica integral de la situación actual, a fin de

desarrollar recomendaciones y pautas para mejorar la seguridad digital en el contexto educativo superior.

La importancia de llevar a cabo una investigación sobre la seguridad digital en estudiantes de educación superior radica en el papel crucial que desempeña la tecnología en la vida de estos jóvenes, tanto en el ámbito académico como en el personal (Çebi y Reisoğlu, 2020; Cózar y Roblizo, 2014). Dado que los estudiantes universitarios son usuarios activos de internet y están expuestos a una gran variedad de riesgos y amenazas en línea, es fundamental comprender sus conocimientos, actitudes y comportamientos en relación con la seguridad digital.

Una revisión sistemática de la literatura en este campo permitiría identificar las tendencias y brechas en la investigación existente, así como resaltar las áreas que requieren una mayor atención. Al sintetizar y analizar el conocimiento actual sobre la seguridad digital en estudiantes universitarios, se podrían desarrollar estrategias y programas de intervención más eficaces para mejorar la conciencia y la protección de estos jóvenes en el entorno digital. Además, esta investigación podría informar a educadores, administradores y responsables políticos sobre las mejores prácticas y enfoques para fomentar una cultura de seguridad en línea en las instituciones de educación superior.

La metodología de esta investigación consiste en un enfoque descriptivo y documental, analizando fuentes secundarias para obtener información relevante sobre la seguridad digital en la educación superior. Se utilizará un método mixto, combinando enfoques cuantitativos y cualitativos, para ofrecer un análisis sólido y comprensivo. La recopilación de datos se realizará a través de las bases de datos Scopus y Web of Science, siguiendo un procedimiento de investigación específico que incluye la selección de la base de datos, definición de tesauro de búsqueda, depuración de la información, selección de artículos y elaboración del informe de literatura.

La presente revisión de literatura se divide en cuatro secciones incluyendo la presente introducción; seguidamente, se describe la metodología utilizada. Posteriormente, se detallan los principales indicadores de literatura para entender el fenómeno investigativo. Finalmente, se relacionan las conclusiones y principales resultados.

METODOLOGÍA

En este trabajo se ha optado por acudir a una metodología propia de los estudios bibliométricos, pues permite analizar y evaluar la producción científico-investigadora en un área de

conocimiento determinada (Cruz, 1999; Fernández-Cano y Bueno-Sánchez, 1998). A continuación, se exponen los diferentes componentes tenidos en cuenta a la hora de la realización del presente estudio y los cuales determinan los resultados del mismo.

Tipo de estudio

Para el desarrollo de la presente investigación se requiere un estudio de tipo descriptivo y documental debido al interés acerca del análisis de la literatura. Un estudio descriptivo es el que muestra conocimiento acerca de la realidad encontrada en un espacio, dicho de otro modo, es el estado real en el que se encuentra un objeto de estudio o una variable de investigación (Gutiérrez-Osco y Luján-Coronel, 2022). Por otra parte, una investigación de tipo documental es un procedimiento cuya esencia es la indagación en fuentes secundarias para obtener información que pueda ser recuperada, analizada e interpretada y se encuentra digitalizada, impresa, entre otras (Dávila-Morán et al., 2022). La recopilación se llevará a cabo por medio de los documentos almacenados en la base de datos Scopus y *Web of Science* sobre la seguridad digital en la educación superior. Según lo anterior, estos dos tipos de estudios permitirán la descripción de los diferentes enfoques y conceptos, así como los principales indicadores de literatura.

Método de investigación

Para el desarrollo del presente objeto de estudio se precisa aplicar un método de investigación mixto. El método de investigación mixto es el más completo, ya que profundiza, amplia y nos brinda mayor seguridad en las conclusiones de la investigación, combinar los métodos cuantitativos y cualitativos, nos brindan soporte (Del Carpio y Gilvonio, 2019). Adicionalmente, se recurre al procedimiento de investigación definido por Rodríguez et al., (2020) donde se hacen específicos el cumplimiento de seis pasos así: la base de datos seleccionada es Scopus y Web of Science; la definición de tesauro de búsqueda; depuración de la información que consiste en refinar los resultados e incluso eliminar duplicados; la selección de artículos para la revisión que comprendan el total de la muestra; finalmente, el informe de literatura.

Al seleccionar las bases de datos Scopus y Web of Science para realizar una revisión sistemática de literatura, se garantiza el acceso a una amplia y rigurosa colección de publicaciones académicas y científicas de alta calidad. Scopus es la base de datos de resúmenes y citas de literatura científica más grande del mundo, que abarca diversas disciplinas y proporciona herramientas analíticas para rastrear, analizar y visualizar la investigación. Por

otro lado, Web of Science es un recurso multidisciplinario conocido por su índice de citas y su capacidad para identificar investigaciones relevantes y de impacto. Ambas bases de datos ofrecen una cobertura exhaustiva y actualizada de la literatura académica, lo que permite identificar estudios y tendencias relevantes en el tema de investigación, garantizando una revisión sistemática de alta calidad y confiabilidad.

Los metadatos que finalmente se han obtenido fueron extraídos del análisis de otros estudios de corte semejante (Wright y Liang, 2019). Los indicadores que se han seguido son el año de publicación, autores más productivos, documentos más citados, las corrientes de investigación más seguidas en la temática de estudio y conexión entre descriptores. La confección de la muestra final (n=62) se llevó a cabo tras un refinamiento guiado por una serie de criterios (tabla 1).

Las palabras clave fueron buscadas y delimitadas por el Thesaurus ERIC. Partiendo de esa base, los conceptos extraídos resultantes fueron “Computer segurity” AND “Higher Education”. Estas palabras fueron introducidas en las bases de datos ya mencionadas con el operador booleano “AND”, como también se muestra arriba, para así, extraer la producción científica que tenga estos términos en su título, resumen, palabras clave y cuerpo del texto. No solo es preciso tener en cuenta los criterios de inclusión y exclusión, sino que es preciso delimitar una serie de preguntas que pretenden alcanzar un objetivo determinado a través de la consecución de un indicador (tabla 2). Por otro lado, se recurre al protocolo PRISMA (figura 1) donde se sintetiza la depuración de los documentos a estudiar.

Tabla 1: Criterios de inclusión y exclusión utilizados en el análisis bibliométrico

Criterios de inclusión	Criterios de exclusión
Producción desde su origen al año 2022	Producción del año 2023 al tratarse de un año no finalizado
Artículos de revista	Capítulos de libro, libros, comunicaciones a congresos, etc.
Estudios empíricos	Estudios o revisiones teóricas
Artículos escritos en inglés o español	Artículos no escritos en inglés o español

Investigaciones y experiencias que aborden cómo se trabaja la seguridad digital con los estudiantes de Educación Superior	Investigaciones y experiencias que no aborden la seguridad digital en Educación Superior o que lo hagan con otros agentes implicados en el proceso de E-A (docentes, familias, etc.)

Tabla 2: Objetivos, preguntas de investigación e indicadores bibliométricos

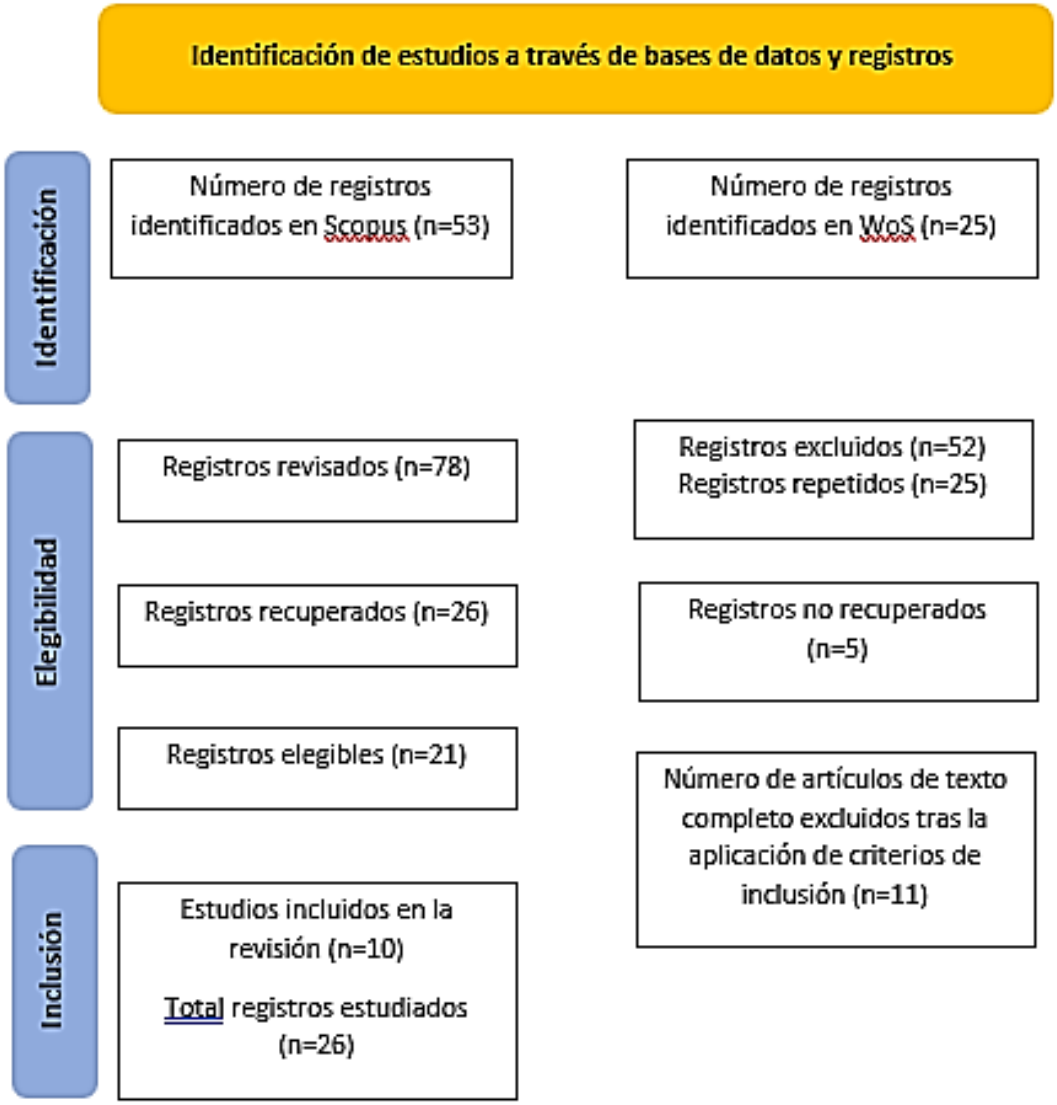
Objetivo	Pregunta	Indicador
Evolución del área y su productividad (A)	¿Cuándo se fecha el origen de la investigación acerca de la seguridad digital en la Educación Superior? ¿Cómo ha evolucionado esta tendencia investigativa a lo largo del tiempo?	A1. Producción científica a través del tiempo
Características de las revistas y dispersión de la producción científica (B)	¿Cuáles son las principales revistas que publican sobre la influencia y la enseñanza de la seguridad digital en la etapa de Educación Superior?	B1. Documentos más citados B2. Diagrama de dispersión científica
Productividad del autor e instituciones más prolíficas (C)	¿Quiénes son los autores más prolíficos?	C1. Autores más productivos
Temáticas más investigadas dentro de la muestra (D)	¿Qué temáticas son las más relevantes entro de la seguridad digital en la etapa de Educación Superior? ¿Cuáles son las palabras clave y la conexión entre	D1. Corrientes de investigación D2. Mapa de descriptores

	ellas en los distintos artículos científicos?	

Fig. 1: Diagrama de flujo

RESULTADOS

Es en esta sección donde se van a exponer los principales resultados de la literatura científica que se han generado tras la búsqueda anteriormente indicada. Estos están divididos en diferentes subsecciones, las cuales hacen referencia a los distintos indicadores y sus



correspondientes elementos tenidos en cuenta para analizar la producción científica de la temática aquí tratada.

Indicadores de Literatura

A continuación, se exponen los indicadores de la literatura que se han tenido en cuenta dentro de la temática que se trata.

Producción Científica a Través del Tiempo

En la figura que aquí se expone (figura 2), se puede observar el número de publicaciones (eje vertical) y su desarrollo a lo largo de los años (eje horizontal) desde que empezó a publicarse sobre la temática y hasta la actualidad. La producción científica sobre seguridad digital en estudiantes de educación ha experimentado un crecimiento sostenido durante las últimas dos décadas, con un mayor interés y atención en los últimos años. Los datos indican que en los últimos tres años (2020-2022), se han publicado 81 documentos, lo que representa más de la mitad de la producción total de los últimos 24 años. Este aumento podría deberse a la creciente preocupación por la seguridad digital en el entorno educativo y al aumento de la utilización de tecnologías digitales en la educación. Además, los datos sugieren que la investigación sobre este tema ha experimentado altibajos en los últimos años, con un pico en el año 2022 y una caída en el número de publicaciones en 2019. En general, la tendencia es positiva, lo que indica que la investigación sobre seguridad digital en estudiantes de educación sigue siendo un tema relevante y en constante evolución en la comunidad científica.

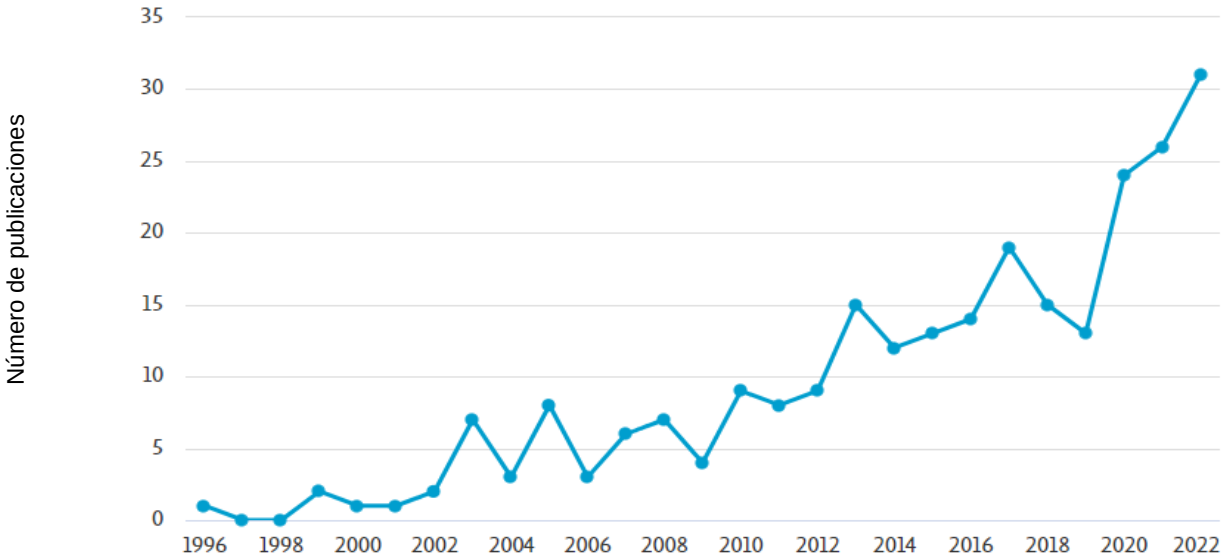


Fig. 2: Producción científica a través del tiempo

Del mismo modo, se ha querido analizar la dispersión de estas publicaciones en la literatura científica, es decir, cómo se concentran los registros o artículos (eje vertical) con respecto a las revistas científicas (eje horizontal). Así, se puede observar (figura 3) cómo son muy pocas las publicaciones, en concreto dos, aquellas que engloban prácticamente la totalidad de los

artículos sobre esta temática, mientras que existen muchas publicaciones que tienen solamente una o dos publicaciones sobre la temática.

Fig. 3: Diagrama de dispersión de la literatura científica

Autores más Productivos

Los autores más productivos en el campo de la seguridad digital en estudiantes de educación son principalmente investigadores de universidades de Finlandia y Estonia (Tabla 1). En primer lugar, el autor más productivo es Hartikainen H., con 3 documentos publicados, afiliado a la Universidad de Oulu, Finlandia. En segundo lugar, se encuentra Iivari N., también de la Universidad de Oulu, con otros 3 documentos publicados. En tercer lugar, el investigador Kikkas K. de la Universidad Tecnológica de Tallin, Estonia, también cuenta con 3 documentos publicados. Los siguientes dos autores más productivos también son de la misma universidad estonia: Laanpere M. y Kinnula M., con 3 publicaciones cada uno. Estos autores han demostrado una dedicación constante en la investigación del campo de la seguridad digital en estudiantes de educación, lo que sugiere un alto interés y compromiso en el desarrollo de nuevas soluciones y mejores prácticas en la materia.

Tabla 1: Autores más productivos

N°	*Autor*	*N° Documentos*
1	Hartikainen, H.	3

2	Iivari, N.	3
3	Kikkas, K.	3
4	Kinnula, M.	3
5	Laanpere, M.	3
6	Lazarinis, F.	3
7	Lorenz, B.	3
8	Moreno, M.A.	3
9	Schellens, T.	3
10	Tomczyk, Ł.	3

Documentos más citados

Los artículos más citados en el campo de la seguridad digital en estudiantes de educación son variados en su enfoque, pero todos han logrado generar un impacto significativo en la comunidad científica. El artículo más citado, con 111 citas, es "Promoting personal responsibility for internet safety" de LaRose et al., (2008), que propone un enfoque de responsabilidad personal para fomentar la seguridad en internet. En segundo lugar, se encuentra el artículo "Got phished? Internet security and human vulnerability" de Goel et al., (2017), con 106 citas, que se centra en la vulnerabilidad humana en la seguridad en línea.

El tercer artículo más citado es "Cost-sensitive online active learning with application to malicious URL detection" de Zhao y Hoy (2013), con 100 citas, que presenta un enfoque innovador de aprendizaje activo para la detección de URL maliciosas. El cuarto y quinto artículo más citados son "Older adults' knowledge of internet hazards" de Grimes et al., (2010) con 71 citas, y "The Internet Use for Health Information Seeking among Ghanaian University Students: A Cross-Sectional Study" de Asibey et al., (2017) con 50 citas. Estos artículos destacan la importancia de la educación y la concienciación en la seguridad en línea y su aplicación en contextos específicos, como la detección de URL maliciosas y la búsqueda de información de salud en línea.

Tabla 2: Documentos más citados

Artículo	*Autores*	*Año*	*Citas*
Promoting personal responsibility for internet safety	LaRose, R., Rifon, N.J., Enbody, R.	2008	111
Got phished? Internet security and human vulnerability	Goel, S., Williams, K., Dincelli, E.	2017	106
Cost-sensitive online active learning with application to malicious URL detection	Zhao, P., Hoi, S.C.H.	2013	100
Older adults' knowledge of internet hazards	Grimes, G.A., Hough, M.G., Mazur, E., Signorella, M.L.	2010	71
The Internet Use for Health Information Seeking among Ghanaian University Students: A Cross-Sectional Study	Asibey, B.O., Agyemang, S., Dankwah, A.B.	2017	50

Corrientes de investigación

La primera corriente de investigación destacada es: Riesgo Digital – Perspectivas Estudiantiles. La línea de investigación "Riesgo Digital - Perspectivas Estudiantiles" se enfoca en explorar los riesgos asociados con el uso de la tecnología en la vida estudiantil, así como las percepciones y experiencias de los estudiantes en relación con estos riesgos. Se busca identificar estrategias efectivas para prevenir y manejar los riesgos digitales en el ámbito estudiantil y promover el uso seguro y responsable de la tecnología.

En una primera investigación, El-Asam et al., (2021) analizan cómo los servicios públicos de atención infantil en Inglaterra abordan casos con riesgos digitales para niños vulnerables, revelando una conciencia limitada de estos riesgos y la necesidad de mejorar la colaboración multiagencia en tales situaciones. Seguidamente, la contextualización de correos electrónicos de phishing para grupos específicos afecta la susceptibilidad de las personas a ser engañadas; los resultados revelan que apelar a debilidades psicológicas, como el miedo a perder o la anticipación de ganar, aumenta la vulnerabilidad a estos ataques (Goel et al., 2017). Adicionalmente Harriman et al., (2020), investigan la exposición de los jóvenes a materiales

de odio en línea, identificando factores asociados como tiempo en línea, rendimiento académico, comunicación con extraños en redes sociales y desinhibición benigna en línea.

El reconocimiento de los riesgos involucra investigar las tendencias del comportamiento arriesgado del usuario y la conciencia de seguridad a lo largo de la vida. Los resultados han demostrado el crecimiento del comportamiento arriesgado en línea a lo largo de la vida y el crecimiento del conocimiento y la conciencia de seguridad en la adultez media (Velki y Romstein, 2018). Finalmente, Adorjan y Ricciardelli (2019) se enfocan en las opiniones de los estudiantes canadienses sobre los programas escolares de seguridad cibernética. Los resultados muestran apoyo a mensajes repetidos, incluyendo aquellos que evocan miedo, especialmente entre los estudiantes más jóvenes.

La presente línea de investigación aborda temas como la conciencia limitada de riesgos digitales en servicios de atención infantil, la susceptibilidad a ataques de phishing, la exposición de jóvenes a materiales de odio en línea y las tendencias en comportamiento arriesgado y conciencia de seguridad. Estos estudios destacan la importancia de mejorar la colaboración multiagencia, entender las debilidades psicológicas, e identificar factores de riesgo en el entorno digital. Además, se resalta la relevancia de los programas escolares de seguridad cibernética y la efectividad de mensajes repetidos y evocadores de miedo en la prevención de riesgos digitales.

La segunda corriente es la que aborda el concepto: Digital Children. La línea de investigación "Digital Children" se centra en explorar el impacto de la tecnología en el desarrollo cognitivo, emocional y social de los niños. Esta investigación busca entender cómo los niños interactúan con los dispositivos digitales y las redes sociales, y cómo estas interacciones pueden afectar su bienestar y su capacidad para aprender y relacionarse con otros.

Se evidencia un primer estudio que investiga la conciencia de los padres en Arabia Saudita sobre los riesgos de Internet para sus hijos y las estrategias de mediación. Los hallazgos revelan una brecha significativa entre las actividades en línea de los niños y el conocimiento de los padres, así como la falta de colaboración entre ambos para garantizar la seguridad en línea (Alqahtani et al., 2017). Al desarrollar paquetes educativos, se deben considerar objetivos y valores de niños y educadores, integrar la cultura mediática de los niños, brindar consejos concretos, mantener un tono positivo e involucrar a niños y maestros en el diseño y evaluación (Hartikainen et al., 2019). Por otra parte, aunque los niños sienten seguridad en línea, pueden carecer de conocimientos objetivos para mantenerse realmente seguros. Esto resalta la

necesidad de evaluar y educar a los niños en seguridad en línea (Macaulay et al., 2020). En la presente línea de investigación "Digital Children", se destaca la importancia de comprender las percepciones y conocimientos de los padres y los niños sobre los riesgos en línea y las medidas de seguridad necesarias.

La tercera corriente destaca aúna los siguientes conceptos: Jóvenes Digitales y Ciberacoso. La línea de investigación "Jóvenes Digitales y Ciberacoso" se enfoca en estudiar cómo la tecnología afecta la identidad, la comunicación y las relaciones sociales de los jóvenes en la actualidad. Esta investigación busca entender cómo los jóvenes utilizan las redes sociales y otras plataformas digitales para construir y expresar su identidad, así como para interactuar con otros jóvenes y con la sociedad en general.

Se explora el fenómeno del ciberacoso entre estudiantes universitarios, revelando la falta de consenso sobre su definición, preocupaciones al traducir definiciones de acoso tradicional y manifestaciones distintas en comparación con adolescentes más jóvenes (Moreno et al., 2014). Por otra parte, se exploran las sugerencias de estudiantes para prevenir el ciberacoso, destacando la importancia de aumentar la seguridad en línea y la conciencia de su entorno digital. Se sugieren estrategias como capacitación para adultos, intervenciones enfocadas en comportamiento y mejorar la seguridad en línea. (Parris et al., 2014).

En conclusión, la línea de investigación "Jóvenes Digitales y Ciberacoso" aborda aspectos clave en relación con el impacto de la tecnología en la vida de los jóvenes y cómo estos interactúan en el entorno digital. Hemos analizado la falta de consenso en la definición de ciberacoso y las diferencias en su manifestación en distintos grupos etarios. Además, se han identificado estrategias de prevención del ciberacoso, incluida la capacitación para adultos y la promoción de la seguridad en línea y la conciencia de los jóvenes sobre su entorno digital. A través de esta investigación, se busca generar conciencia y comprensión sobre el ciberacoso y sus implicaciones en la vida de los jóvenes, así como proporcionar herramientas y estrategias efectivas para enfrentar y prevenir este problema en constante evolución.

La última corriente es: Comportamiento Digital. La línea de investigación "Comportamiento Digital" se enfoca en analizar cómo las personas se comportan en línea y cómo estos comportamientos afectan su vida y la sociedad en general. Esta investigación busca comprender cómo las personas interactúan en el mundo digital, cómo toman decisiones y cómo se relacionan entre sí. También se examina cómo las plataformas digitales y los algoritmos influyen en el comportamiento humano y en la toma de decisiones.

Se analiza la investigación basada en la Teoría de la Motivación de Protección (PMT) para examinar el papel de la responsabilidad personal en el comportamiento protector en línea de estudiantes universitarios (Boehmer et al., 2015). Los resultados sugieren que la responsabilidad personal influye en el comportamiento seguro en línea y puede ser impulsada a través de intervenciones dirigidas (Boehmer et al., 2015).

Adicionalmente se encuentra, la investigación realizada por Chou y Chou (2016) la cual se centra en las percepciones de los maestros sobre su propio comportamiento de seguridad de la información y cómo estos factores, basados en la Teoría de la Motivación de Protección, influyen en su conducta. Al entender las intenciones de comportamiento y la motivación de protección, se pueden diseñar programas de capacitación para mejorar la seguridad de la información tanto en maestros como en estudiantes. Finalmente, Chou y Sun (2017) investigan las motivaciones del comportamiento en línea riesgoso de maestros en servicio y examina el papel moderador del género y las normas sociales basándose en la Teoría de la Motivación de Protección. Se concluye que es necesario, pero no suficiente, mejorar las habilidades de los maestros para enfrentar problemas de seguridad en línea y crear un ambiente que fomente medidas de protección.

En resumen, la línea de investigación "Comportamiento Digital" aborda diversos aspectos del comportamiento humano en línea y cómo estos afectan a la vida y la sociedad. La Teoría de la Motivación de Protección ha demostrado ser útil para entender y mejorar el comportamiento seguro en línea en diferentes contextos, como estudiantes universitarios y maestros en servicio. Los estudios mencionados sugieren que es fundamental desarrollar intervenciones y programas de capacitación para impulsar la responsabilidad personal, la conciencia sobre la seguridad en línea y las habilidades de afrontamiento. Además, se debe tener en cuenta el papel moderador de factores como el género y las normas sociales al diseñar estrategias de prevención y educación en seguridad digital. Estos hallazgos ofrecen una base sólida para futuras investigaciones y el desarrollo de intervenciones eficaces en la promoción de un comportamiento digital responsable y seguro.

Mapa bibliométrico

Por último, se expone un mapa bibliométrico o mapa de descriptores. En este mapa (figura 4) se exponen las conexiones existentes entre las diferentes palabras clave de los diferentes documentos en esta área. Esta figura está compuesta por redes que, a su vez, están compuestas por nodos. El software empleado para esto ha sido VOSviewer, a través del cual se ha creado un mapa de redes donde los nodos de mayor tamaño indican que esa palabra clave es utilizada en más ocasiones que las que aparecen con un tamaño menor. De igual modo, los colores indican los diferentes grupos que se conectan entre sí. Partiendo de todo esto, las palabras clave más empleadas y que destacan son "internet security", "education", "online safety" y "human".

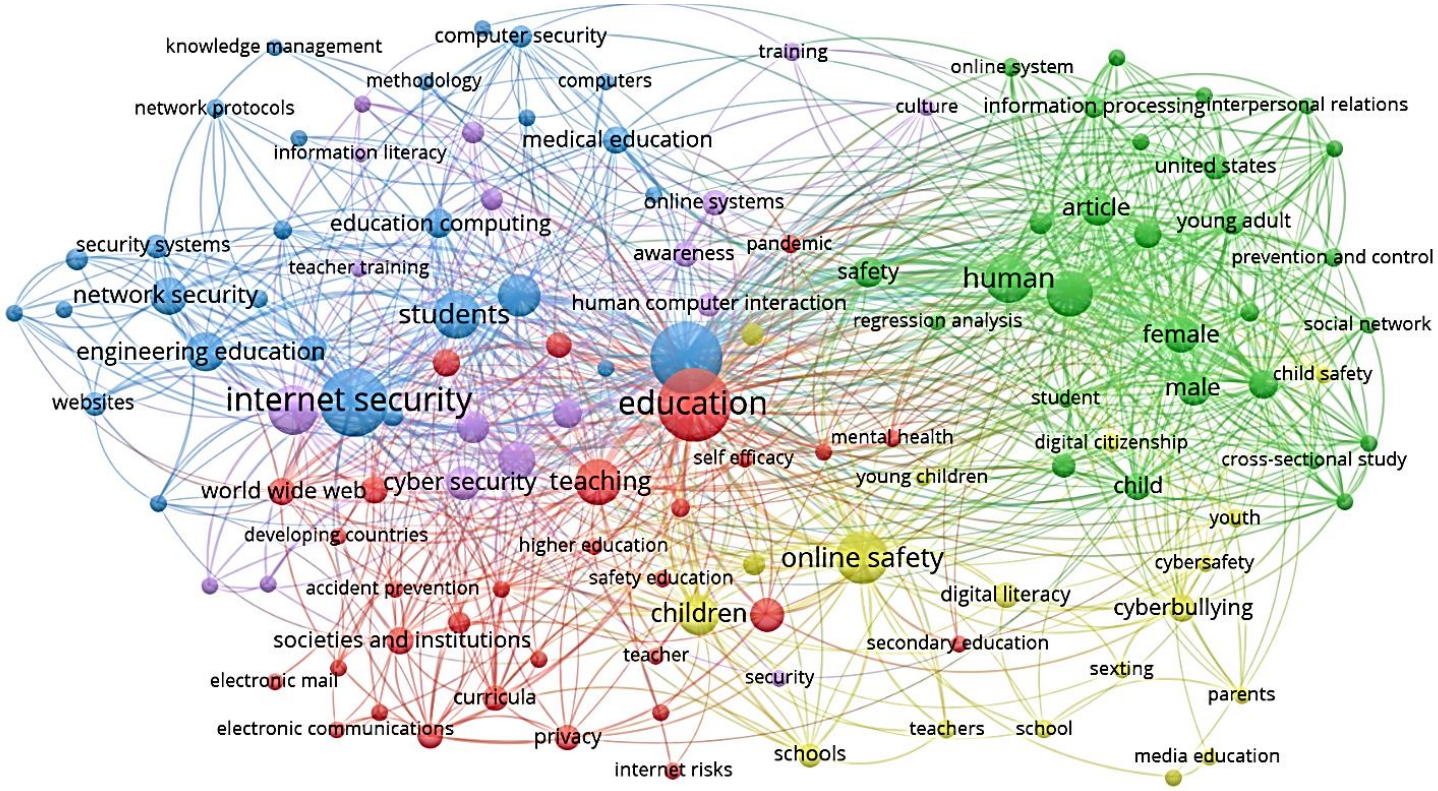


Fig. 4: Mapa de descriptores

DISCUSIÓN

En los resultados se han mostrado los datos que se han obtenido a través de los objetivos planteados en esta investigación. De este modo, el presente estudio sobre seguridad digital en estudiantes de Educación Superior ha mostrado un crecimiento sostenido en las últimas dos décadas, con un aumento significativo en los últimos años.

Los autores más productivos provienen principalmente de universidades de Finlandia y Estonia, y los artículos más citados en el campo abordan temas como la responsabilidad personal en la seguridad en línea, la vulnerabilidad humana, la detección de URL maliciosas y la búsqueda de información de salud en línea, como bien ya exponían Boehmer et al., (2015),

Goel et al., (2017), Macauly et al., (2020) y Asibey et al., (2017), respectivamente. Estos hallazgos resaltan la relevancia y evolución constante de la seguridad digital en esta etapa, así como el interés y compromiso de los investigadores en el desarrollo de soluciones y mejores prácticas en este ámbito, siguiendo así lo expuesto por Guaña-Moya (2023).

A lo largo de la investigación, se identificaron diversas corrientes de investigación relevantes en el ámbito de la seguridad digital en la Educación Superior. Entre estas corrientes se encuentran: (1) "Riesgo Digital, Perspectivas Estudiantiles", que aborda los riesgos y amenazas a los que se enfrentan los estudiantes en el entorno digital y cómo perciben y gestionan estos desafíos, esta corriente concuerda con lo investigado por Alqahtani et al., (2017), El-Asam et al., (2021) y Hartikainen et al., (2019).

La siguiente corriente es (2) "Digital Children", que se centra en el estudio de los niños y jóvenes que crecen en un mundo cada vez más digitalizado, y cómo se ven afectados por la tecnología en su vida cotidiana y educación. Por un lado, sobre esta corriente se pueden encontrar publicaciones que exponen los aspectos positivos de este impacto de la digitalización en la vida de los estudiantes, como los estudios de Castillejos et al., (2016) y Hartikainen et al., (2019); mientras que, por otro lado, son muchas las publicaciones (Dávila-Morán et al., 2022; Harriman et al., 2020; Macaulay et al., 2020; Parris et al., 2014) que exponen los aspectos negativos de esta inclusión de la tecnología en la vida diaria de los discentes.

Por último, la corriente (3) "Jóvenes Digitales y ciberacoso", que examina el papel de los jóvenes en la era digital, así como sus habilidades, oportunidades y desafíos en el uso de tecnologías digitales, a este respecto son muchas las investigaciones, como la de Adorjan et al., (2019), que exponen el ciberacoso como una de las grandes problemáticas derivadas del amplio uso de la tecnología por parte de los jóvenes sumado a una falta de formación en seguridad digital; y (4) "Comportamiento Digital", que investiga las actitudes, comportamientos y prácticas de los individuos en relación con la utilización de tecnologías digitales y su impacto en la seguridad en línea, pues dependiendo de factores como la edad de los usuarios (Asibey et al., 2017) o el sexo (Moreno et al., 2014) los comportamientos y modos de empleo que se le da tanto a la seguridad digital como a la competencia digital en general difieren sustancialmente.

Estas corrientes de investigación proporcionan una base sólida para comprender y abordar la problemática de la seguridad digital en Educación Superior, y destacan la importancia de considerar las múltiples dimensiones y perspectivas involucradas en este fenómeno.

CONCLUSIONES

En síntesis, la revisión sistemática de la literatura sobre la seguridad digital en estudiantes de educación superior ha permitido identificar y analizar las principales corrientes de investigación y temas abordados en este campo. El crecimiento sostenido en la producción científica y la diversidad de enfoques demuestran la relevancia y evolución constante de la seguridad digital en el ámbito educativo. Sin embargo, esta investigación presenta algunas limitaciones, como la restricción de las bases de datos consultadas y el enfoque en la producción científica en inglés, lo que podría excluir investigaciones relevantes en otros idiomas.

En cuanto a futuras investigaciones, es necesario profundizar en el estudio de las habilidades y competencias digitales de los estudiantes de educación superior, así como en la evaluación de la efectividad de las estrategias y programas de prevención y protección implementados por las instituciones educativas. Además, sería de gran interés investigar cómo la adaptación a nuevos contextos y desafíos, como el aprendizaje a distancia y el trabajo en línea, afecta la seguridad digital de los estudiantes y sus prácticas en línea. También sería relevante analizar las diferencias culturales y contextuales en la percepción y abordaje de la seguridad digital en la educación superior, incluyendo la perspectiva de estudiantes y docentes de distintas regiones y entornos socioeconómicos. Esta investigación deberá continuar evolucionando para adaptarse a los constantes cambios tecnológicos y a las necesidades de los estudiantes en el entorno educativo digital.

La seguridad digital es un tema de gran importancia en la sociedad actual, especialmente en el contexto de la educación superior, donde los estudiantes están expuestos a diversos riesgos en línea. La revisión sistemática de la literatura sobre seguridad digital en estudiantes de educación superior tiene como objetivo examinar la investigación previa en este campo y destacar los hallazgos clave, las brechas en el conocimiento y las direcciones futuras para la investigación. Al llevar a cabo esta revisión sistemática, se logra una mejor comprensión de los riesgos en línea a los que se enfrentan los estudiantes de educación superior, así como de las mejores prácticas y estrategias para abordar estos riesgos. La revisión sistemática de la literatura también es importante porque ayuda a los investigadores a identificar los temas y problemas críticos en el campo de la seguridad digital en estudiantes de Educación Superior.

REFERENCIAS

Adorjan, M., y Ricciardelli, R. Student perspectives towards school responses to cyber-risk and safety: the presumption of the prudent digital citizen, https://doi.org/10.1080/17439884.2019.1583671, Lear. Media Tech., 44(4), 430-442 (2019)

Asibey, B. O, Agyemang, S., y Boakye Dankwah, A. The Internet use for health information seeking among Ghanaian university students: A cross-sectional study, https://doi.org/10.1155/2017/1756473, Int. J. Telemedicine Appl., 2017, 1-7 (2017)

Alqahtani, N., Furnell, S., Atkinson, S., y Stengel, I. (2017). Parents' perceptions and attitudes: An investigative study of the Saudi Context. In 2017 Internet Technologies and Applications (ITA) (pp. 98-103). IEEE.

Anderson, J. M. Why we need a new definition of information security, https://doi.org/10.1016/S0167-4048(03)00407-3 Comp. Sec., 22(4), 308–313 (2003)

Björk, G., Hernández, H., Colomer, J., y Hatlevik, H. Student teachers' responsible use of ICT: Examining two samples in Spain and Norway, https://doi.org/10.1016/j.compedu.2020.103877, Comp. Educ., 152, (2020)

Boehmer, J., LaRose, R. y otros tres autores, Determinants of online safety behavior: Towards an intervention strategy for college students, https://doi.org/10.1080/0144929X.2015.1028448, Behav. Inf. Tech., 34(10), 1022-1035 (2015)

Castillejos, B., Torres, C.A., y Lagunes, A. Safety in the digital skills of millennials, https://doi.org/10.32870/Ap.v8n2.914, Apertura, 8(2), 54–69 (2016)

Çebi, A., y Reisoğlu, İ. Digital competence: A study from the perspective of pre-service teachers in Turkey, https://doi.org/10.7821/naer.2020.7.583, J. New Approaches Educ. Res., 9(2), 294–308 (2020)

Chou, H. L., y Chou, C. An analysis of multiple factors relating to teachers' problematic information security behavior, https://doi.org/10.1016/j.chb.2016.08.034, Comp. Hum. Behav., 65, 334-345 (2016)

Cózar, R., y Roblizo, M. Digital skill in would-be teachers: Perceptions from the teacher training degree students, https://doi.org/10.17398/1695-288X.13.2.119, Rev. Lat. Tec. Ed., 13(2), 119–133 (2014)

Cruz, M., Bibliometría y Ciencias Sociales, Clío: History and History Teaching, 7, 1-10 (1999)

Dávila Morán, R. C., Zuta Arriola, N., Espinoza Camus, F. C., y Chávez-Díaz, J. M. Educación remota y estrés académico en estudiantes universitarios peruanos en tiempos de pandemia del covid-19, Rev. Univ. Soc.,14(3), 775-783 (2022)

Del Carpio Hurtado, D. I., y Gilvonio Herrera, H. I. Los principales factores que influyen en el uso del e-commerce en las Mypes del sector textil - confecciones en el emporio de Gamarra en el periodo del 2013 al 2018. Universidad Peruana de Ciencias Aplicadas (UPC)., Lima, Perú. https://doi.org/10.19083/tesis/626108 (2019)

El-Asam, A., Katz, A., Street, C., Nazar, N. M., y Livanou, M. Children's services for the digital age: A qualitative study into current procedures and online risks among service users, https://doi.org/10.1016/j.childyouth.2020.105872, Children Youth Services Rev., 122, 105872 (2021)

Fernández-Cano, A., y Bueno-Sánchez, A., Síntesis de estudios bibliométricos españoles en educación. una dimensión evaluativa, Rev. Esp. Doc. Cient., 21(3), 269-285 (1998)

Goel, S., Williams, K., y Dincelli, E. Got phished? Internet security and human vulnerability, https://doi.org/10.17705/1jais.00447, J. Assoc. Inf. Syst., 18(1), 2 (2017)

Grimes, G. A., Hough, M. G., Mazur, E., y Signorella, M. L. Older adults' knowledge of internet hazards, Educ. Gerontology, 36(3), 173-192 (2010)

Guaña-Moya, J. La importancia de la seguridad informática en la educación digital: retos y soluciones, RECIMUNDO: Rev. Cient. Inv. Conoc., https://doi.org/10.26820/recimundo/7.(1).enero.2023.609-616, 7(1), 609-616 (2023)

Gutiérrez Oscco, E., y Luján Coronel, R. S. *Valoración del incumplimiento de obligaciones comerciales en un sector económico emergente* (tesis). Universidad Peruana Unión, Lima. (2022)

Harriman, N., Shortland, N. y otros cuatro autores, Youth exposure to hate in the online space: an exploratory analysis, https://doi.org/10.3390/ijerph17228531, Int. J. Env. Res. Pub. Health, 17(22), 8531 (2020)

Hartikainen, H., Iivari, N., y Kinnula, M. Children's design recommendations for online safety education, https://doi.org/10.1016/j.ijcci.2019.100146, Int. J. Child-Comp. Inter. 22, 100146 (2019)

Kota, R., Schoohs, S., Benson, M., y Moreno, M. A. Characterizing cyberbullying among college students: Hacking, dirty laundry, and mocking, https://doi.org/10.3390/soc4040549, Soc., 4(4), 549-560 (2014)

LaRose, R., Rifon, N. J., y Enbody, R. Promoting personal responsibility for internet safety, http://doi.acm.org/10.1145/1325555.1325569, Communications of the ACM, 51(3), 71-76 (2008)

Macaulay, P. J., Boulton, M. J., y otros siete autores, Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom, https://doi.org/10.1080/17482798.2019.1697716, J. Child. Med., 14(3), 376-395 (2020)

Moreno, M. A., Kelleher, E., Ameenuddin, N., y Rastogi, S. Young adult females' views regarding online privacy protection at two time points, https://doi.org/10.1016/j.jadohealth.2014.03.005, J. Adolescent Health, 55(3), 347-351 (2014)

Parris, L. N., Varjas, K., y Meyers, J. "The Internet is a Mask": High School Students' Suggestions for Preventing Cyberbullying, https://doi.org/10.5811/westjem.2014.4.20725, Western J. Emergency Med., 15(5), 587 (2014)

Rodríguez Orejuela, A., Osorio Andrade, C. F., y Peláez Muñoz, J. Dos décadas de investigación en electronic word-of-mouth: un análisis bibliométrico, Pensamiento & Gestión, 48, 251-275 (2020)

Velki, T., y Romstein, K. User risky behavior and security awareness through lifespan, https://doi.org/10.32985/ijeces.9.2.2, Int. J. Electr. Comp. Eng. Syst., 9(2), 53-60 (2018)

Zhao, P., y Hoi, S. C. Cost-sensitive online active learning with application to malicious URL detection. In Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 919-927). (2013)

5.4.Cuarta publicación

Metaanálisis sobre la Seguridad Digital en estudiantes de Educación Superior

Este artículo ha sido publicado en la revista *Píxel-Bit: Revista de medios y formación* (ISSN: 1133- 8482). Esta revista tiene como objetivo servir de plataforma para el intercambio de ideas,

experiencias e investigaciones sobre la aplicación de las TIC, sea cual sea su contexto (formal, no formal e informal) y en cualquier nivel educativo.

Esta revista está presente entre los principales indicadores de calidad nacionales e internacionales más conocidos y mejor valorados por los organismos de evaluación de la actividad investigadora.

Se encuentra en el cuartil Q1 de educación 2022, SJR **0.63**. Encontrándose En la posición 163 de 1469.

La revista se encuentra indexada en las siguientes bases de datos: Emerging Sources Citation Index, Journal Citation Indicator, Ranking FECYT, Dialnet, Ranking REDIB, Google Scholar, CIRC, MIAR, ERIHPLUS, Journal Scholar Metric, CARHUS PLUS+, INDEX COPERNICUS, DICE.

Referencia bibliográfica:

Rodríguez-Jiménez, C., Trujillo-Torres, J.M., Alonso-García, S., y Martínez-Domingo, J.A. (2025). Metaanálisis sobre la Seguridad Digital en Estudiantes de Educación Superior [Metaanalysis on Digital Safety in Higher Education Students]. *Pixel-Bit. Revista de Medios y Educación, 72*, En Prensa.

Metaanálisis sobre la Seguridad Digital en Estudiantes de Educación Superior

Metaanalysis on Digital Safety in Higher Education Students

Carmen Rodríguez Jiménez[1], Juan Manuel Trujillo Torres[2], Santiago Alonso García[2], José Antonio Martínez Domingo[2]

[1]Universidad de Granada. Facultad de Ciencias de la Educación y del Deporte. Melilla.

[2]Universidad de Granada. Facultad de Ciencias de la Educación. Granada.

RESUMEN

La presente investigación parte de la importancia de la seguridad en línea y la alfabetización digital. Esta se fundamenta en estudios previos que analizan aspectos como la seguridad en sistemas de billetera digital, la exposición de jóvenes a riesgos en línea, la alfabetización digital

de futuros profesores y la necesidad de capacitación en seguridad digital para profesores universitarios. Además, se investigó la relación entre la exposición a materiales de odio en línea y la autoeficacia de los padres en el manejo del uso de Internet de sus hijos adolescentes. Este meta-análisis sobre seguridad digital en estudiantes de Educación Superior resalta la relevancia de la seguridad en línea y la alfabetización digital en diversos contextos. Los resultados sugieren la necesidad de desarrollar estrategias y programas de capacitación en seguridad digital para profesores y estudiantes, así como promover la conciencia de los riesgos en línea y el manejo parental del uso de Internet.

ABSTRACT

This research is based on the importance of online safety and digital literacy. It builds on previous studies looking at issues such as security in digital wallet systems, exposure of young people to online risks, digital literacy of future teachers and the need for digital safety training for university teachers. In addition, the relationship between exposure to online hate materials and parents' self-efficacy in managing their teenagers' Internet use was investigated. This meta-analysis on digital safety in higher education students highlights the relevance of online safety and digital literacy in various contexts. The results suggest the need to develop strategies and training programmes on digital safety for teachers and students, as well as to promote awareness of online risks and parental management of internet use.

PALABRAS CLAVES · KEYWORDS

Protección de datos; Alfabetización digital; Educación Superior; Análisis Dodumental; Análisis de Datos

Data Protection; Digital Literacy; Higher Education; Data Analysis; Document Analysis;

1. Introducción

En la era digital actual, el acceso a la información y las comunicaciones en línea se ha vuelto fundamental para la vida cotidiana. Con el creciente uso de dispositivos electrónicos y la proliferación de plataformas de redes sociales, la importancia de garantizar la seguridad digital no puede ser subestimada. La Educación Superior es un ámbito particularmente relevante para abordar este tema (Sayaf, et al., 2021), ya que los estudiantes universitarios están cada vez más expuestos a riesgos en línea y dependen de la tecnología para sus estudios e interacciones

sociales (Gümüş, et al., 2023). Es necesario un enfoque sistemático y riguroso para comprender la magnitud del problema y las posibles soluciones. Por lo tanto, la presente investigación titulada "Metaanálisis sobre la seguridad digital en estudiantes de Educación Superior" tiene como objetivo evaluar la literatura existente y obtener información valiosa sobre cómo se puede mejorar la seguridad digital en este grupo demográfico.

La seguridad digital es una preocupación creciente en todo el mundo debido al aumento de la ciberdelincuencia, el robo de identidad, el acoso en línea y otros riesgos asociados con el uso de Internet. Los estudiantes universitarios son particularmente vulnerables a estos riesgos, ya que a menudo carecen de la formación y conciencia adecuadas sobre cómo protegerse en línea (Gómez Galán, et al., 2020). Además, las instituciones de Educación Superior suelen ser blanco de ataques cibernéticos, lo que aumenta la importancia de abordar esta problemática en el ámbito académico. El propósito de este metaanálisis es examinar los resultados de estudios previos sobre la seguridad digital en estudiantes universitarios y proporcionar una evaluación exhaustiva y objetiva de la evidencia disponible.

Un metaanálisis es una herramienta estadística poderosa que permite combinar y analizar los resultados de varios estudios para obtener una visión más precisa y confiable de un fenómeno (Botella & Zamora, 2017). Al considerar múltiples investigaciones y analizar de manera conjunta sus resultados, un metaanálisis puede revelar patrones y tendencias que no serían evidentes al examinar cada estudio de forma individual. Además, al cuantificar y evaluar la heterogeneidad entre los estudios, este enfoque puede proporcionar información valiosa sobre las variables que pueden influir en la relación entre la Educación Superior y la seguridad digital. En última instancia, el metaanálisis puede ayudar a los investigadores, educadores y formuladores de políticas a tomar decisiones informadas sobre cómo abordar el tema de la seguridad digital en el contexto de la Educación Superior.

El presente metaanálisis se centrará en estudios que investiguen la seguridad digital en estudiantes universitarios, incluyendo temas como la conciencia sobre ciberseguridad, el comportamiento en línea seguro, la capacitación en seguridad digital y las políticas y prácticas institucionales relacionadas. Además, se explorarán las diferencias entre grupos demográficos, como género, edad y disciplina académica, para identificar posibles áreas de vulnerabilidad y oportunidades de intervención. Al realizar este metaanálisis, se espera contribuir significativamente al conocimiento y la comprensión de la seguridad digital en estudiantes de Educación Superior, lo que permitirá a las instituciones académicas, a los educadores y a los

propios estudiantes tomar medidas adecuadas para garantizar la seguridad en línea y minimizar los riesgos asociados al uso de la tecnología.

En el ámbito educativo, la seguridad digital es de suma importancia, ya que los estudiantes de Educación Superior a menudo manejan información confidencial y utilizan tecnologías avanzadas para comunicarse, investigar y completar sus estudios. Por lo tanto, es crucial que los estudiantes y docentes estén capacitados adecuadamente en el uso responsable y seguro de las tecnologías digitales, así como en la identificación y prevención de riesgos en línea. Además, la creciente prevalencia de la educación en línea y a distancia en los últimos años ha incrementado la necesidad de garantizar que tanto los estudiantes como los profesores estén protegidos en entornos digitales (Vázquez-Cano & Pascual-Moscoso, 2022).

Por otro lado, la adaptación a la era digital también ha generado nuevos desafíos en el ámbito de la Educación Superior, como el ciberacoso, la suplantación de identidad, el acceso no autorizado a información confidencial y el robo de propiedad intelectual. Estos riesgos pueden tener consecuencias negativas tanto para los estudiantes como para las instituciones educativas, lo que destaca la importancia de implementar políticas y estrategias efectivas de seguridad digital en el entorno académico (Hernández-Serrano, et al., 2021; Ojeda Pérez, & Rey Alamillo, 2021). Asimismo, es fundamental fomentar la educación y concienciación sobre estos temas para empoderar a los individuos en la protección de su privacidad y seguridad en línea (Gkioulos, et al., 2017).

Finalmente, en el contexto de la Educación Superior, es esencial abordar la brecha en habilidades digitales y competencias entre estudiantes y profesores. Un enfoque integral que combine la enseñanza de habilidades técnicas, la promoción de la conciencia sobre riesgos en línea y el fomento de la responsabilidad y ética digital puede resultar beneficioso para mejorar la seguridad digital en el entorno educativo. En este sentido, los resultados de estudios previos pueden proporcionar información valiosa sobre las áreas en las que se deben enfocar los esfuerzos para garantizar un entorno digital seguro y protegido para todos los involucrados en la Educación Superior.

En este trabajo, por tanto, se aborda esta problemática desde una perspectiva metodológica de metaanálisis. Esta permite determinar el efecto global y particular de todas las investigaciones analizadas a este respecto. La justificación de la importancia y relevancia de este trabajo se muestra a través de las siguientes preguntas de investigación que conducen el mismo:

- ¿Tienen los estudiantes de Educación Superior un correcto nivel de seguridad digital?

- ¿Se implementa la seguridad digital como contenido a trabajar en la etapa de Educación Superior?

- ¿Se publican mayoritariamente artículos con resultados positivos sobre la relevancia de la seguridad digital en Educación Superior?

2. Metodología

La metodología empleada en esta investigación se centra en el análisis de correlación para examinar la relación entre dos variables de interés. En primer lugar, se seleccionaron ocho estudios relevantes (k = 8) para ser incluidos en el análisis. A continuación, se extrajeron los coeficientes de correlación (r, N) y otros datos relevantes de cada uno de los estudios. Para homogeneizar los coeficientes de correlación y facilitar su comparación, se aplicó la transformación de Fisher r-to-z a los coeficientes de correlación de cada estudio.

Posteriormente, se implementó un modelo de efectos aleatorios en los datos transformados con el objetivo de obtener una estimación más precisa de la relación entre las variables, considerando las diferencias entre los estudios. Además, se calculó la heterogeneidad entre los estudios mediante el uso del estimador Tau* de máxima verosimilitud restringida y otras estadísticas relevantes (Tau, F, H, R, df, Q y P). A fin de evaluar la significancia de la correlación obtenida, se analizaron el valor Z, el intervalo de confianza (CI) y el valor p.

En el siguiente paso del proceso metodológico, se examinaron los residuos estudentizados y las distancias de Cook para identificar estudios atípicos o influyentes que pudieran afectar los resultados del análisis. Además, se evaluó la asimetría del gráfico de embudo mediante la realización de la prueba de correlación de rangos y la prueba de regresión, utilizando el error estándar de los resultados observados como predictor. Finalmente, los resultados del análisis de correlación se presentaron de manera gráfica mediante un diagrama de bosque y un gráfico de embudo, facilitando su interpretación. De manera más esquemática, a continuación, se exponen los pasos seguidos para el proceso metodológico del presente estudio:

1. Selección de estudios: Seleccionar un total de 8 estudios relevantes (k = 8) para el análisis de correlación.

2. Extracción de datos: Extraer los coeficientes de correlación (r, N) y otros datos relevantes de cada estudio.

3. Conversión de coeficientes de correlación: Transformar los coeficientes de correlación de cada estudio utilizando la transformación de Fisher r-to-z.

4. Modelo de efectos aleatorios: Aplicar un modelo de efectos aleatorios a los datos para obtener una estimación más precisa de la relación entre las variables, teniendo en cuenta las diferencias entre los estudios.

5. Estimación de heterogeneidad: Calcular la heterogeneidad entre los estudios utilizando el estimador Tau* de máxima verosimilitud restringida y otras estadísticas (Tau, F, H, R, df, Q y P).

6. Evaluación de la significancia: Analizar el valor Z, el intervalo de confianza (CI) y el valor p para determinar la significancia de la correlación.

7. Análisis de atipicidad e influencia: Examinar los residuos estudiantizados y las distancias de Cook para identificar estudios atípicos o influyentes.

8. Evaluación de la asimetría del gráfico de embudo: Realizar la prueba de correlación de rangos y la prueba de regresión utilizando el error estándar de los resultados observados como predictor para verificar la asimetría del gráfico de embudo.

9. Presentación de resultados: Presentar los resultados del análisis en un diagrama de bosque y un gráfico de embudo.

10. Interpretación de resultados: Analizar e interpretar los resultados obtenidos en función de los coeficientes de correlación estimados, la heterogeneidad entre los estudios, la significancia y la presencia de estudios atípicos o influyentes.

2.1. Selección de artículos

La ecuación de búsqueda presentada se centra en la identificación de investigaciones y estudios relacionados con la ciberseguridad, la seguridad en línea y la seguridad en internet, específicamente en el contexto de la Educación Superior.

Las bases de datos seleccionadas para la búsqueda, filtrado y obtención de resultados y la muestra final son Scopus y Web of Science. Del mismo modo, los términos o palabras clave han sido obtenidas del tesauro de ERIC. Sin embargo, no todos los términos han sido extraídos de ahí. Las palabras clave referentes a la seguridad digital (cibersecurity, online safety, internet security, etc.) no aparecen como keywords ni en ese tesauro ni en el tesauro de la UNESCO, tesauros de referencia en el ámbito de la investigación. Esto puede deberse a la juventud de los

términos y de la temática de investigación. Aun así, se ha decidido emplearlos pues su uso se justifica por el simple hecho de la gran cantidad de estudios e investigaciones de relevancia que los emplean en las bases de datos.

Las ecuaciones utilizadas emplean una combinación de términos clave en los campos de título, resumen y palabras clave (TITLE-ABS-KEY) para garantizar una búsqueda exhaustiva y precisa de la literatura relevante. Los términos "cibersecurity", "online safety" e "internet security" se buscan de manera independiente, pero también se combinan con términos relacionados con el ámbito educativo, como "higher education", "college" y "university", utilizando el operador booleano "AND" para refinar la búsqueda. De esta manera, la ecuación de búsqueda permite identificar estudios y trabajos de investigación que aborden temas relacionados con la seguridad digital en entornos educativos, en concreto la etapa de Educación Superior, brindando una visión amplia y detallada de las tendencias, desafíos y soluciones existentes en el ámbito de la seguridad en línea en el contexto ya mencionado.

A continuación, se exponen (Tabla 1) los criterios de inclusión y exclusión elegidos para refinar los resultados una vez empleadas las palabras clave en las bases de datos.

Tabla 1. Criterios de inclusión y exclusión

Criterios de inclusión	**Criterios de exclusión**
Producción desde su origen al año 2022	Producción del año 2023 al tratarse de un año no finalizado
Artículos de revista	Capítulos de libro, libros, comunicaciones a congresos, etc.
Estudios empíricos	Estudios o revisiones teóricas
Artículos escritos en inglés o español	Artículos no escritos en inglés o español
Investigaciones y experiencias que aborden cómo se trabaja la seguridad digital con los estudiantes de Educación Superior	Investigaciones y experiencias que no aborden la seguridad digital en Educación Superior o que lo hagan con otros agentes implicados en el proceso de E-A (docentes, familias, etc.)

2.2. Documentos de la literatura seleccionados

En la era actual de la tecnología y las redes sociales, la seguridad digital es fundamental, especialmente en relación con los sistemas de billetera digital. Un estudio realizado por Muhtasim et al. (2022) buscó determinar un marco eficiente que aborde la seguridad y la satisfacción del consumidor en estos sistemas. Los resultados sugieren que la seguridad financiera, la privacidad, la seguridad del sistema, el cibercrimen y la confianza influyen en la intención de compra en línea. Este estudio puede ayudar a los proveedores de billeteras digitales a comprender la perspectiva del cliente sobre la seguridad y, por lo tanto, a implementar regulaciones adecuadas que atraigan a los clientes a utilizar estos servicios.

Paralelamente, los jóvenes de hoy tienen un acceso sin precedentes a la información en línea, tanto positiva como negativa. Un estudio realizado por Savoia et al. (2021) examinó cómo los adolescentes usan internet y su susceptibilidad a la exposición a riesgos en línea. Los resultados del estudio proporcionan información importante para los educadores, quienes pueden utilizar estos hallazgos para adaptar sus iniciativas a las necesidades de las poblaciones potencialmente vulnerables.

Otro estudio realizado por Nabhan (2021) analizó las concepciones de la alfabetización digital de los futuros profesores en el contexto de la enseñanza del inglés como lengua extranjera. Se encontró que aunque los estudiantes carecían de habilidades críticas y de comprensión de la cultura digital, poseían competencias en la búsqueda de información, la comunicación y las habilidades funcionales.

Por otro lado, Alvarez-Flores (2021) realizó un estudio para identificar las medidas de capacitación necesarias para lograr prácticas de navegación en línea seguras por parte de los profesores universitarios. Los resultados mostraron que hay una necesidad de capacitación en seguridad digital para los profesores universitarios para prevenir comportamientos riesgosos.

En un estudio comparativo entre Hungría y Vietnam, Mai y Tick (2021) encontraron que los estudiantes universitarios en general poseen un conocimiento deficiente de la seguridad cibernética, lo que lleva a un bajo nivel de conciencia sobre las amenazas cibernéticas.

Harriman et al., (2020) investigaron la exposición de los jóvenes a materiales de odio en línea y descubrieron una asociación entre la exposición a mensajes de odio y el tiempo pasado en línea, el rendimiento académico, la comunicación con extraños en las redes sociales y la desinhibición en línea benigna.

Además, Hsieh et al. (2020) estudiaron la autoeficacia de los padres en el manejo del uso de Internet de sus hijos adolescentes y encontraron que el comportamiento y la crianza de los hijos contribuyen a la autoeficacia de los padres en el manejo del uso de Internet de los adolescentes.

En conjunto, estos estudios destacan la importancia de abordar la seguridad digital, la alfabetización digital y la conciencia de riesgos en línea en diversos contextos, desde la educación hasta el uso de billeteras digitales y el manejo parental del uso de Internet.

3. Análisis y resultados

A continuación, se exponen los diferentes resultados que se derivan del análisis de los datos obtenidos en este metaanálisis.

3.1. Análisis de correlación

El análisis de correlación es una técnica estadística que se utiliza para evaluar la relación entre dos variables (figura 1). Los coeficientes de correlación (r, N) proporcionan información sobre la fuerza y dirección de dicha relación. Un valor de r cercano a 1 indica una correlación positiva fuerte, mientras que un valor cercano a -1 indica una correlación negativa fuerte. Un valor cercano a 0 sugiere que no hay correlación entre las variables. La letra "N" representa el tamaño de la muestra utilizada en el análisis.

En este caso, se utiliza un modelo de efectos aleatorios con 8 estudios (k = 8) para obtener una estimación más precisa de la relación entre las variables en cuestión. Este enfoque tiene en cuenta las diferencias entre los estudios y proporciona una estimación más generalizable. En este análisis, el coeficiente de correlación estimado es de 1.10, lo que sugiere una correlación positiva entre las variables.

Además, se presenta información adicional sobre el análisis, como el error estándar (se), el valor Z, el intervalo de confianza (CI) y el valor p. El error estándar mide la variabilidad en las estimaciones de la correlación, mientras que el valor Z indica cuán significativa es la correlación. En este caso, el valor Z es de 556, lo que sugiere una correlación altamente significativa (<<.001). El intervalo de confianza proporciona un rango en el cual es probable que se encuentre el verdadero coeficiente de correlación. El límite inferior del intervalo de confianza es 1.484 y el límite superior es 0.197. Por último, el valor p indica la probabilidad de obtener un resultado tan extremo o más extremo que el observado, asumiendo que no hay correlación en la población; en este caso, el valor p es de 0.710. El estimador Tau* de máxima

verosimilitud restringida se utiliza para calcular la heterogeneidad entre los estudios en el modelo de efectos aleatorios.

Random-Effects Model (k = 8)

	Estimate	se	Z	p	CI Lower Bound	CI Upper Bound
Intercept	1.10	0.197	5.56	< .001	0.710	1.484
	.	.	.	.	.	.

Nota. Tau^2 Estimator: Restricted Maximum-Likelihood

Figura 1. *Análisis de correlación*

Por otro ladom la heterogeneidad en el contexto de estudios combinados o metaanálisis se refiere a la variabilidad o diversidad entre los estudios incluidos en el análisis (figura 2). La presencia de heterogeneidad puede afectar la precisión y generalización de las conclusiones obtenidas. Para cuantificar y evaluar la heterogeneidad entre los estudios, se utilizan varias estadísticas, como Tau, F, H, R, df, Q y P.

Tau es una medida de la heterogeneidad entre los estudios y, en este caso, su valor es de 0.3076 con un error estándar (SE) de 0.1668. Un valor de Tau más grande indica una mayor heterogeneidad. La prueba Q es otra medida utilizada para evaluar la heterogeneidad. Un valor de Q más alto sugiere una mayor variabilidad entre los estudios. En este ejemplo, el valor de Q es 606.396. El valor de los grados de libertad (df) asociados a la prueba Q es 7.000, lo que indica que se han incluido 8 estudios en el análisis (k-1, donde k es el número de estudios).

Las otras estadísticas presentadas, como F, H, R y P, también proporcionan información adicional sobre la heterogeneidad en el análisis. F es una medida de la proporción de la variación total explicada por la variación entre los estudios, y su valor es de 0.555 en este caso. H es una medida de la consistencia entre los estudios y su valor es de 98.86%. R es una medida de la relación entre la heterogeneidad y la variación total. Por último, el valor P se utiliza para evaluar la significancia estadística de la heterogeneidad. Un valor P más pequeño sugiere una mayor probabilidad de que la heterogeneidad sea estadísticamente significativa. En este caso, el valor P es <.001, lo que indica una heterogeneidad significativa entre los estudios incluidos en el análisis.

Heterogeneity Statistics

Tau	Tau^2	I^2	H^2	R^2	df	Q	p
0.555	0.3076 (SE= 0.1668)	98.86%	87.717	.	7.000	606.396	< .001

Figura 2. *Transformación z de Fisher*

El análisis se llevó a cabo utilizando el coeficiente de correlación transformado de Fisher r-to-z como medida de resultado. Se ajustó un modelo de efectos aleatorios a los datos. La cantidad de heterogeneidad (es decir, tau^3) se estimó utilizando el estimador de máxima verosimilitud restringida (Viechtbauer 2005). Además de la estimación de tau, se informan la prueba Q para la heterogeneidad (Cochran 1954) y la estadística. En caso de detectar alguna cantidad de heterogeneidad (es decir, $tau^2 > 0$ independientemente de los resultados de la prueba Q), también se proporciona un intervalo de predicción para los resultados verdaderos. Los residuos estudiantizados y las distancias de Cook se utilizan para examinar si los estudios pueden ser atípicos y/o influyentes en el contexto del modelo. Se consideran posibles valores atípicos aquellos estudios con un residuo estudiantizado mayor que el percentil 100 x (1 -0.05/12 X k) de una distribución normal estándar (es decir, utilizando una corrección de Bonferroni con alfa de dos colas = 0.05 para k estudios incluidos en el metaanálisis). Se consideran influyentes aquellos estudios con una distancia de Cook mayor que la mediana más seis veces el rango intercuartil de las distancias de Cook. La prueba de correlación de rangos y la prueba de regresión utilizando el error estándar de los resultados observados como predictor se utilizan para verificar la asimetría del gráfico de embudo.

Se incluyeron un total de k = 8 estudios en el análisis. Los coeficientes de correlación transformados de Fisher r-to-z observados oscilaron entre 0.3654 y 1.7645, con la mayoría de las estimaciones siendo positivas (100%). El coeficiente de correlación transformado promedio de Fisher r-to-z estimado en base al modelo de efectos aleatorios fue de backslash hat[Mmu] = 1.0973 (95% CI 0.7103 a 1.4844). Por lo tanto, el resultado promedio difirió significativamente de cero (z = 5.5567, p < 0.0001). Según la prueba Q, los resultados verdaderos parecen ser heterogéneos (a(7) = 606.3958, p < 0.0001 tau = 0.3076 98.8600%). Un intervalo de predicción del 95% para los resultados verdaderos es dado por -0.0565 = hasta 2.2511. Por lo tanto, aunque el resultado promedio se estima que es positivo, en algunos estudios el resultado verdadero podría ser de hecho negativo. Un examen de los residuos estudiantizados reveló que ninguno de los estudios tenía un valor mayor que ± 2.7344 y, por lo tanto, no había indicios de valores

atípicos en el contexto de este modelo. Según las distancias de Cook, ninguno de los estudios podría considerarse excesivamente influyente. Tanto la prueba de correlación de rangos como la prueba de regresión indicaron una posible asimetría en el gráfico de embudo ($p = 0.0312$ y $p = 0.0013$, respectivamente.

3.2. Diagrama de Bosque

En la siguiente figura (figura 3), se puede observar un diagrama de bosque. Este es empleado para tener una visualización gráfica de de los resultados estimados de investigaciones científicas que abordan la misma cuestión.

Así, se pueden observar en el diagrama tres columnas. La primera hace referencia a los estudios analizados. La segunda es la representación visual de los resultados de los estudios. La línea vertical central se denomina línea de 'no efecto' y simboliza que no hay diferencia entre el grupo de intervención y el grupo control. En este metaanálisis la línea de no efecto tiene el valor de «cero». Ambos lados de la línea, simbolizan si los resultados favorecen o no la intervención.

Dentro de la gráfica, los cuadrados representan el efecto evaluado en cada estudio y su tamaño está directamente relacionado con el peso de los estudios en el metaanálisis, además esto se expresa de manera numérica en la columna de la derecha. La línea horizontal que los atraviesa representa el intervalo de confianza (Martínez-Rodríguez, 2015). Si la línea es más larga esto quiere decir que mayor es el intervalo y, por ende, los resultados de la investigación menos concretos.

Los cuadrados que se encuentran en medio de cada línea horizontal son los efectos individuales. Dependiendo de dónde se posicionen, si a la izquierda o a la derecha de la línea de referencia, la heterogeneidad de los estudios será más alta o más baja. En este caso, todos ellos se posicionan a la derecha de la línea, por lo que al estar todos en un mismo lado se concluye que la heterogeneidad de todos ellos es baja.

El diamante que aparece en la parte baja de la gráfica representa el resultado global del metaanálisis con el intervalo de confianza al 95 %. Claramente, se puede observar cómo el diamante se posiciona a un lado de la línea de referencia sin traspasarla o rozarla, por lo que se puede afirmar que el intervalo de confianza sí es estadísticamente significativa.

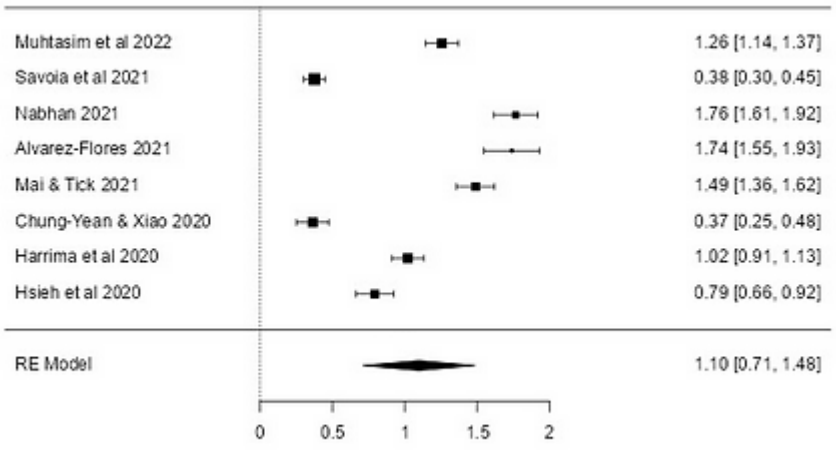


Figura 3. *Diagrama de bosque*

3.3. Gráfico en Embudo

La siguiente figura (figura 4) se trata de un gráfico de embudo, en él se representa la magnitud del efecto medido (eje X) frente a una medida de precisión (eje Y), que se trata del error estándar. Cada estudio primario es representado con un punto y, por lo tanto, se obtiene una nube de puntos (Sterne & Egger, 2001).

En el caso de la figua que aquí se presenta, se puede observar cómo sí existe una simetría en la parte central del embudo; sin embargo, no la hay en el resto de la figura pues hay estudios con mayor desviación estándar y otros con menos.

Esta asimetría puede deberse a que el tamaño muestral de este metaanálisis no es lo suficientemente grande o está indicando que los estudios publicados de la temática de estudio solo hacen referencia a determinados resultados, no son de suficiente calidad o se trata de intervenciones las cuales varían de efecto según su tamaño muestral.

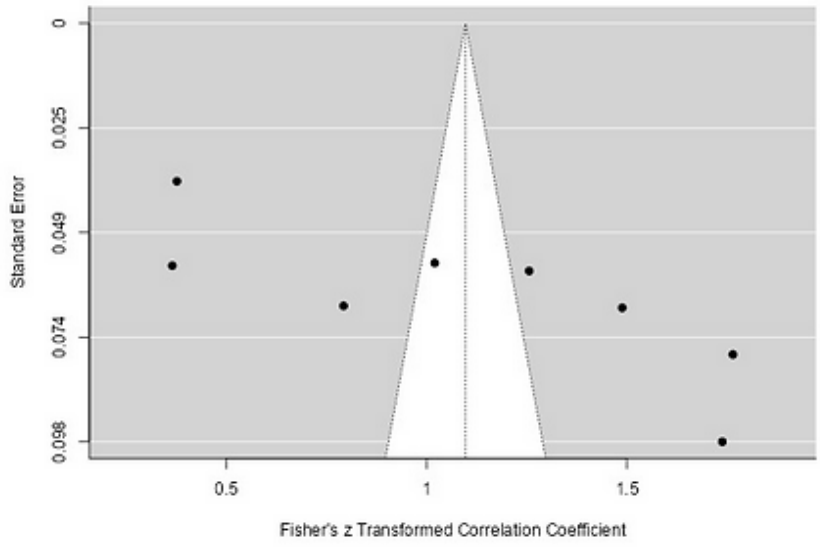


Figura 4. *Gráfico de embudo*

4. Discusión

El estudio de Muhtasim et al. (2022) sobre la seguridad de las billeteras digitales y otros estudios relacionados con la alfabetización digital, la seguridad en línea y la conciencia de riesgos en línea en diferentes contextos, resaltan la importancia de abordar estos temas desde distintas perspectivas, tales como la educación y el uso de servicios digitales. De igual modo, el análisis de correlación realizado en ese estudio muestra una relación positiva entre las variables estudiadas, aunque se encontró una heterogeneidad significativa entre los estudios incluidos.

En esta misma línea, Rodríguez-García, et al., (2019) muestran en su investigación la importancia de investigar sobre la temática de competencia digital dentro del ámbito educativo destacando a España como uno de los países con más contribuciones a este respecto en los últimos años. De igual modo y en una investigación más reciente todavía, Savoia et al. (2021) establecen que es inconmensurable la cantidad de información a la que tienen acceso los jóvenes gracias a la tecnología, lo que supone también un aumento de los peligros y riesgos en red a consecuencia del uso de los diferentes dispositivos.

En los últimos años la seguridad digital representa una de las grandes temáticas de estudio no solo por su importancia para un correcto uso de las TIC (Recio Muñoz, et al., 2020), si no por la poca formación de los estudiantes y de los docentes de cualquier nivel educativo (Pozo Sánchez, et al., 2020). Aspecto que no frena que la competencia digital y el uso de los dispositivos se frene en cualquier aspecto de la vida ya sea formativo o de ocio.

Otros autores como Harriman et al., (2020), han estudiado la conexión entre la exposición inadecuada de los estudiantes a mensajes negativos en redes (odio, ciberacoso, etc.) y cómo afecta eso al rendimiento académico, entre otras cosas. De igual modo, Quiñones-Negrete, et al., (2021) establecen que los docentes a este respecto deben adaptar ese uso de los dispositivos y las diferentes plataformas a cada estudiante y su estilo de aprendizaje para que así se reduzcan las posibilidades de riesgos en internet y ante el uso de su competencia digital.

5. Conclusiones

Este análisis de correlación ha demostrado una relación positiva entre las dos variables estudiadas, con un coeficiente de correlación estimado de 1.10. La significancia estadística de esta correlación se ve respaldada por el valor Z de 556 y un valor p de 0.710. Sin embargo, se ha detectado una heterogeneidad significativa entre los estudios incluidos en el análisis, lo que puede afectar la precisión y generalización de las conclusiones obtenidas. A pesar de esta heterogeneidad, no se identificaron estudios atípicos o influyentes que pudieran haber sesgado los resultados.

El intervalo de predicción del 95% proporciona un rango en el que es probable que se encuentren los coeficientes de correlación verdaderos de otros estudios similares. Aunque el resultado promedio sugiere una correlación positiva, es importante tener en cuenta que en algunos estudios el resultado verdadero podría ser negativo. Por lo tanto, se recomienda interpretar estos resultados con precaución y considerar la posibilidad de realizar investigaciones adicionales para obtener una comprensión más profunda de la relación entre las variables.

Además, es necesario prestar atención a la posible asimetría en el gráfico de embudo, ya que las pruebas de correlación de rangos y de regresión sugieren la presencia de un sesgo potencial. Esto se debe a la publicación selectiva de estudios con resultados positivos o a otras fuentes de sesgo en la literatura disponible. Para abordar esta preocupación, se podrían buscar y analizar estudios no publicados o con resultados negativos para obtener una visión más completa y equilibrada de la relación entre las variables en estudio.

Por último, se va a dar respuesta a las preguntas de investigación que han guiado la investigación.

¿Tienen los estudiantes de Educación Superior un correcto nivel de seguridad digital?

Los diferentes estudios analizados establecen que existe un nivel correcto en cuanto a seguridad dentro de estos estudiantes; sin embargo, si ese nivel se compara con el resto de las áreas dentro de la competencia digital es más bajo, lo que indica que no es el área a la que más importancia se le da o que es la que más dedicación y trabajo necesita para que este nivel aumente.

¿Se implementa la seguridad digital como contenido a trabajar en la etapa de Educación Superior?

Este aspecto de la formación dentro de la competencia digital sí es trabajado, pero en la mayoría de los casos como contenido trasversal asociado a otros conocimientos o prácticas. Mucho del conocimiento de los estudiantes a este respecto proviene de una formación autodidacta.

¿Se publican mayoritariamente artículos con resultados positivos sobre la relevancia de la seguridad digital en Educación Superior?

Como se ha mencionado anteriormente, sí. Esto se puede comprobar a través del gráfico de embudo. Es una práctica habitual que los investigadores publiquen solo los resultados positivos y desechen los negativos. Nos encontramos entonces con dos tipos de corrientes dentro la temática que nos ocupa: por un lado, el nivel de seguridad digital en los estudiantes de Educación Superior es correcto en aquellos lugares donde se trabaja o, hay escasez de publicaciones que expresen lo contrario.

Finalmente, cabe destacar que el modelo de efectos aleatorios utilizado en este análisis tiene en cuenta las diferencias entre los estudios y proporciona una estimación más generalizable. No obstante, es importante recordar que este enfoque no elimina completamente el impacto de la heterogeneidad en los resultados. Por lo tanto, es fundamental considerar las limitaciones del análisis y reconocer que las conclusiones obtenidas pueden verse influenciadas por las diferencias entre los estudios incluidos. En el futuro, se podrían realizar análisis adicionales que examinen las posibles fuentes de heterogeneidad y cómo estas pueden afectar la relación entre las variables analizadas.

En resumen, es importante continuar investigando y abordando la seguridad digital, la alfabetización digital y la conciencia de riesgos en línea en diversos contextos, para mejorar la educación y el uso seguro de las tecnologías digitales. Los estudios futuros deben considerar las limitaciones y heterogeneidades encontradas en los análisis de correlación, y buscar fuentes adicionales de información para obtener una comprensión más precisa y completa de las relaciones entre estas variables.

6. Financiación

Este estudio forma parte de un proyecto de investigación financiado con fondos públicos del Ministerio de Educación, Cultura y Deportes del Gobierno de España (Referencia: FPU18/01595).

Referencias

Álvarez-Flores, E. P. (2021). Uso crítico y seguro de tecnologías digitales de profesores universitarios. *Formación universitaria*, *14*(1), 33-44.

Botella, J., & Zamora, Á. (2017). El meta-análisis: una metodología para la investigación en educación. *Educación XXI: revista de la Facultad de Educación*, *20*(2), 17-38. https://doi.org/10.5944/educxx1.19030

Chiang, C. Y., & Tang, X. (2022). Use public Wi-Fi? Fear arouse and avoidance behavior. *Journal of Computer Information Systems*, *62(*1), 73-81

Francis, G. (2013). Replication, statistical consistency, and publication bias. *Journal of Mathematical Psychology, 57*(5), 153-169.

Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., & Kotzanikolaou, P. (2017). Security awareness of the digital natives. *Information*, *8*(2), 42. https://doi.org/10.3390/info8020042

Gómez-Galán, J., Martínez-López, J. Á., Lázaro-Pérez, C., & Sarasola Sánchez-Serrano, J. L. (2020). Social networks consumption and addiction in college students during the COVID-19 pandemic: Educational approach to responsible use. *Sustainability*, *12*(18), 7737. https://doi.org/10.3390/su12187737

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*, 1-23. https://doi.org/10.1007/s10639-023-11785-7

Harriman, N., Shortland, N., Su, M., Cote, T., Testa, M. A., & Savoia, E. (2020). Youth exposure to hate in the online space: an exploratory analysis. *International journal of environmental research and public health, 17*(22), 8531.

Hernández Serrano, M. J., Renés-Arellano, P., Campos Ortuño, R. A., & González-Larrea, B. (2021). Privacidad en redes sociales: análisis de los riesgos de auto-representación digital de adolescentes españoles. *Revista Latina de Comunicación Social, 79,* 133–154. https://doi.org/10.4185/RLCS-2021-1528

Hsieh, Y. P., Wu, C. F., Chou, W. J., & Yen, C. F. (2020). Multidimensional correlates of parental self-efficacy in managing adolescent internet use among parents of adolescents with attention-deficit/hyperactivity disorder. *International Journal of Environmental Research and Public Health, 17*(16), 5768.

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica, 18*(8), 67-89.

Martínez-Rodríguez, R. (2015). *Cómo interpretar un metaanálisis.* http://fedn.es/blog/evidencianutricion/como-interpretar-un-metaanalisis/

Muhtasim, D. A., Tan, S. Y., Hassan, M. A., Pavel, M. I., & Susmit, S. (2022). Customer satisfaction with digital wallet services: An analysis of security factors. *International Journal of Advanced Computer Science and Applications, 13*(1), 195-206.

Nabhan, S. (2021). Pre-service teachers' conceptions and competences on digital literacy in an efl academic writing setting. *Indonesian Journal of Applied Linguistics*, *11*(1), 187-199.

Nabhan, S. (2021). Pre-service teachers' conceptions and competences on digital literacy in an efl academic writing setting. *Indonesian Journal of Applied Linguistics*, *11*(1), 187-199.

Ojeda Pérez, M., & Rey Alamillo, R. D. (2021). Prevenir e intervenir en los riesgos asociados a las tecnologías de la información y la comunicación: el caso del cyberbullying. *Tecnología, Ciencia y Educación, 19,* 53-80. https://doi.org/10.51302/tce.2021.612

Pozo Sánchez, S., López Belmonte, J., Fernández Cruz, M., & López Núñez, A.J. (2020). Análisis correlacional de los factores incidentes en el nivel de competencia digital del profesorado. *Revista Electrónica Interuniversitaria de Formación del Profesorado*, *23*(1), 143-159. https://doi.org/10.6018/reifop.396741

Quiñones-Negrete, M. M., Martin-Cuadrado, A. M., & Coloma-Manrique, C. R. (2021). Rendimiento académico y factores educativos de estudiantes del programa de educación en

entorno virtual. Influencia de variables docentes. *Formación universitaria*, *14*(3), 25-36. http://dx.doi.org/10.4067/S0718-50062021000300025

R Core Team (2021), R: A Language and environment for statistical computing. (Version 4.1) [Computer software]. Retrieved from https://cran.r-project.org. (R packages retrieved from MRAN snapshot 2022-01-01).

Recio Muñoz, F., Silva Quiroz, J., & Abricot Marchant, N. (2020). Análisis de la Competencia Digital en la Formación Inicial de estudiantes universitarios: Un estudio de meta-análisis en la Web of Science. *Píxel-Bit. Revista de Medios y Educación*, (59), 125-146. https://doi.org/10.12795/pixelbit.77759

Rodríguez García, A. M., Raso Sánchez, F., & Ruiz Palmero, J. (2019). Competencia digital, educación superior y formación del profesorado: un estudio de meta-análisis en la Web of Science. *Pixel-Bit Revista de Medios y Educación*, (54), 65-81. https://doi.org/10.12795/pixelbit.2019.i54.04

Savoia, E., Harriman, N. W., Su, M., Cote, T., & Shortland, N. (2021). Adolescents' exposure to online risks: Gender disparities and vulnerabilities related to online behaviors. *International journal of environmental research and public health*, *18*(11), 5786.

Sayaf, A. M., Alamri, M. M., Alqahtani, M. A., & Al-Rahmi, W. M. (2021). Information and communications technology used in higher education: An empirical study on digital learning as sustainability. *Sustainability*, *13*(13), 7074. https://doi.org/10.3390/su13137074

Sterne, J. A., & Egger, M. (2001). Funnel plots for detecting bias in meta-analysis: guidelines on choice of axis. *Journal of clinical epidemiology*, *54*(10), 1046-1055. https://doi.org/10.1016/S0895-4356(01)00377-8

The jamovi project (2022). jamovi. (Version 2.3) [Computer Software]. Retrieved from https://www.jamovi.org.

van Houwelingen, H. C., Zwinderman, K. H., Stijnen, T. (1993). A bivariate approach to meta-analysis. *Statistics in Medicine*, *12*(24), 2273-2284.

Vázquez-Cano, E., & Pascual-Moscoso, C. (2022). Protección de datos y uso ético de la tecnología para una didáctica sostenible. *Revista Electrónica Interuniversitaria de Formación del Profesorado*, *25*(3), 95-110. https://doi.org/10.6018/reifop.529831

Viechtbauer, W. (2010), Conducting meta-analyses in R with the metafor package. *Journal of Statistical Software, 36*, 1-48.

5.5.Quinta publicación

Evaluación de las Competencias en Seguridad Digital de los Estudiantes de Educación Superior de la Universidad de Granada

Este trabajo ha sido publicado como capítulo del libro de la editorial Dykinson, que lleva por título Espacios de Aprendizaje e Implicaciones Prácticas (ISBN 978-84-1122-697-4). Esta editorial independiente publica mayoritariamente literatura especializada para profesionales de diferentes áreas, destacando las relativas a la Educación y a la Psicología. Esta se haya entre las seis 6 editoriales españolas, obteniendo también el puesto 14 de 272 en Scholarly Publishers Indicators (SPI) “In Humanities and Social Sciences” de todas las editoriales españolas con un indicador de prestigio (ICEE) de 20.763 del general de 504 editoriales. En lo relativo al área de Educación se haya en la posición 16 de 94 de un total de 156 editoriales con un ICEE de 0.954 (cuartil Q1).

Referencia bibliográfica:

Rodríguez-Jiménez. C., Trujillo-Torres, J.M., Alonso-García, S., y Martínez-Domingo, J.A. (2023). Evaluación de las Competencias en Seguridad Digital de los Estudiantes de Educación Superior de la Universidad de Granada. En (Coords. G. Estuardo Ceballos Uve, M.J. Santos Villalba, M.J. Alcalá del Olmo Fernández y D. Álvarez Ferrándiz) *Educación integral con perspectivas innovadoras para el desarrollo educativo* (pp. 43-53). Dykinson. ISBN 978-84-1170-706-0.

Evaluación de las Competencias en Seguridad Digital de los Estudiantes de Educación Superior de la Universidad de Granada

Carmen Rodríguez Jiménez, Juan Manuel Trujillo Torres, José Antonio Martínez Domingo.

Datos de contacto:

Carmen Rodríguez Jiménez

Universidad de Granada

carmenrj@ugr.es

Juan Manuel Trujillo Torres

Universidad de Granada

jttorres@ugr.es

Santiago Alonso García

salonsog@ugr.es

José Antonio Martínez Domingo

Universidad de Granada

josemd@ugr.es

RESUMEN

La seguridad digital como elemento de la competencia digital es fundamental para la formación de cualquier persona en la sociedad actual. Ser consciente de los peligros asociados al uso de los dispositivos y de internet es prioritario para todos los usuarios. Este aspecto adquiere aún mayor relevancia cuando se trata de la formación de estudiantes de educación. En esta investigación se analizan las puntuaciones obtenidas en el área de formación de seguridad digital de los estudiantes de educación de la Universidad de Granada (n=269). Se tienen en cuenta todas las subáreas de esta competencia para comprobar en cuáles se obtienen mayores puntaciones, si existen diferencias significativas entre sexos y por edad y si existen correlaciones de algún tipo entre las diferentes subáreas. Los resultados muestran que el área de seguridad digital está presente en estos estudiantes; sin embargo, existen deficiencias en algunas subáreas, en este caso la más deficitaria es la correspondiente a la Protección de la salud y del bienestar personal. Se concluye que debería incrementarse la formación en determinados elementos de la competencia en seguridad digital para que la formación en este aspecto sea lo más completa posible, haciendo así que los futuros docentes tengan una competencia digital eficiente.

PALABRAS CLAVE: competencia digital; seguridad digital; Educación Superior; estudiantes; cuestionario; evaluación

Assessment of the Digital Security Competences of University Education Students in the University of Granada

ABSTRACT

Digital safety as an element of digital competence is fundamental to the education of any person in today's society. Being aware of the dangers associated with the use of devices and the internet is a priority for all users. This becomes even more relevant when it comes to the education of students in education. This research analyses the scores obtained in the area of digital safety training of education students at the University of Granada (n=269). All the sub-areas of this competence are taken into account in order to check in which ones the highest scores are obtained, if there are significant differences between sexes and by age and if there are any correlations of any kind between the different sub-areas. The results show that the area of digital security is present in these students; however, there are deficiencies in some sub-areas, in this case the most deficient is the one corresponding to the Protection of health and personal well-being. It is concluded that training in certain elements of digital safety competence should be increased in order to make training in this area as complete as possible, thus making future teachers digitally competent.

KEYWORDS: digital competence; digital security; higher education; students; questionnaire; assessment

Introducción

La seguridad digital se ha convertido en la actualidad en una cuestión de relevancia crítica en todos los ámbitos de la sociedad, y su importancia se acentúa aún más en el contexto de la Educación Superior (Fernández-Cruz y Fernández-Díaz, 2016). La relevancia ya establecida de la competencia digital y de todas sus áreas dentro del ámbito educativo hace que cada una de ellas esté siendo estudiada y promovida de forma más exhaustiva (Escudero, et al., 2019). Así, el área 4 dentro de la competencia digital, el área de seguridad se está convirtiendo en la actualidad en una de las más importantes por los beneficios que puede aportar a los usuarios y los problemas que puede prevenir o paliar (INTEF, 2022). Las subáreas que la componen abarcan todos los componentes que pueden causar problemas o inconvenientes a la hora de utilizar un dispositivo tecnológico. Estas subáreas son (Comisión Europea, 2016):

- Protección de dispositivos

- Protección de los datos personales
- Protección de la salud
- Protección del medio ambiente

Es importante que la formación se imparta en todas las subáreas para que la formación sea lo más completa posible, así como para que la concienciación e implementación de la seguridad sea lo más eficiente y eficaz posible (Ortega-Sánchez, et al., 2013).

Este artículo explorará la seguridad digital en los estudiantes de Educación Superior y destacará su especial relevancia en el contexto de los estudiantes de educación, que son los futuros formadores y educadores de la sociedad. La seguridad digital aborda un conjunto de principios y prácticas destinados a proteger la información, la privacidad y la integridad de los usuarios en el entorno digital.

Seguridad digital en Educación Superior

La Educación Superior, al igual que otros sectores, ha experimentado una transformación digital en las últimas décadas. Los estudiantes de Educación Superior, al hacer un uso extensivo de la tecnología y las redes digitales en su aprendizaje, investigación y comunicación, se han convertido en usuarios frecuentes y vulnerables de los entornos digitales. La seguridad digital en este contexto se convierte en un componente esencial para garantizar un entorno de estudio seguro y productivo (Ramírez-Montoya, et al., 2017).

Tanto la ciberseguridad como la protección de datos son elementos esenciales dentro de las instituciones de Educación Superior. Por ello, es fundamental conocer el nivel de competencia en seguridad digital entre los estudiantes de este nivel educativo (Singar y Akhilesh, 2020).

Del mismo modo, también son importantes otras partes de la seguridad digital que no siempre se tienen en cuenta. Como la protección de la propia seguridad o del entorno que nos rodea.

Todos los elementos de la competencia digital han sido objeto de numerosas investigaciones en los últimos años. Éstas han determinado en muchos casos que el área de seguridad digital es siempre la menos valorada y la que menos se forma en las aulas (García-Vandewalle, et al., 2023).

Importancia de la Seguridad Digital en los estudiantes de educación

Los futuros educadores desempeñan un papel crucial en la formación de las generaciones venideras y, por tanto, la seguridad digital es especialmente relevante para ellos (Tárraga-Mínguez, et al., 2021). Algunas razones clave son:

- Los profesores como modelos a seguir durante muchas etapas: Los educadores no sólo transmiten conocimientos académicos, sino que también sirven de modelo para sus alumnos. Si no tienen, adoptan y transmiten buenas prácticas de seguridad digital, es menos probable que los alumnos, independientemente de su etapa educativa, adopten comportamientos seguros y responsables en línea.

- Enseñanza digital: La tecnología se ha convertido en una parte integral y fundamental de la educación actual. Los educadores deben estar bien preparados para enseñar habilidades de seguridad digital a sus alumnos y fomentar el uso responsable de la tecnología.

- Protección de la comunidad educativa: Los estudiantes de Educación también deben estar capacitados para proteger la seguridad digital y todo lo que ello implica, del resto de agentes implicados en el proceso de Enseñanza-Aprendizaje, ayudando a prevenir situaciones de ciberbullying, phishing u otras amenazas que se puedan generar.

Numerosos estudios recientes han analizado las competencias de los estudiantes de educación respecto a su nivel de seguridad digital. Así, Gallego-Arrufat, et al. (2019) establecen que estos futuros docentes tienen una buena actitud hacia esta competencia; sin embargo, su nivel de conocimientos y habilidades sobre el uso seguro y responsable de las redes sociales e Internet es menor. En la misma línea, Alonso-Ferreiro, et al. (2019) establecen que existe una discordancia o desacuerdo entre las buenas actitudes presentes en el alumnado y la alta concienciación sobre el uso seguro de la tecnología, especialmente por parte del sexo femenino.

Latorre-Medina y Fuentes Amaya (2022) determinan que una gran parte de los estudiantes de educación reconocen no estar suficientemente formados en seguridad como parte fundamental de su competencia digital. Todo ello a pesar de ser conscientes de la importancia de conocer las normas y precauciones a tomar en el uso de medios digitales y redes sociales.

Grande-de-Prado, et al., (2020), García-Martín y García-Sánchez (2017) y Martínez-Garcés y Garcés-Fuenmayor (2020) vuelven a establecer que existen diferencias significativas entre géneros en cuanto a la autopercepción del nivel de competencia digital de los estudiantes de educación. Muestran que los hombres se auto perciben mejor formados en protección de

dispositivos, mientras que las mujeres se auto perciben mejor formadas en protección de datos e identidad personal.

El problema de la investigación radica en que la competencia y la formación digitales que reciben los estudiantes en la enseñanza revelan déficits en la dimensión de la seguridad, que no saben identificar.

Este artículo intentará responder a la siguiente pregunta:

¿Están preparados los futuros docentes para hacer frente a los riesgos de seguridad digital y de red que pueden encontrarse en el desarrollo de su profesión?

Esta pregunta de investigación da lugar a las hipótesis que se plantean para llevar a cabo esta investigación:

H0: La seguridad digital como elemento de la competencia digital no está presente en los estudiantes de educación durante su formación inicial.

Hi: La seguridad digital como elemento de la competencia digital de los docentes está presente en los estudiantes de educación durante su formación inicial.

El propósito de esta investigación será, por tanto, eliminar la hipótesis nula (H0) y a través del análisis y evaluación del tema tratado contrastar la premisa que dicta la hipótesis planteada por el investigador (Hi).

Así, este trabajo se presenta con el objetivo general de averiguar e interpretar el grado de conocimiento y aplicación de buenos mecanismos de seguridad digital en todas las subáreas de la seguridad digital.

Método

El enfoque elegido para esta investigación es cuantitativo, utilizando un instrumento de cuestionario para conocer y describir la autopercepción de los alumnos sobre su competencia en el área de seguridad, así como la valoración del nivel en esta área en su conjunto y de sus diferentes subáreas en particular.

El trabajo se enmarca, por tanto, dentro de un proyecto de investigación no experimental. En concreto, el diseño del mismo será transversal o transversal, exploratorio, descriptivo y correlacional (Hernández, et al., 2016).

Población y muestra

El objeto de estudio son los estudiantes de Ciencias de la Educación de la Universidad de Granada, en todos sus campus. En concreto, la muestra está formada por estudiantes de los grados en Educación Primaria y Educación Infantil, Pedagogía y Educación Social. Para su elaboración se ha utilizado un muestreo por conveniencia (Hernández, et al., 2016).

La muestra está formada por un total de 269 participantes (n = 269). La Universidad de Granada es un caso particular ya que consta de 3 campus diferenciados; Campus de Granada, Campus de Ceuta y Campus de Melilla, estos dos últimos en las respectivas ciudades autónomas de España.

En cuanto al género de los participantes, 191 son mujeres y 76 son hombres, sólo dos de ellos prefirieron no contestar a esta pregunta. Se puede observar que hay una mayoría de mujeres, tendencia muy común en las titulaciones de educación (Salas-Morera, et al., 2021).

Por otro lado, los estudiantes se distribuyen de la siguiente manera en las diferentes titulaciones dentro de las universidades:

- Grado en Educación Primaria: 81 alumnos (30,3%).
- Grado en Educación Infantil: 75 alumnos (28,1%)
- Grado en Pedagogía: 61 alumnos (22,8%)
- Grado en Educación Social: 52 alumnos (19,5%)

Instrumento

El instrumento utilizado en esta investigación es un cuestionario ya validado (García-Valcárcel, et al., 2019), ya que fue sometido a discusión entre pares y a la evaluación de expertos. Por tanto, el cuestionario está compuesto por un total de 16 ítems, de los cuales 6 hacen referencia a conocimientos y 10 a habilidades. Del mismo modo, todos ellos miden las 4 subáreas existentes dentro del ámbito de la seguridad digital, a saber:

- Protección de dispositivos (ítems 1-4)
- Protección de datos personales (ítems 5-8)
- Protección de la salud (puntos 9-12)
- Protección del medio ambiente (puntos 13-16)

Las preguntas están configuradas de la siguiente manera: la suma de los ítems de conocimientos y habilidades, que son un total de 16, son de tipo prueba objetiva con 4 alternativas de respuesta, donde sólo una es correcta. En este caso, las respuestas se han codificado dicotómicamente:

- 0= ha elegido la respuesta correcta
- 1= ha elegido la respuesta incorrecta

Esto significa que la puntuación máxima de la prueba es de 16 puntos.

Análisis estadístico

Se calcularon estadísticas descriptivas para cada variable. Antes de realizar cualquier análisis estadístico paramétrico, se comprobaron los supuestos de normalidad y homocedasticidad con las pruebas de Kolmogorov-Smirnov y Levene, respectivamente. Para determinar las diferencias entre hombres y mujeres se utilizó una prueba t de muestras emparejadas. La d de Cohen fue el indicador del tamaño del efecto. Para interpretar la magnitud del tamaño del efecto, se adoptaron los siguientes criterios: $d \leq 0,20$, pequeño; $d \leq 0,50$, mediano; y $d \leq 0,80$, grande.

Se utilizó el coeficiente de correlación r de Pearson para examinar la relación entre la edad y la puntuación global. Para interpretar la magnitud de estas correlaciones, se adoptó el siguiente criterio: Trivial: $\leq 0,10$; pequeña: 0,10 a 0,29; moderada: 0,30 a 0,49; grande: 0,50 a 0,69; muy grande: 0,70 a 0,89; casi perfecta: $\geq 0,90$.

Asimismo, se utilizó el coeficiente de correlación r de Pearson para examinar la relación entre cada una de las cuatro áreas del área de seguridad (Subárea 1 (S1): Protección de Dispositivos; Subárea 2 (S2): Protección de datos personales y privacidad; Subárea 3 (S3): Protección de la salud y el bienestar; Subárea 4 (S4): Protección del Medio Ambiente). Al igual que antes, para interpretar la magnitud de estas correlaciones se adoptó el siguiente criterio: Trivial: $\leq 0,10$; pequeña: 0,10 a 0,29; moderada: 0,30 a 0,49; grande: 0,50 a 0,69; muy grande: 0,70 a 0,89; casi perfecta: $\geq 0,90$.

Se utilizó el análisis de regresión múltiple para modelizar la predicción del nivel de competencia en seguridad digital de los estudiantes de educación a partir del resto de variables del área de seguridad. En este análisis de regresión, todas las variables se examinaron por separado. Los datos se analizaron utilizando Statistica (versión 13.3).

Resultados

Se calcularon estadísticas descriptivas para cada variable (Tabla 1).

Tabla 1

Tabla de frecuencias

	Puntuación subárea 1	Puntuación subárea 2	Puntuación subárea 3	Puntuación subárea 4	Puntuación Total
Media	2,57992565	2,4795539	2,91078067	2,14869888	10,1189591
Error estándar	0,06182187	0,06611599	0,05522406	0,05673475	0,14521312
Mediana	3	3	3	2	10
Moda	3	3	3	2	11
Desviación Estándar	1,01395413	1,08438294	0,90574192	0,93051912	2,38167233
Muestra Varianza	1,02810298	1,17588637	0,82036842	0,86586584	5,67236309
Kurtosis	-0,38050512	-0,64343587	-0,15021921	-0,38519089	-0,06770441
Asimetría Coeficiente	-0,40327722	-0,35391091	-0,55127453	-0,10452471	-0,4844543
Rango	4	4	4	4	13
Mínimo	0	0	0	0	2
Máximo	4	4	4	4	15
Suma	694	667	783	578	2722
Recuento	269	269	269	269	269
Nivel de confianza (95,0%)	0,12171832	0,13017282	0,10872817	0,11170251	0,28590361

Como se puede observar en esta tabla la S4 (Protección del Medio Ambiente) es la que menos puntuación tiene. Esto significa que es el aspecto que menos se trabaja y en el que menos se incide en la formación en seguridad digital.

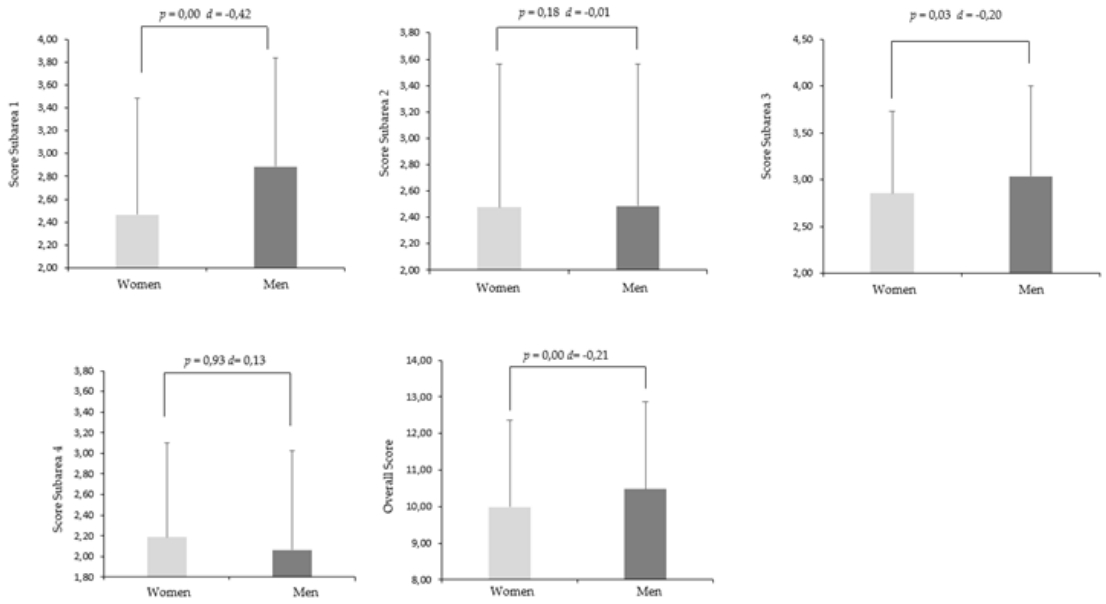
Si nos fijamos en los valores establecidos por la curtosis, podemos ver que en todos los casos es negativa. Esto significa que la distribución es relativamente plana, es decir, platicúrtica. Es decir, los valores de los datos están menos concentrados en torno a la media y hay más valores atípicos, una mayor dispersión de los datos y una mayor probabilidad de encontrar valores extremos.

Para determinar las diferencias entre hombres y mujeres en cuanto a su nivel de competencia en seguridad se utilizó una prueba t para muestras pareadas. Por un lado, una prueba t con datos de cada subárea del área de seguridad reveló diferencias significativas entre hombres y mujeres en S1 (Protección de los dispositivos), S3 (Protección de la salud y el bienestar) y la puntuación global entre todas las subáreas, p=<0,05 en todos los casos.

Sin embargo, el conjunto de datos no reveló diferencias significativas entre S2 (Proteger los datos personales y la privacidad) y S4 (Proteger el medio ambiente), p=0,18, p=0,93, respectivamente. Esto puede verse en la siguiente figura (figura 1):

Figura 1

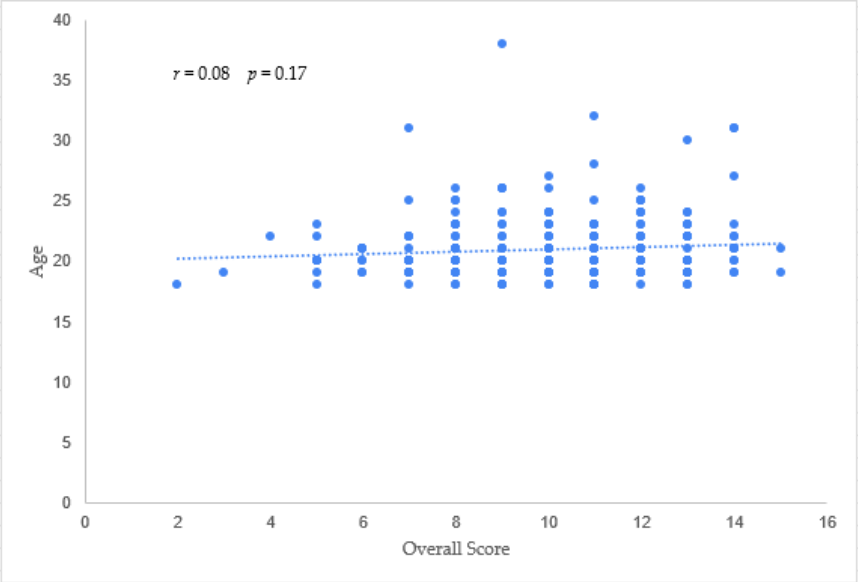
Correlaciones entre sexo y puntuaciones en las subáreas



Se realizó un análisis de correlación para examinar la relación entre la edad y la puntuación global. Así, en lo que respecta a la edad, no existe una correlación significativa con la puntuación global, r=,08, p=,17 (Para más información, véase la figura 2).

Figura 2

Correlaciones entre edad y puntuación total



En cuanto a la edad y cada una de las subáreas, se observan correlaciones diferentes. Se encuentra una pequeña correlación positiva entre la edad y la S1 (Protección de dispositivos): r=.09, p=.15.

En cuanto a las correlaciones entre las cuatro subáreas entre sí, se realizó un análisis para examinar la relación existente. Así, hay algunas correlaciones estadísticamente significativas; la primera es entre el S1 (Protección de los dispositivos) y el S3 (Protección de la salud y el bienestar), r=.17, p=.01; entre el S1 y el S4 (Protección del medio ambiente), r=.21, p=.00; entre el S2 (Protección de los datos personales y la privacidad) y el S4, r=.18, p=.00. Sólo dos de las correlaciones no son estadísticamente significativas: entre S1 y S2, y entre S2 y S3.

Posteriormente, se realizó un análisis de regresión múltiple (Tabla 2) para comprobar qué variables del área de seguridad (de acuerdo con el análisis de correlación), podrían utilizarse para explicar mejor la importancia de las distintas subáreas (S1: Protección de dispositivos, S2: Protección de datos personales y privacidad, S3: Protección de la salud y el bienestar, S4: Protección del medio ambiente). Por un lado, la regresión múltiple para el total de subáreas

reveló efectos significativos para S1 S3, S1 S4, S1 Todas, S2-S4, S2 Todas, S3 Todas y S4 Todas (r2=.03, r2=.04, r2=.39, r2=.03, r2=.37, r2=.32, r2=.39, respectivamente.

Tabla 2

Valores del análisis de regresión que explican la pertinencia de las variables de la subárea en el ámbito de la seguridad

		R	R^2	R^2 Ajustada	F	P	SE
Subáreas Seguridad Digital	S1-S3	0.17	0.03	0.03	7.98	0.01**	0.89
	S1-S4	0.21	0.04	0.04	12.17	0.00**	0.91
	S1-Todas	0.62	0.39	0.39	169.70	0.00**	1.87
	S2-S4	0.18	0.03	0.03	8.62	0.00*	0.92
	S2-Todas	0.60	0.37	0.36	154.04	0.00**	1.90
	S3-Todas	0.56	0.32	0.31	123.21	0.00**	1,97
	S4-Todas	0.63	0.39	0.39	174.26	0.00**	1.86

*** denota significancia p<0,01*

Un valor p bajo (< 0,01) indica que puede rechazarse la hipótesis nula enunciada anteriormente. Este es el caso de todas las regresiones presentadas aquí, las que no aparecen en la tabla no rechazan la hipótesis nula y, por lo tanto, no son estadísticamente significativas. Del mismo modo, esto indica qué combinaciones de subáreas deben mantenerse en el modelo de regresión y cuáles deben descartarse.

Discusión

Las puntuaciones de los estudiantes de educación de la Universidad de Granada han puesto de manifiesto que el área de seguridad digital está presente en su competencia digital y en su formación en la etapa de Educación Superior. Asimismo, se ha podido demostrar que dentro de esta área existen elementos más desarrollados que otros y que, por tanto, obtienen mejores puntuaciones, siendo la protección del medio ambiente la subárea con peores resultados.

Los resultados también muestran que existen diferencias significativas entre hombres y mujeres en determinadas subáreas (Latorre-Medina, et al., 2023), como la protección de los dispositivos y la protección de la salud y de los bienes personales. Los hombres siempre obtienen puntuaciones más altas que las mujeres, haciendo también que sus puntuaciones totales para toda el área de seguridad sean más altas que las de las mujeres (García-Martín, y García-Sánchez, 2017; Grande-de-Prado, et al., 2020; Martínez-Garcés y Garcés-Fuenmayor, 2020).

En cuanto a la edad de los participantes, no se encontraron diferencias significativas entre su edad y las puntuaciones obtenidas, contradiciendo así a [20].

Siguiendo el modelo de regresión descrito anteriormente, se puede observar cómo determinadas combinaciones de subáreas son estadísticamente significativas, lo que es un claro ejemplo de a qué elementos dentro de la seguridad digital se le da mayor importancia y presencia en la formación de los alumnos (Castillejos-López, et al., 2016).

Conclusiones

En conclusión, es importante señalar que la seguridad digital es un área que consta de un gran número de elementos que deben tenerse en cuenta en su totalidad para una formación completa de los alumnos. No sólo los dispositivos y su correcta utilización son importantes en la formación.

Asimismo, cabe destacar que, aunque la tendencia en las titulaciones de educación es a tener un mayor número de alumnas, son los hombres los que obtienen mejores puntuaciones en esta área. Este es un aspecto que debería abordarse en futuras líneas de trabajo.

En este sentido, también se debería explorar por qué hay subáreas dentro de la seguridad digital que son menos estudiadas o menos relevantes, como la protección del medio ambiente, los datos personales y la identidad digital.

Entre las limitaciones de esta investigación se encuentra el tamaño de la muestra, que debe ser ampliada y comparada con otras instituciones para comprobar si existen diferencias en los planes de formación.

Por último, abordar la cuestión de la seguridad digital es esencial para que la competencia y la formación digitales sean completas, eficientes y eficaces. Hacerlo desde la educación superior

y centrarse en la formación de los futuros formadores es un paso fundamental para garantizar que la buena educación que reciben pueda continuar en un futuro próximo en el ejercicio de su profesión.

Agradecimientos

Esta investigación ha sido financiada por el Ministerio de Educación y Formación Profesional de España, subvención número FPU18/01595".

Conflicto de intereses

Los autores declaran no tener ningún conflicto de intereses. Los financiadores no tuvieron ningún papel en el diseño del estudio; en la recopilación, análisis o interpretación de datos; en la redacción del manuscrito, o en la decisión de publicar los resultados.

Contribuciones de los autores

Conceptualización, C.R.-J.; metodología, C.R.-J. y J.-A.M.-D.; software, J.-M.T.-T.; validación, C.R.-J.; análisis formal, J.-A.M.-D..; investigación, J.-M.T.-T.; recursos, J.-M.T.-T.; análisis de datos, J.-A.M.-D.; redacción del borrador original, C.R.-J.; redacción, revisión y edición, J.-A.M.-D.; supervisión, J.-M.T.-T.; administración de proyectos, C.R.-J.; adquisición de financiación, C.R.-J.

Referencias

Alonso-Ferreiro, A., Regueira, U., y Zapico-Barbeito, M. H. (2019). Actitudes de alumnado preadolescente ante la seguridad digital: un análisis desde la perspectiva de género. *Revista de Educación a Distancia (RED)*, *19*(61). https://doi.org/10.6018/red/61/02

Castillejos López, B., Torres Gastelú, C. A., y Lagunes Domínguez, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura*, *8*, 54-69. http://dx.doi.org/10.18381/Ap.v8n2.914

Escudero, V. G., Gutiérrez, R. C., y González-Calero Somoza, J. A. (2019). Analysis of self-perception on the level of teachers' digital competence in teachers training. *Revista Electrónica Interuniversitaria de Formación del Profesorado*, *22*(3), 193–218. https://doi.org/10.6018/reifop.373421

European Comission. (2016). *DigComp 2.0: The Digital Competence Framework for Citizens*. https://publications.jrc.ec.europa.eu/repository/handle/JRC101254

Fernández-Cruz, F., y Fernández-Díaz, M. (2016). Generation z's teachers and their digital skills. *Comunicar*, *24*(46), 97–105. https://doi.org/10.3916/C46-2016-10

Gallego-Arrufat, M. J., Torres-Hernández, N., y 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-Martín, J. y García-Sánchez, J.N. (2017). Pre-service teachers' perceptions of the competence dimensions of digital literacy and of psychological and educational measures. Computers & Education, 107, 54-67. http://dx.doi.org/10.1016/j.compedu.2016.12.010

García-Valcárcel, A., Salvador, L., Casillas, S. y Basilotta, V. (2019). Evaluación de las competencias digitales sobre seguridad de los estudiantes de Educación Básica. *RED. Revista Educación a Distancia*, (61), 1-34. http://dx.doi.org/10.6018/red/61/05

García-Vandewalle García, J.M., García-Carmona, M., Trujillo Torres, J.M. y Moya-Fernández, P. (2023). Analysis of digital competence of educators (DigCompEdu) in teacher trainees: the context of Melilla, Spain. *Technology, Knowledge and Learning 28*, 585–612. https://doi.org/10.1007/s10758-021-09546-x

Grande-de-Prado, M., Cañón-Rodríguez, R., y García-Martín, S. (2020). Seguridad digital, ¿cómo se perciben los docentes en formación? *International Journal of Educational Research and Innovation (IJERI), 14*, 265-275. https://doi.org/10.46661/ijeri.3983

Hernández, R., Fernández, C. y Baptista, P. (2016). *Metodología de la investigación* (6a edición). México: McGraw-Hill – Interamericana de México.

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). *Marco de Referencia de la Competencia Digital Docente.* http://aprende.intef.es/sites/default/files/2023-02/MRCDD_V06B_GTTA.pdf

Jiménez-Hernández, D., González-Calatayud, V., Torres-Soto, A., y Martínez Mayoral, A.; Morales, J. (2020). Digital competence of future secondary school teachers: Differences according to gender, age, and branch of knowledge. *Sustainability, 12,* 9473. https://doi.org/10.3390/su12229473

Latorre-Medina, M. J., y Fuentes Amaya, M. J. (2022). La formación en el área de seguridad digital en las instituciones de educación superior: ¿qué piensan los futuros docentes? In *La*

formación en el área de seguridad digital en las instituciones de educación superior: ¿qué piensan los futuros docentes? (p. 114-119).

Latorre-Medina, M. J., y Tnibar-Harrus, C. (2023). Digital Security in Educational Training Programs: A Study based on Future Teachers' Perceptions. *Inf. Tech. Learn. Tools, 95*, 102-111. https://doi.org/10.33407/itlt.v95i3.5204

Martínez-Garcés, J., y Garcés-Fuenmayor, J. (2020). Competencias digitales docentes y el reto de la educación virtual derivado de la covid-19: Digital teaching competences and the challenge of virtual education arising from COVID-19. *Educación y humanismo*, *22*(39), 1-16. https://doi.org/10.17081/eduhum.22.39.4114

Ortega-Sánchez, D., Gómez-Trigueros, I. M., Trestini, M., y Pérez-González, C. (2020). Self-perception and training perceptions on teacher digital competence (TDC) in Spanish and French university students. *Multimodal Technologies and Interaction*, *4*(4), 74. https://doi.org/10.3390/mti4040074

Ramírez-Montoya, M. S., Mena, J., y Rodríguez-Arroyo, J. A. (2017). In-service teachers' self-perceptions of digital competence and OER use as determined by a xMOOC training course. *Computers in Human Behavior*, *77*, 356-364. https://doi.org/10.1016/j.chb.2017.09.010

Salas-Morera, L., Ruiz-Bustos, R., Cejas-Molina, M. A., Olivares-Olmedilla, J. L., García-Hernández, L., y Palomo-Romero, J. M. (2021). Understanding why women don't choose engineering degrees. *International Journal of Technology and Design Education*, *31*, 325-338. https://doi.org/10.1007/s10798-019-09550-4

Singar, A. V., y Akhilesh, K. B. (2020). Role of cyber-security in higher education. *Smart Technologies: Scope and Applications*, 249-264. https://doi.org/10.1007/978-981-13-7139-4_19

Tárraga-Mínguez, R., Suárez-Guerrero, C., y Sanz-Cervera, P. (2021). Digital teaching competence evaluation of pre-service teachers in Spain: a review study. *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje*, *16*(1), 70-76. https://doi.org/10.1109/RITA.2021.3052848

6. CONCLUSIONES

En este epígrafe se recogen las conclusiones de cada una de las publicaciones que forman el conjunto de la tesis y, también, las conclusiones generales de la investigación. Además, se incluyen las limitaciones que han ido surgiendo durante el desarrollo del trabajo y la prospectiva del mismo, esto es, las futuras líneas de trabajo de la investigación. La finalidad es poder realizar mejores futuras intervenciones en cuanto a seguridad digital en la etapa educativa de Educación Superior en general, y en los estudiantes de educación en particular, para que así el nivel de competencia digital incluyendo el de seguridad aumenten en toda la población.

Objetivo general de la tesis doctoral: Analizar el grado de competencia digital en el área de seguridad, los riesgos asociados y el grado de implementación de dicha competencia en el alumnado de educación.

La seguridad digital supone una parte esencial de la competencia digital para que esta pueda desarrollarse de la manera más adecuada, así esta área aborda la protección de todo lo relacionado con el empleo de la competencia digital (protección de dispositivos, protección de la identidad y los datos personales, protección de la salud y el bienestar personal y protección del medio ambiente). Este aspecto en la etapa de Educación Superior y más en estudiantes de educación, es decir, futuros docentes, resulta imprescindible dentro de su formación y ejercicio profesional. La aplicación de diferentes investigaciones a este respecto y, por último, de test estadísticos han arrojado que la seguridad digital está presente dentro de los estudiantes de educación, aunque hay subáreas que deben ser más trabajadas y desarrolladas y hay que tener en cuenta aspectos como el sexo de los usuarios para saber qué elementos son los que hay que desarrollar más. Por lo tanto, aunque este trabajo solo analiza el grado de esta competencia sin ahondar en las causas de este nivel que se muestra, lo que se pretende es invitar a reflexionar a los lectores sobre la necesidad de otorgarle a la seguridad digital una importancia mayor dentro de los programas de formación. Tras esto, se pone el foco en la necesidad de apostar por un papel más relevante no solo de la competencia digital en general, si no de tener en cuenta todas sus áreas para que vayan de la mano y se desarrollen a la misma velocidad y que así esta sea lo más eficaz posible. La finalidad última siempre va a ser que los futuros docentes tengan asimilada la competencia digital en un alto nivel para que puedan incluirla en los procesos de enseñanza-aprendizaje para con sus futuros estudiantes.

Primera publicación: Conocer el concepto de seguridad digital, a qué marco teórico y legislativo pertenece Caracterización del término y trabajo de esta desde el área educativa.

Tras la profunda revisión bibliográfica realizada se llega a la conclusión de que la competencia digital es primordial en el área educativa en el momento presente. Además, esto va a seguir siéndolo pues todos los elementos relacionados con la digitalización van cambiando y actualizándose constantemente.

Siguiendo con la competencia digital en su conjunto, es fundamental conocer la existencia de diferentes marcos de referencia pues estos abalan su importancia, su vigencia y ayudan a toda la población a formarse a este respecto.

En cuanto al área de seguridad digital se resalta la importancia de trabajarla de manera específica y no solo asociada a las demás áreas, pues son demasiadas las desventajas que se derivan de un mal uso de la competencia digital a causa de no tener una suficiente formación en seguridad digital.

Segunda publicación: Exponer el rendimiento y producción de la literatura sobre "cyberbullying". Precisar le evolución científica del concepto de estudio. Determinar las temáticas más relevantes en el campo de estudio sobre el concepto. Establecer los autores más notables en la literatura sobre el término que se estudia.

El análisis bibliométrico en este estudio revela que una de las temáticas más import6es dentro de la seguridad digital es el ciberbullying. En esta misma línea, se demuestra cómo la temática se centra en los adolescentes y en la necesidad de intervenir cuando se produce este fenómeno.

Por otro lado, muchas de las investigaciones a este respecto se centran en el desarrollo de instrumentos que permitan detectar casos de ciberbullying. Los estudios también ponen el foco en la diferencia existente entre sexos cuando se da este problema.

Por último, los estudios ponen de manifiesto que la edad de incidencia de este fenómeno está descendiendo lo que supone que la investigación a este respecto ponga ahora el foco en etapas educativas más tempranas.

Se determina entonces que esta temática dentro de la seguridad digital es una temática joven e irregular. La comunidad educativa va oscilando dentro de la temática sobre diferentes puntos relevantes haciendo que las investigaciones relativas a este problema no sigan una línea de producción científica regular.

Tercera publicación: Obtener una panorámica integral de la situación actual, a fin de desarrollar recomendaciones y pautas para mejorar la seguridad digital en el contexto educativo superior.

De la revisión sistemática realizada se llega a la conclusión de que existen unas corrientes y temáticas principales que son las que se abordan mayoritariamente. A nivel general la corriente que más destaca es la búsqueda y desarrollo de soluciones y mejores prácticas en el ámbito de la seguridad digital. Sin embargo, de manera más específica hay tres áreas que engloban la mayor parte de la producción científica.

Por un lado, todas las investigaciones referidas a niños y jóvenes y cómo la digitalización afecta a los mecanismos de seguridad que tienen, exponiendo tanto los aspectos positivos de la tecnología como los negativos.

Por otro lado, se establece siempre que el cyberbullying es uno de los mayores problemas en los adolescentes y este se da por la suma de dos factores, en primer lugar, por un amplio uso de la tecnología pero que va de la mano con una falta de formación en seguridad digital.

En último lugar, se destacan diferencias sustanciales en varias investigaciones en cuanto al comportamiento digital de las personas dependiendo de factores como el sexo o la edad de los usuarios.

De igual modo, se demuestra cómo la seguridad digital en educación es una temática con un crecimiento y evolución constantes con una gran producción científica y una gran variedad de enfoques.

Cuarta publicación: Determinar el efecto global y particular de todas las investigaciones analizadas sobre la seguridad digital en estudiantes de Educación Superior.

Se confirma la correlación positiva existente entre las dos variables de estudio, en este caso la seguridad digital y la etapa de Educación Superior. Además, este metaanálisis da respuesta a interrogantes sobre si en las publicaciones sobre esta temática se habla del nivel de seguridad digital de los discentes en esta etapa, al igual que si la seguridad se trabaja como contenido propio. En el primer caso, las investigaciones establecen que sí existe un cierto nivel en cuanto a seguridad en los estudiantes, pero, sin embargo, no es porque se trabaje como tal en los diferentes programas formativos, si no que se trabaja siempre desde una perspectiva transversal y siempre asociada a otros contenidos o materias.

Además, se confirma que mayoritariamente las publicaciones al respecto del tema tratado solo publican resultados positivos, lo que puede significar dos cosas: que en aquellos lugares donde se trabaja el aspecto de la seguridad digital el nivel que consiguen siempre es alto y positivo, o que los resultados negativos no se publiquen.

Quinta publicación: Conocer e interpretar cuál es el grado de conocimiento y aplicación de buenos mecanismos sobre seguridad en todas las subáreas de esta.

Por medio de la aplicación del cuestionario ya validado (García-Valcárcel, et al., 2019) en el estudiantado de titulaciones de educación de la Universidad de Granada y atendiendo a los resultados obtenidos, se afirma que la seguridad digital es un elemento que está presente en la competencia digital de estos estudiantes, así como en su formación. De igual manera, se ha reafirmado que existen unos elementos o aspectos de esta área más desarrollados que otros. Así, es la subárea 4, referida a la protección del medio ambiente, la menos desarrollada y trabajada en la formación en estas titulaciones. Mientras que la más desarrollada y de la que más conocimiento tienen es la subárea 3, protección de la salud y el bienestar personal.

Estas diferencias quedan más patentes sobre todo cuando se distingue por sexos y según la subárea que se esté analizando. Por ejemplo, en cuanto a la protección de los dispositivos y la protección de la salud y del bienestar personal son los hombres los que obtienen puntuaciones más altas haciendo así que sus puntuaciones totales de toda el área de seguridad aumenten.

Por otro lado, se destaca que no existen diferencias significativas entre las puntuaciones obtenidas y la edad de los usuarios dentro de las titulaciones de educación.

6.1.Limitaciones

La principal limitación de este trabajo es referente al tamaño de la muestra de la investigación principal, debido al tamaño no se pueden extraer conclusiones que se extrapolen a otros contextos y otras poblaciones. En esta misma línea, la elección de la muestra, en este caso por muestreo por conveniencia es otra de las principales limitaciones del estudio.

Por otro lado, al tratarse de un estudio cuantitativo de corte transversal, exploratorio, descriptivo y correlacional puede verse envuelto en el debate de si existen verdaderamente relaciones causales entre las áreas estudiadas. Lo que se quiere destacar entonces a través de este trabajo de tesis doctoral es que se trata de un análisis que se basa en la descripción de una realidad concreta observada sin pretensión de realizar afirmaciones a través de la inferencia causal.

6.2.Futuras líneas de investigación

En lo que respecta a las líneas futuras de investigación a partir del trabajo que aquí se presenta, se defiende la necesidad de seguir estudiando el nivel de competencia en seguridad digital del estudiantado de educación. Con esto se pretende abordar otros contextos, otras instituciones para comprobar si estos resultados son extrapolables a más instituciones de Educación Superior y, por lo tanto, este elemento está presente ya de manera permanente en esta etapa. Del mismo modo, conocer las causas de por qué el nivel es el que es y por qué hay subáreas menos desarrolladas que otras sería un paso importante en la investigación relativa a esta temática. Asimismo, conocer las causas de las diferencias significativas entre las puntuaciones de hombres y mujeres abre un amplio campo de investigación a este respecto. En este caso sería importante diseñar investigaciones de carácter mixto que conjuguen la parte cuantitativa con la cualitativa y así poder conocer las autopercepciones de los estudiantes de primera mano.

Finalmente, como última reflexión sobre futuros trabajos relacionados con la tesis doctoral, resulta adecuado pensar en una futura revisión y análisis de los títulos de educación de la Universidad de Granada para una posterior propuesta de formación complementaria en torno a la competencia digital del estudiantado de educación y, más concretamente, en torno a la formación en seguridad digital. Esto podría adquirir aún más solidez científica si se compara con aquellas demandas de la sociedad y de la labor de los docentes en los centros educativos y se compara con aquello que se ofrece dentro de las aulas universitarias.

7. CONCLUSIONS

This section contains the conclusions of each of the publications that make up the thesis as a whole, as well as the general conclusions of the research. It also includes the limitations that have arisen during the development of the work and its prospective, i.e. the future lines of work of the research. The aim is to be able to carry out better future interventions in terms of digital security in the educational stage of Higher Education in general, and in education students in particular, so that the level of digital competence, including security, increases in the whole population.

General objective of the doctoral thesis: To analyse the degree of digital competence in the area of security, the associated risks and the degree of implementation of this competence in education students.

Digital security is an essential part of digital competence so that it can be developed in the most appropriate way, so this area addresses the protection of everything related to the use of digital

competence (protection of devices, protection of identity and personal data, protection of health and personal well-being and protection of the environment). This aspect in Higher Education, and more so in education students, i.e., future teachers, is essential in their training and professional practice. The application of different research in this regard and, finally, statistical tests have shown that digital security is present among education students, although there are sub-areas that need to be worked on and developed further and aspects such as the gender of users must be considered in order to know which elements need to be developed further. Therefore, although this work only analyses the degree of this competence without delving into the causes of the level shown, the aim is to invite readers to reflect on the need to give digital security greater importance in training programmes. After this, the focus is placed on the need to focus on a more relevant role not only for digital competence in general, but also to consider all its areas so that they go hand in hand and develop at the same speed and thus be as effective as possible. The aim will always be for future teachers to have assimilated digital competence at a high level so that they can include it in the teaching-learning processes for their future students.

First publication: Knowing the concept of digital security, to which theoretical and legislative framework it belongs Characterisation of the term and work of this from the educational area.

After a thorough review of the literature, it was concluded that digital competence is of paramount importance in education at the present time. Moreover, this will continue to be the case as all the elements related to digitalisation are constantly changing and updating.

In the area of digital competence, it is essential to be aware of the existence of different reference frameworks as they support its importance, its relevance and help the whole population to be educated in this respect.

Regarding the area of digital security, the importance of working on it specifically and not only associated with the other areas is highlighted, as there are too many disadvantages arising from the misuse of digital competence due to insufficient training in digital security.

Second publication: To expose the performance and production of the literature on "cyberbullying". To clarify the scientific evolution of the concept under study. To determine the most relevant topics in the field of study on the concept. To establish the most notable authors in the literature on the term under study.

The bibliometric analysis in this study reveals that one of the most important topics within digital security is cyberbullying. Along the same lines, it shows how the topic focuses on adolescents and the need to intervene when this phenomenon occurs.

On the other hand, much of the research in this respect focuses on the development of tools to detect cases of cyberbullying. Studies also focus on the gender gap when cyberbullying occurs.

Finally, studies show that the age of incidence of this phenomenon is decreasing, which means that research in this area is now focusing on earlier educational stages.

It is therefore clear that this issue of digital safety is a young and irregular one. The educational community is oscillating within the subject on different relevant points, which means that research on this problem does not follow a regular line of scientific production.

Third publication: To obtain a comprehensive overview of the current situation in order to develop recommendations and guidelines for improving digital security in the higher education context.

From the systematic review carried out, it can be concluded that there are a number of main currents and themes that are the ones that are mostly addressed. At a general level, the most prominent trend is the search for and development of solutions and best practices in the field of digital security. However, more specifically, there are three areas that encompass most of the scientific production.

On the one hand, all research referring to children and young people and how digitalisation affects their safety mechanisms, exposing both the positive aspects of the technology and the negative ones.

On the other hand, it is always established that cyberbullying is one of the biggest problems in adolescents and this is due to the sum of two factors, firstly, due to a wide use of technology but which goes hand in hand with a lack of training in digital safety.

Lastly, substantial differences are highlighted in various research studies in terms of people's digital behaviour depending on factors such as the sex or age of the users.

Similarly, it shows how digital security in education is a subject with a constant growth and evolution with a large scientific production and a wide variety of approaches.

Fourth publication: To determine the overall and particular effect of all the research analysed on digital safety in higher education students.

The positive correlation between the two study variables, in this case digital safety and the higher education stage, is confirmed. In addition, this meta-analysis provides answers to questions about whether the publications on this topic discuss the level of digital safety of students at this stage, as well as whether safety is worked on as its own content. In the first case, the research establishes that there is a certain level of security among students, but, however, this is not because it is worked on as such in the different training programmes, but rather because it is always worked on from a transversal perspective and always associated with other content or subjects.

Furthermore, it is confirmed that many publications on the subject only publish positive results, which could mean two things: that in those places where digital security is addressed, the level achieved is always high and positive, or that the negative results are not published.

Fifth publication: To find out and interpret the degree of knowledge and application of good security mechanisms in all the subareas of security.

Through the application of the already validated questionnaire (García-Valcárcel, et al., 2019) in the students of education degrees at the University of Granada and according to the results obtained, it is affirmed that digital security is an element that is present in the digital competence of these students, as well as in their training. Similarly, it has been reaffirmed that there are some elements or aspects of this area that are more developed than others. Thus, sub-area 4, referring to the protection of the environment, is the least developed and worked on in the training of these degrees. The most developed and the one they are most aware of is sub-area 3, protection of health and personal wellbeing.

These differences become more evident especially when distinguishing by gender and according to the sub-area being analysed. For example, in terms of protection of devices and protection of personal health and well-being, it is men who obtain higher scores, thus increasing their overall scores for the whole area of security.

On the other hand, it should be noted that there are no significant differences between the scores obtained and the age of the users within the educational qualifications.

7.1.Limitations

The main limitation of this work relates to the size of the sample of the main research. Due to its size, it is not possible to draw conclusions that can be extrapolated to other contexts and

other populations. Along the same lines, the choice of the sample, in this case by convenience sampling, is another of the main limitations of the study.

On the other hand, as this is a quantitative, cross-sectional, exploratory, descriptive and correlational study, it may be involved in the debate as to whether there are truly causal relationships between the areas studied. The aim of this doctoral thesis is to highlight the fact that it is an analysis based on the description of a concrete observed reality without the pretension of making affirmations through causal inference.

7.2.Future lines of research

Regarding future lines of research based on the work presented here, the need to continue studying the level of digital security competence of education students is advocated. The aim is to address other contexts, other institutions, to check whether these results can be extrapolated to other Higher Education institutions and, therefore, whether this element is already present permanently at this stage. In the same way, knowing the reasons why the level is the way it is and why some sub-areas are less developed than others would be an important step in research on this subject. Similarly, understanding the causes of the significant differences between the scores of men and women opens up a wide field of research in this respect. In this case, it would be important to design mixed research that combines quantitative and qualitative research to learn about students' self-perceptions at first hand.

Finally, as a last reflection on future work related to the doctoral thesis, it is appropriate to think about a future review and analysis of the education degrees of the University of Granada for a subsequent proposal of complementary training around the digital competence of education students and, more specifically, around training in digital security. This could become even more scientifically sound if it is compared with the demands of society and the work of teachers in educational centres and compared with what is offered in university classrooms.

8. REFERENCIAS BIBLIOGRÁFICAS

Agencia Estatal de Protección de Datos (AEPD). (2019). *Guía para Centros Educativos.* https://www.aepd.es/documento/guia-centros-educativos.pdf

Ala-Mutka, K., Punie, Y., y Redecker, C. (2008). Digital competence for lifelong learning. *Institute for Prospective Technological Studies (IPTS), European Commission, Joint Research Centre. Technical Note: JRC, 48708*, 271-282.

Alvarez-Flores, E. P. (2021). Uso crítico y seguro de tecnologías digitales de profesores universitarios. *Formación universitaria*, *14*(1), 33-44. http://dx.doi.org/10.4067/S0718-50062021000100033

Álvarez-Flores, E. P., Núñez-Gómez, P., y Crespo, C. R. (2017). Adquisición y carencia académica de competencias tecnológicas ante una economía digital. *Revista latina de comunicación social*, (72), 540-559. https://doi.org/10.4185/RLCS-2017-1178

Anderson, J.M. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308-313. https://doi.org/10.1016/S0167-4048

Area-Moreira, M., Borrás-Machado, J. F., y San Nicolás-Santos, B. (2015). Educar a la generación de los Millennials como ciudadanos cultos del Ciberespacio. *Revista de estudios de juventud*, *109*, 13-32.

Barrow, C., y Heywood-Everett, G. (2006). *E-safety: The experience of English educational establishments: Summary and recommendations*. British Educational Communications and Technology Agency (BECTA). https://bit.ly/2Gz6aoD

Boletín Oficial del Estado núm. 106, de 04 de mayo de 2006. *Ley Orgánica 2/2006, de 3 de mayo, de Educación.* https://www.boe.es/buscar/pdf/2006/BOE-A-2006-7899-consolidado.pdf

Boletín Oficial del Estado núm. 294, de 06 de diciembre de 2018. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Buendía Eisman, L., Colás Bravo, M.P., y Hernández Pina, F. (1998). *Métodos de investigación en psicopedagogía*. McGraw-Hill: Madrid.

Cabero-Almenara, J., Barragán Sánchez, R., y Palacios Rodríguez, A. D. P. (2021). DigCompOrg: Marco de referencia para la transformación digital de los centros educativos andaluces. *eCO. Revista Digital de Educación y Formación del Profesorado, 18, 1-21.*

Cabero-Almenara, J., Barroso-Osuna, J., Rodríguez-Gallego, M., y Palacios-Rodríguez, A. (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., y Martínez, A. (2019). Information and Communication Technologies and initial teacher training. Digital models and competences. *Profesorado*, *23*(3), 247-268.

Cabezas, M., Casillas, S. y Pinto, A.M. (2014). Percepción de los alumnos de Educación Primaria de la Universidad de Salamanca sobre su competencia digital. *EDUTEC, Revista Electrónica de Tecnología Educativa*, 48, 1-14 https://doi.org/10.21556/edutec.2014.48.156

Cantón, I., Cañón, R. y Grande, M. (2017). La comunicación como subdimensión de la competencia digital en futuros maestros de Educación Primaria. *Pixel-Bit: Revista de medios y educación*, *48*, 33-47. http://dx.doi.org/doi.org/10.12795/pixelbit.2017.i50.02

Carabel, T. C., Meneghel, I., Martínez, N. O., y García, S. A. (2020). Nuevos retos asociados a la tecnificación laboral: el tecnoestrés y su gestión a través de la Psicología Organizacional Positiva. *Aloma: revista de psicologia, ciències de l'educació i de l'esport Blanquerna*, *38*(1), 21-30. https://doi.org/10.51698/aloma.2020.38.1.21-30

Castillejos López, B., Torres Gastelú, C. A., y Lagunes Domínguez, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura (Guadalajara, Jal.)*, *8*(2), 54-69. http://dx.doi.org/10.18381/Ap.v8n2.914

Chou, C., y Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education*, *14*(1), 44-53. https://doi.org/10.1016/j.iheduc.2010.03.006

D'Antonio, G., y de Lima Pancorbo, M. (2019). Digital Security en la nueva era de transformación digital. *Análisis del Real Instituto Elcano (ARI)*, (32), 1.

De Waal, E., y Grösser, M. (2014). On safety and security in education: Pedagogical needs and fundamental rights of learners. *Educar*, *50*(2), 0339-361. https://doi.org/10.5565/rev/educar.44

Dodel, M., y Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, *21*(5), 712-728. https://doi.org/10.1080/1369118X.2018.1428652

EDUCASE. (2022). *Horizon Report. Teaching and Learning Edition*. https://library.educause.edu/resources/2022/4/2022-educause-horizon-report-teaching-and-learning-edition

European Commission. Joint Research Centre, Brande, L., Carretero, S., Vuorikari, R. (2016). *DigComp 2.0: the digital competence framework for citizens*, Publications Office. https://data.europa.eu/doi/10.2791/11517

European Commission. Joint Research Centre, 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. https://data.europa.eu/doi/10.2760/38842

European Commission. Joint Research Centre, Punie, Y., Ferrari, A., Brečko, B. (2013). *DIGCOMP: a framework for developing and understanding digital competence in Europe*, (Y.Punie,editor,B.Brečko,edito) Publications Office. https://data.europa.eu/doi/10.2788/52966

European Commission, Joint Research Centre, Redecker, C., Punie, Y. (2017). *European framework for the digital competence of educators: DigCompEdu*, (Y.Punie,edito) Publications Office. https://data.europa.eu/doi/10.2760/159770

European Commission, Joint Research Centre, Vuorikari, R., Kluzer, S., Punie, Y. (2022). *DigComp 2.2, The Digital Competence framework for citizens: with new examples of knowledge, skills and attitudes*, Publications Office of the European Union. https://data.europa.eu/doi/10.2760/115376

Gallego-Arrufat, M. J., Torres-Hernández, N., y 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

Gamito Gómez, R., Aristizabal Llorente, P., Vizcarra Morales, M. T., y León Hernández, I. (2020). Digital safety and protection of children: Challenges of the 21st-century school. *Educar, 56*(1), 519-237. https://doi.org/10.5565/rev/educar.1113

García-Martín, J. y García-Sánchez, J.N. (2017). Pre-service teachers' perceptions of the competence dimensions of digital literacy and of psychological and educational measures. *Computers & Education, 107*, 54-67. http://dx.doi.org/10.1016/j.compedu.2016.12.010

García-Ruiz, R., y Escoda, A. P. (2021). La competencia digital docente como clave para fortalecer el uso responsable de Internet. *Campus virtuales, 10*(1), 59-71.

García-Valcárcel, A., Salvador, L., Casillas, S. y Basilotta, V. (2019). Evaluación de las competencias digitales sobre seguridad de los estudiantes de Educación Básica. *RED. Revista Educación a Distancia*, (61), 1-34. http://dx.doi.org/10.6018/red/61/05

García Vélez, K. A., Ortiz Cárdenas, T., y Chávez Loor, M. D. (2021). Relevancia y dominio de las competencias digitales del docente en la educación superior. *Revista Cubana de Educación Superior*, *40*(3).

Garmendia, M., Jiménez, E., Casado, M.A. y Mascheroni, G. (2016). Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015). https://addi.ehu.es/bitstream/handle/10810/21546/Informe%20NCGM%20Espa%C3%B1a%202010-2015.pdf?sequence=1

Garzón Artacho, E., Martínez, T. S., Ortega Martin, J. L., Marin Marin, J. A., y Gomez Garcia, G. (2020). Teacher training in lifelong learning—The importance of digital competence in the encouragement of teaching innovation. *Sustainability*, *12*(7), 2852. https://doi.org/10.3390/su12072852

Ghislieri, C., Dolce, V., Sanseverino, D., Wodociag, S., Vonthron, A. M., Vayre, É., ... y Molino, M. (2022). Might insecurity and use of ICT enhance internet addiction and exhaust people? A study in two European countries during emergency remote working. *Computers in Human Behavior*, *126*, 107010. https://doi.org/10.1016/j.chb.2021.107010

Grande-de-Prado, M., Cañón-Rodríguez, R., y García-Martín, S. (2020). Seguridad digital, ¿cómo se perciben los docentes en formación? *International Journal of Educational Research and Innovation (IJERI)*, *14*, 262-275. https://doi.org/10.46661/ijeri.3983

Gros, B. (2016). The dialogue between emerging pedagogies and emerging technologies. *The future of ubiquitous learning: Learning designs for emerging pedagogies*, 3-23.

INTEF. Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado. (2017). *Marco Común de Competencia Digital Docente. Octubre 2017.* http://educalab.es/documents/10180/12809/Marco+competencia+digital+docente+2017/afb07987-1ad6-4b2d-bdc8-58e9faeeccea

INTEF. Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado. (2022). *Marco De Referencia de la Competencia Digital Docente. Enero 2022.* https://aprende.intef.es/sites/default/files/2023-02/MRCDD_V06B_GTTA.pdf

INTEF. Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado. (2013). *Plan de Cultura Digital en la Escuela.* https://intef.es/Noticias/plan-de-cultura-digital-en-la-escuela/

Kesharwani, A. (2020). Do (how) digital natives adopt a new technology differently than digital immigrants? A longitudinal study. *Information & Management*, *57*(2), 103170. https://doi.org/10.1016/j.im.2019.103170

Latorre-Medina, M. J., y 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

Lemus, M. (2017). Jóvenes frente al mundo: Las tecnologías digitales como soporte de la vida cotidiana. *Revista Latinoamericana de Ciencias Sociales, Niñez y Juventud*, *15*(1), 161-172. http://dx.doi.org/10.11600/1692715x.1510902022016

Limas Suárez, S. J., y Vargas Soracá, G. (2020). Redes sociales como estrategia académica en la educación superior: ventajas y desventajas. *Educación y Educadores*, *23*(4), 559-574. https://doi.org/10.5294/edu.2020.23.4.1

López Berlanga, M. C., y Sánchez Romero, C. (2019). La interacción y convivencia digital de los estudiantes en las redes sociales. *Revista de Educación Inclusiva, 12*(2), 114-130.

López-Gil, M. y Bernal-Bravo, C. (2019). El perfil del profesorado en la Sociedad Red: reflexiones sobre las competencias digitales de los y las estudiantes en Educación de la Universidad de Cádiz. *International Journal of Educational Research and Innovation (IJERI), 11,* 83-100.

Manassero-Mas, M. A., y Vázquez Alonso, Á. (2020). Desarrollo curricular de las competencias clave: su evaluación para el aprendizaje desde la normativa educativa. *Enseñanza & Teaching*, *38*(1), 29-48. https://doi.org10.14201/et20203812948

Martínez-Garcés, J., y Garcés-Fuenmayor, J. (2020). Competencias digitales docentes y el reto de la educación virtual derivado de la covid-19: Digital teaching competences and the challenge of virtual education arising from COVID-19. *Educación y humanismo*, *22*(39), 1-16. https://doi.org/10.17081/eduhum.22.39.4114

Matienzo López, R. (2020). Percepciones de docentes sobre el aprendizaje móvil en Educación Superior. *Educación Superior*, *7*(2), 37-48.

Ministerio de Asuntos Económicos y Transformación Digital. (2026). *España digital 2026.* https://espanadigital.gob.es/encuentra-tu-programa

Mladenović, M., Ošmjanski, V., y Stanković, S. V. (2021). Cyber-aggression, cyberbullying, and cyber-grooming: a survey and research challenges. *ACM Computing Surveys (CSUR)*, *54*(1), 1-42. https://doi.org/10.1145/3424246

Moreno Rodríguez, M., Gabarda Méndez, V., y Rodríguez Martín, A. (2018). Alfabetización informacional y competencia digital en estudiantes de Magisterio. *Profesorado, Revista De Currículum Y Formación Del Profesorado, 22*(3), 253-270. https://doi.org/10.30827/profesorado.v22i3.8001

Muñoz-Rodríguez, J. M., Torrijos Fincias, P., Serrate González, S., y Murciano Hueso, A. (2020). Entornos digitales, conectividad y educación. Percepción y gestión del tiempo en la construcción de la identidad digital de la juventud. *Revista Española de Pedagogía*, *78*(277), 457-476. https://doi.org/10.22550/REP78-3-2020-07

Orden ECD/65/2015, de 21 de enero, por la que se describen las relaciones entre las competencias, los contenidos y los criterios de evaluación de la educación primaria, la educación secundaria obligatoria y el bachillerato. https://www.boe.es/boe/dias/2015/01/29/pdfs/BOE-A-2015-738.pdf

Pérez, F., y Vilchez, J. E. (2012). El uso de los videojuegos y redes sociales como predictores de la integración curricular de las TIC en estudiantes de Magisterio. *Sphera Pública,* (12), 199-215.

Pérez, M. O., del Rey Alamillo, R., Walrave, M., y Vandebosch, H. (2020). Sexting en adolescentes: Prevalencia y comportamientos. *Comunicar: Revista científica iberoamericana de comunicación y educación*, *28*(64), 9-19. https://doi.org/10.3916/C64-2020-01

Prensky, M. (2011). *Enseñar a Nativos Digitales.* Madrid: SM.

Ramas Arauz, F. E., Ruiz Torres, A. A., García García, M. A., López González, R., y Martínez Sánchez, M. E. (2015). *TIC en Educación*. Ediciones Díaz de Santos.

Recomendación 2006/962/CE del Parlamento Europeo y del Consejo, de 18 de diciembre de 2006, sobre las competencias clave para el aprendizaje permanente. http://europa.eu/legislation_summaries/education_training_youth/lifelong_learning/c11090_es.htm

Reigada, A. T. (2018). Del principio de seguridad de los datos al derecho a la seguridad digital. *Economía industrial*, *410*, 127-151.

Restrepo-Palacio, S., y Segovia Cifuentes, Y. M. (2020). Diseño y validación de un instrumento de evaluación de la competencia digital en Educación Superior. *Ensaio: Avaliação e Políticas Públicas em Educação, 28*(109), 932-961. https://doi.org/10.1590/s0104-40362020002801877

Rodríguez García, A. M., Martínez Heredia, N., y Raso Sánchez, F. M. (2017). La formación del profesorado en competencia digital: clave para la educación del siglo XXI. *Revista Internacional de Didáctica y Organización Educativa*, 46-65.

Rodríguez-García, A. M., Raso Sanchez, F., y Ruiz-Palmero, J. (2019). Digital competence, higher education and teacher training: a meta-analysis study on the Web of Science. *Pixel-BIT-Revista de Medios y Educación*, (54), 65-81.

Suárez-Guerrero, C., Lizandra, J., y Ros-Garrido, A. (2019). Análisis pedagógico de la competencia digital docente en la educación técnico profesional. *EDUTEC*, 701-707.

Schwartz, T. J., y Lonborg, S. D. (2011). Security management in telepsychology. *Professional Psychology: Research and Practice, 42*(6), 419. https://doi.org/10.1037/a0026102

Tárraga-Mínguez, R., Suárez-Guerrero, C., y Sanz-Cervera, P. (2021). Digital teaching competence evaluation of pre-service teachers in Spain: a review study. *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje*, *16*(1), 70-76.

Vargas-Murillo, G. (2019). Competencias digitales y su integración con herramientas tecnológicas en educación superior. *Cuadernos Hospital de clínicas*, *60*(1), 88-94.

Vidal, E. A. (2021). Las consecuencias de un mal uso de las redes sociales en los adolescentes. *Revista de Formación Continuada de la Sociedad Española de Medicina de la Adolescencia*, *9*(2), 46-53.

Walrave, M., y Heirman, W. (2011). Cyberbullying: Predicting victimisation and perpetration. *Children & Society*, *25*(1), 59-72. https://doi.org/10.1111/j.1099-0860.2009.00260.x

9. ANEXOS

Cuestionario

Cuestionario de evaluación de las competencias digitales de seguridad de los estudiantes universitarios de educación.

Antes de comenzar tenga en cuenta las siguientes CONDICIONES:

1. Se solicita su participación voluntaria.

2. No se recoge información privada. Los datos se utilizarán con carácter académico y científico. Igualmente, cualquier información se gestionará de acuerdo a la normativa vigente.

Instrucciones: Para responder al cuestionario, BASTA CON MARCAR CON UNA SOLA "X" LA RESPUESTA QUE MEJOR SE ADECUE A SU REALIDAD PERSONAL.

Cada pregunta tiene una sola respuesta correcta, por cada respuesta correcta obtendrás un punto de un total de 16 puntos. Al finalizar el cuestionario sabrás cuál es tu nivel de competencia digital en el área de seguridad.

¡Muchas gracias por su colaboración!

* Indica que la pregunta es obligatoria

1. Correo *

A. DATOS DE IDENTIFICACIÓN DE LOS ESTUDIANTES Y LA TITULACIÓN CURSADA

2. Su género es: *

Marca solo un óvalo.

- o Hombre
- o Mujer
- o No binario
- o Prefiero no responder

3. Su edad es: *

_____

4. Universidad a la que pertenece: *

- Universidad de Granada. Campus de Granada
- Universidad de Granada. Campus de Melilla
- Universidad de Granada. Campus de Ceuta

5. Grado que estudia: *

- Grado de Educación Primaria
- Grado de Educación Infantil
- Grado de Pedagogía
- Grado de Educación Social
- Doble Grado en Educación Primaria y Ciencias de la Actividad Física y del Deporte

6. Curso en el que se encuentra: *

- 1º
- 2º
- 3º
- 4º
- 5º (solo para los estudiantes del doble grado) 6º (solo para los estudiantes del doble grado)

B. ÁREA DE SEGURIDAD: PROTECCIÓN DE DISPOSITIVOS

Seleccione la respuesta que más se adecúa a su realidad

7. 1. Cuando mi ordenador, tablet o móvil ha sido infectado por algún virus debo:

a. Pagar un rescate por recuperar la información.

b. Pasar inmediatamente el antivirus

c. Seguir trabajando normalmente como si no hubiera pasado nada

d. Enviar un archivo adjunto a un amigo para avisarle

8. 2. ¿Qué contraseña pondría para proteger mi ordenador, tablet o móvil? *

a. Mi nombre y fecha de nacimiento

b. Mi número de DNI

c. Mi dirección del domicilio

d. Las iniciales de mi cantante favorito y del año que nació

9. 3. Cuando utilizo el ordenador: *

a. De vez en cuando abro el antivirus y examino el disco duro

b. Nunca examino con el antivirus el ordenador

c. No uso antivirus porque nunca lo he necesitado

d. Uso el antivirus sólo para revisar dispositivos externos (ej. pen-drive….).

4. Si pongo una contraseña siempre sigo estas normas: *

a. Que tenga muchos y variados caracteres (mayúsculas, minúsculas, números, símbolos, etc.)

b. Que sea una palabra corta para poderla recordar mejor

c. Que solo tenga minúsculas

d. Que tenga solamente letras

C. ÁREA DE SEGURIDAD: PROTECCIÓN DE DATOS PERSONALES

Seleccione la respuesta que más se adecúa a su realidad

5. Si publico fotos o datos sobre mi familia, como fotos de mi casa, la profesión de mis padres, la calle donde vivo…. en Internet:

a. La información la controlo yo y la puedo borrar cuando quiera.

b. Una vez que publico algo en Internet pierdo el control sobre ello

c. Sólo lo verán mis verdaderos amigos

d. La información no afectará en ningún caso a mi futuro ni al de mi familia

6. Si un compañero de clase descubre la contraseña de mi correo electrónico podría:

a. Enviar mensajes a los profesores haciéndose pasar por mí

b. Leer los mensajes que he recibido de cualquiera de mis contactos

c. Cambiar mi contraseña y no poder ver yo mis propios mensajes

d. Hacer todo lo señalado en las opciones anteriores

7. ¿Cuáles de las siguientes publicaciones no pondría en peligro la protección de mi identidad?

a. Una fotografía en la puerta de mi casa en la que aparece el número y nombre de la calle

b. Una entrada en un blog en el que facilito mi número de teléfono

c. Una fotografía de las vacaciones del último verano

d. Un comentario personal sobre una noticia que he leído

8. En el caso de que hayan etiquetado una foto en una red social sin mi permiso, ¿qué haría para eliminar mi etiqueta?

a. Esperar a que me elimine la persona que me ha etiquetado

b. Enviar un mensaje a la red social para que eliminen mi etiqueta

c. No se pueden eliminar las etiquetas de las fotos una vez que se han puesto

d. Acceder a la imagen etiquetada y borrarla.

D. ÁREA DE SEGURIDAD: PROTECCIÓN DE LA SALUD

9. Para evitar sufrir problemas de acoso a través de Internet: *

a. No me fiaría de personas que no conozco y quieren contactar conmigo

b. No me comunico con nadie si no es presencialmente

c. Considero que no voy a sufrir acoso a través de la Red tal y como soy

d. Utilizo una falsa personalidad en la Red

10. Cuando me conecto con mis amigos para jugar: *

a. Consigo mantener buenas relaciones con ellos, aunque vaya perdiendo en el juego

b. Suelo enfadarme al poco tiempo y abandono el juego formando otro grupo

c. Me termino poniendo nervioso y después no duermo bien

d. Suelen ocurrir situaciones desagradables que nos terminan enfrentando

11. Cuando uso el ordenador, tablet, TV, consola de videojuegos… en mi casa:

a. Me tumbo en el suelo

b. Me siento correctamente en una silla, sofá, sillón, etc.

c. Me terminan doliendo la espalda, piernas o cuello.

d. No tengo una postura concreta y acabo cansado

12. Cuando navego por Internet buscando una información que me interesa:

a. Suelo tardar bastante porque encuentro páginas divertidas con las que me entretengo

b. Voy directamente a la información que necesito para terminar cuanto antes

c. Termino leyendo o viendo vídeos que no tienen nada que ver con la información que buscaba

d. Reviso normalmente muchas páginas, pero no termino de encontrar lo que quiero

E. ÁREA DE SEGURIDAD: PROTECCIÓN DEL ENTORNO

13. . Cambiar frecuentemente de ordenador, tablet, móvil, videoconsola…

a. Tiene un impacto en el medio ambiente por generar basura difícil de reciclar

b. Es necesario cambiar frecuentemente los dispositivos para poder utilizar las nuevas aplicaciones que van saliendo

c. No tiene ningún impacto negativo sobre el medio ambiente

d. No son cuestiones relacionadas con el medio ambiente

14. La fabricación de móviles, tablet y otros dispositivos electrónicos tiene un impacto medioambiental negativo que afecta

a. A todos los países y continentes por igual

b. Solo a los países más desarrollados

c. A los países menos desarrollados

d. A ningún país ni continente

15. Estoy realizando un trabajo en el ordenador y tengo que irme a comer pero aún no lo he terminado

a. Dejo el ordenador encendido porque en poco tiempo volveré a terminar el trabajo

b. Uso la opción “suspender” para ahorrar energía

c. Apago la pantalla y dejo encendido el ordenador

d. Dejo encendido el ordenador sin plantearme nada más

16. Si estoy jugando con un videojuego y me empiezo a sentir nervioso y estresado por el ritmo que el juego me exige:

a. Dejo de jugar para evitar sentirme más nervioso

b. Sigo jugando porque un poco de estrés y nerviosismo sirve para mejorar mi rendimiento en el juego

c. Sigo jugando aunque mi rendimiento sea menor

d. Nunca me plantearía dejar el juego por esa razón