Uso responsable de Internet y seguridad digital: revisión sistemática de programas educativos

Responsible Internet use and digital safety: systematic review on educational programs

Berta Aznar-Martínez
Facultat de Psicologia i Ciències de l'Educació i de l'Esport Blanquerna-Universitat Ramon Llull
C/Císter 34, 08022, Barcelona (España)
bertaam@blanquerna.url.edu
https://orcid.org/0000-0002-1658-5053

Aina Casarramona Basany
Facultat de Psicologia i Ciències de l'Educació i de l'Esport Blanquerna-Universitat Ramon Llull
C/Císter 34, 08022, Barcelona (España)
ainacb@blanquerna.url.edu
https://orcid.org/0000-0002-9740-3572

Jaume Grané-Morcillo
Facultat de Psicologia i Ciències de l'Educació i de l'Esport Blanquerna-Universitat Ramon Llull
C/Císter 34, 08022, Barcelona (España)
jaumegm@blanquerna.url.edu
https://orcid.org/0000-0003-0441-2793

Judith Lorente-De-Sanz
Facultat de Psicologia i Ciències de l'Educació i de l'Esport Blanquerna-Universitat Ramon Llull
C/Císter 34, 08022, Barcelona (España)
judithld@blanquerna.url.edu
https://orcid.org/0000-0002-0703-2801

Miquel-Àngel Prats Fernández
Facultat de Psicologia i Ciències de l'Educació i de l'Esport Blanquerna-Universitat Ramon Llull
C/Císter 34, 08022, Barcelona (España)
miquelpf@blanquerna.url.edu
https://orcid.org/0000-0002-9542-7888

Lluís Ballester Brage
Departament de Pedagogia i Didàctiques Específiques
Universitat de les Illes Balears
Cra. de Valldemossa, km. 7,5, 07122, Palma de Mallorca (España)
lluis.ballester@uib.es
https://orcid.org/0000-0003-1861-7511

Financiación: Proyecto subvencionado por el Institut Balear de la Dona. Realización del estudio sobre Impacto de la Pornografía en la Infancia y la juventud de las Islas Baleares (FUEIB-220204).

CÓMO CITAR ESTE ARTÍCULO
Aznar-Martínez, B., Casarramona Basany, A., Grané-Morcillo, J., Lorente-De-Sanz, J., Prats Fernández, M. A. y Ballester Brage, L. (2024). Uso responsable de Internet y seguridad digital: revisión sistemática de programas educativos. *Estudios sobre Educación*, 47, DOI. https://doi.org/10.15581/004.47.006

ISSN: 1578-7001 / DOI: 10.15581/004.47.006

Resumen: El objetivo de esta revisión sistemática fue analizar los programas educativos que abordan el uso responsable de Internet para gestionar los diversos retos y riesgos del espacio digital. Se utilizaron 5 bases de datos para obtener estudios realizados entre 2017 y 2022. Se analizaron las siguientes variables: población diana, duración, contenido y evaluación. Los programas abordaban los siguientes riesgos en línea: ciberacoso, *sexting*, privacidad digital, *grooming*, suplantación de identidad, información falsa, uso problemático de Internet, *phishing* e ingeniería social, identidad digital, compartir excesiva información, *spam* y fraude. Se ha identificado la necesidad del diseño e implementación de programas que involucren a toda la comunidad educativa y aborden las problemáticas del consumo de pornografía y la seguridad *online*.

Palabras clave: Competencia digital, Seguridad digital, Riesgos digitales, Uso responsable de Internet.

Abstract: The objective of this systematic review was to analyze pre-existing programs that address a responsible use of the Internet with the aim of managing the diverse challenges and risks of the digital space. Five databases were used to obtain studies from 2017 to 2022. The following variables were analyzed: target population, duration, content, and evaluation. Programmes included the following online risks: cyberbullying, sexting, digital privacy, grooming, identity theft, false information, problematic Internet use, phishing and social engineering, digital identity and online reputation, excessive information sharing, spam and and fraud. The need for the design and implementation of programs that involve the entire educational community and address the issues of pornography and online safety has been identified.

Keywords: Digital competence, Digital safety, Digital risks, Responsible use of Internet.

Introducción

El auge de la precocidad de acceso a la tecnología en las nuevas generaciones supone un nuevo reto para los menores de edad, así como para sus familias y educadores. De acuerdo con Unicef, las aplicaciones y las redes sociales forman parte del día a día de las nuevas generaciones y ser capaces de integrarlas de forma armónica en su desarrollo personal y social es, sin duda, un enorme desafío (Andrade *et al.*, 2021). Según un informe de *EU Kids Online* (Smahel *et al.*, 2020), los menores europeos han duplicado su consumo de contenido *online* a través del teléfono móvil respecto al 2010, además de ser cada vez más jóvenes en el primer uso del móvil. De hecho, 9 de cada 10 menores de entre 7 y 12 años tienen un dispositivo con conexión a Internet (Kaspersky, 2019). Además, a causa de la pandemia COVID-19, los menores aumentaron su actividad en línea, lo cual incrementó su vulnerabilidad en lo que respecta a los riesgos que conlleva el uso de Internet (Brossard *et al.*, 2021), de los que muchos no son conscientes (Chaudron *et al.*, 2018). La mayoría de las familias, en concreto el 84%, según un estudio realizado por Kaspersky (2019), están preocupadas por la seguridad *online* de sus hijos e hijas, y el 60% dice haber presenciado alguna dificultad en el entorno familiar en referencia al uso de Internet, pero aun así muestran ciertas resistencias a hablar abiertamente de los retos que puede suponer el uso de las tecnologías. Especialmente, consideran que el contenido sexual o violento es el riesgo más importante para sus hijos e hijas (Brossard *et al.*, 2021).

El acceso a Internet sin restricciones ha hecho que el consumo de pornografía se generalice entre niños/as y adolescentes y este supone, según la Organización Mundial de la Salud (World Health Organization, 2016), una de las mayores amenazas para este colectivo, ya que la pornografía es accesible las 24 horas del día, asequible y, generalmente, se puede acceder a ella de manera anónima (Andrie *et al.*, 2021; Ballester *et al.*, 2023; Stoner y Hugues, 2014; Zohor *et al.*, 2021). Además, estos colectivos se encuentran en una etapa durante la cual se producen las primeras aproximaciones a la sexualidad y a la salud sexual, y uno de los aspectos más preocupantes de la pornografía es que los jóvenes la identifiquen como su principal fuente de educación sexual (Ballester *et al.*, 2021; Román García *et al.*, 2021). Kaspersky (2019) señala en su informe que el 27% de los niños y niñas de entre 7 y 12 años ha visto alguna vez contenido sexual o violento, y el 14% ha recibido mensajes instándolos a cometer actos violentos o sexuales. Por lo que respecta a los adolescentes de entre 13 y 18 años, el 90% ya han estado expuestos a contenido pornográfico (Ballester *et al.*, 2023). Según otro estudio llevado a cabo en el contexto europeo en 2021, el 58,9% de los adolescentes de entre 14 y 15 años han visto pornografía y el 23,6% la consume semanalmente (Andrie *et al.*, 2021).

Además, en su análisis, Hornor (2020) señaló que el 89,9% de las escenas pornográficas contenían actos de agresión, dirigidos en el 94,4% de los casos hacia las mujeres y perpetradas el 70,3% de las veces por hombres. Además, apuntó que las agresiones físicas eran cuatro veces superiores a las verbales. Por lo tanto, la pornografía presenta una imagen cosificada de la mujer y promueve expectativas sexuales poco realistas (Ballester *et al.*, 2021; Román *et al.*, 2021). A su vez, varios estudios han enfatizado las consecuencias que la pornografía *online* tiene para sus consumidores: mayor prevalencia de prácticas de riesgo sexual (Ballester *et al.*, 2021; Román *et al.*, 2021; Zohor *et al.*, 2021), disminución de la satisfacción sexual (Román *et al.*, 2021), aumento de la probabilidad de cometer agresiones sexuales (Andrie *et al.*, 2021; Román *et al.*, 2021), imitación de los actos sexuales de la pornografía (Román *et al.*, 2021), prácticas violentas (Ballester *et al.*, 2021; Hatch *et al.*, 2020), adicción (Ballester *et al.*, 2021; Hornor, 2020), insatisfacción con el propio cuerpo y baja autoestima (más negativa en las mujeres debido al refuerzo del estándar de belleza que promueve la pornografía) (Paslakis *et al.*, 2020) y síntomas depresivos (Román *et al.*, 2021). Estudios recientes, bastante concluyentes (analizados en la revisión sistemática de Mestre *et al.*, 2023), acreditan que no solo hay posibles influencias negativas como consumidor sometido a riesgos, sino también posibles incrementos de la agresividad sexual entre los consumidores de pornografía violenta con frecuencias semanales elevadas.

Más allá del impacto del consumo de pornografía a través de Internet, la ciberviolencia es otra situación de riesgo a la que se enfrentan los menores en el espacio digital. Las nuevas tecnologías de la información y la comunicación (TIC) permiten al agresor la desinhibición del comportamiento y el anonimato, y dificultan su capacidad empática hacia la víctima facilitando así la invasión total de su espacio personal (International Child Development, 2021; Feijóo *et al.*, 2021; Pascual *et al.*, 2020).

Según una encuesta realizada por Save the Children en España a 400 jóvenes, el 40% sufrieron ciberacoso, del cual empezaron a ser víctimas a los 8 o 9 años (Save the Children, 2022). Así, las conductas de acoso en línea más frecuentes consisten principalmente en amenazas, insultos, burlas y difusión de fotografías (Pascual *et al.*, 2020). Las consecuencias en la víctima pueden ir desde sentimientos negativos, baja autoestima y rendimiento escolar, afectación en las relaciones interpersonales, conductas agresivas, depresión y ansiedad, hasta psicosomatizaciones (Rial, 2021).

No solo la pornografía y la ciberviolencia son dos de los retos a los que los jóvenes se enfrentan al estar conectados a Internet, sino que el uso constante de las redes sociales, plataformas y videojuegos conllevan la interacción con otros usuarios, un hecho que puede suponer también alguno de los siguientes riesgos (Aznar-Martínez *et al.*, 2023):

– El *sexting* consiste en el intercambio, producción o publicación de contenido sexual (Pascual *et al.*, 2020), que puede derivar a situaciones de coerción o amenaza conocidas como *sextorsión* cuando se comparten sin el consentimiento de la persona implicada (International Child Development, 2021). El *grooming* es uno de los riesgos de mayor gravedad y se refiere a la práctica en la que una persona adulta establece con un o una menor una relación de confianza, haciéndose pasar por un igual o por una figura de referencia (Childnet, 2021), generalmente con el fin de explotarlo/a u obtener algún beneficio de tipo sexual (Internet Segura for Kids, 2022).

– El uso problemático de Internet es un riesgo relevante porque puede llevar consigo un comportamiento adictivo (Internet Segura for Kids, 2022; Labrador *et al.*, 2018; Pascual *et al.*, 2020). El uso adictivo de los adolescentes a las redes sociales e Internet es una preocupación creciente entre padres, docentes, investigadores y la sociedad en general (Peris *et al.*, 2020).

– Otro reto destacable es la privacidad digital: decidir qué información personal se quiere compartir de manera pública o privada para salvaguardar la intimidad (Observatorio de la Infancia e INCIBE, 2019; Pascual *et al.*, 2020). La suplantación de la identidad, que ocurre cuando una persona se hace pasar por otra, normalmente en el contexto de niños, niñas y adolescentes a través de las redes sociales, es otro riesgo relevante que suele tener como objetivo hacer daño a la víctima, ya que se

puede cometer un delito y acceder a contenido personal (Pascual *et al.*, 2020; Síndic de Greuges, 2022).

– Otro peligro fundamental es el de la ingeniería social y el *phishing*. La ingeniería social se define como el uso de técnicas psicológicas para manipular el comportamiento y conseguir que las personas divulguen datos privados, como por ejemplo datos de acceso o información financiera (Avast, 2023). El *phishing*, por su parte, es un tipo de ingeniería social que consiste en el envío de un correo electrónico en nombre de una entidad legítima, como una institución pública, una red social o un banco, entre otros, para robar información privada y realizar un cargo económico o infectar el dispositivo (INCIBE, 2023).

– También es importante enfatizar y abordar con los más jóvenes la relevancia de la identidad digital como imagen que ofrece Internet sobre los datos personales de la persona, que puede ser positiva o negativa e influir en el futuro desarrollo personal o profesional de la persona (Observatorio de la Infancia e INCIBE, 2019), y la netiqueta digital, que se refiere a las normas de conducta socialmente aceptadas en Internet, es decir, a cómo es debido comportarse en el entorno digital (Avast, 2023).

Cada vez más organismos nacionales e internacionales han empezado a preocuparse por los problemas psicológicos y sociales derivados de estos riesgos del espacio digital, relacionados tanto con el bienestar emocional como con la salud afectivo-sexual de la juventud, por lo que se debe abordar la problemática desde una perspectiva multidisciplinar. Se ha señalado como un factor de protección la actitud crítica en los menores, y para ello las personas adultas que deben transferirles los conocimientos para un uso responsable de Internet han de formarse en competencias digitales (Ballester *et al.*, 2022b; Prats *et al.*, 2018; Rodríguez Román, 2022). En lo que se refiere al ciberacoso, la calidad de las interacciones entre estudiantes, docentes, familias y personal educativo, así como el reflejo de los valores de la escuela en esas relaciones, han sido reconocidos como los principales factores de protección porque favorecen un clima de seguridad escolar. Así pues, la promoción de escuelas seguras a través de la mejoría del clima y la participación activa de toda la comunidad escolar debe formar parte de los programas dirigidos a prevenir e intervenir en el ciberacoso (Ferrer-Cascales *et al.*, 2019).

Tanto los organismos internacionales como la literatura científica destacan la necesidad de abordar el desarrollo de las habilidades digitales en docentes y educadores, ya que éstos carecen aún de los conocimientos necesarios en materia de seguridad digital (Arunkumar y Premalatha, 2021; Aznar-Martínez *et al.*, 2023; Potyrała y Tomczyk, 2021; Silber-Varod *et al.*, 2019). Además, Unicef y *EU Kids Online* (Rial, 2021; Smahel *et al.*, 2020) señalan la necesidad de concienciar no solo

a docentes, sino también a padres y madres, sobre los riesgos y peligros del espacio digital, entre ellos el fácil acceso a la pornografía y las consecuencias del uso irresponsable de Internet, para que las familias cuenten con los recursos para tomar las medidas necesarias (Rodríguez Román, 2022). Finalmente, los menores deben también estar formados en alfabetización digital con el objetivo de fomentar un desarrollo emocional y sexual saludable (Chaudron *et al.*, 2018).

Unicef afirma que, para un abordaje eficaz de esta cuestión, las acciones que se deben implementar son: el desarrollo de guías específicas dirigidas a jóvenes, familias y cuidadores; la protección de los grupos vulnerables, ya que son los que tienen más probabilidades de quedar expuestos a los riesgos de Internet, y la implementación de medidas preventivas contra el abuso y la violencia en el espacio digital (Brossard *et al.*, 2021).

También, en un intento de dar respuesta a esta nueva realidad, ESafety Comissioner (Walsh *et al.*, 2020; Walsh y Wallace, 2021) propuso la creación de currículums formativos basados en la literatura científica y la opinión de expertos en este ámbito. En esa línea, la organización Common Sense (James *et al.*, 2021) diseñó un programa en Estados Unidos y Reino Unido basado en dilemas prácticos con el fin de revitalizar la educación para la ciudadanía digital.

Tal y como hemos podido constatar, la literatura científica muestra la necesidad de diseñar e implementar programas de formación para la comunidad educativa (alumnado, profesorado y familias) en seguridad digital y uso responsable de Internet. Además de las iniciativas que existen a nivel internacional, las evidencias parecen no ser concluyentes y todavía no se dispone de una recopilación de los programas validados que acrediten su eficacia para poder avanzar en el conocimiento y generar nuevos programas.

Aunque los organismos internacionales están lanzando propuestas para hacer frente a la problemática de los riesgos digitales, estas iniciativas todavía no han llegado en su totalidad a la comunidad científica. Las revisiones sistemáticas que se han llevado a cabo en este ámbito se han centrado en: analizar las competencias digitales y la alfabetización digital del profesorado a través de cuestionarios (Torres-Hernández y Gallego-Arrufat, 2022), identificar las áreas de competencia digital en el alumnado de Educación Primaria (Godaert *et al.*, 2022), evaluar la relación entre alfabetización digital y bienestar en los jóvenes (Vissenberg *et al.*, 2022) y estudiar la evolución de la ciudadanía digital (Richardson *et al.*, 2021).

No obstante, existe un estudio que analiza los programas de ciudadanía digital implementados en el contexto de Indonesia que abordan la seguridad digital y, además, el cyberbullying, la pornografía, la desinformación y la adicción al juego y a Internet (Heru *et al.*, 2021). También se han identificado dos revisiones

sistemáticas sobre los programas implementados en relación a la Competencia Digital Docente, es decir, aquellos currículums dirigidos al profesorado para mejorar sus competencias digitales, entre las cuales se encuentra la seguridad digital (Jiménez-Hernández *et al.*, 2021; Viñoles-Cosentino *et al.*, 2022). Estos programas, además de ir únicamente dirigidos al personal docente, no abordan los riesgos del espacio digital a los que se enfrentan los menores de edad y que afectan directamente a su salud y bienestar.

Por este motivo, el objetivo del presente trabajo es analizar los programas educativos existentes hoy en día que abordan el uso responsable de Internet para gestionar los diversos retos y riesgos del espacio digital. Es decir, analizar las características más relevantes y los resultados de la evaluación de aquellos programas dirigidos a los miembros de la comunidad educativa. En este contexto, las preguntas principales que guían este estudio son: ¿cuántos programas dirigidos a la comunidad educativa en los últimos cinco años abordan los riesgos del espacio digital? ¿Cuáles son los riesgos que abordan estos programas? ¿Cómo han sido evaluados estos programas y cuáles han sido los resultados?

Material y método

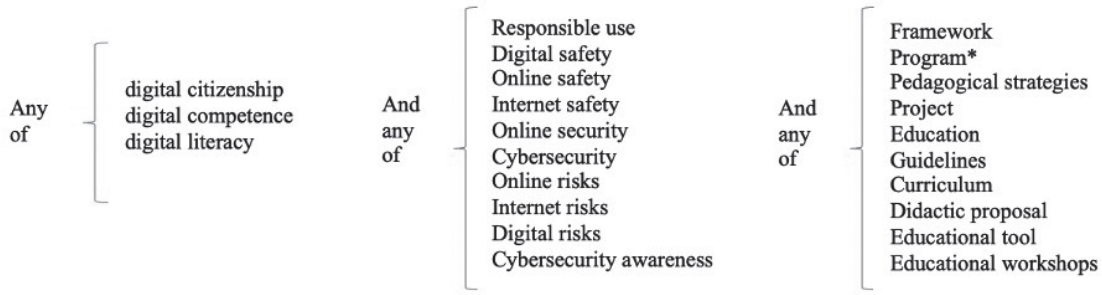
Diseño

Se ha llevado a cabo una revisión sistemática para analizar estudios empíricos sobre la implementación de programas educativos en seguridad digital y uso responsable de Internet dirigidos a alumnado, profesorado y familias. El procedimiento de identificación, selección e idoneidad se ha llevado a cabo siguiendo la propuesta del modelo PRISMA (Urrútia y Bonfill, 2010).

Fuentes de información y estrategia de búsqueda

Se utilizaron 5 bases de datos como fuentes de información para obtener artículos en revistas científicas indexadas: *Medline*, *Scopus*, *Web of Science*, *Eric* y *PubMed*. Los términos de búsqueda fueron seleccionados en base al objetivo de la revisión (véase Figura 1).

Figura 1. Palabras clave incorporadas en la primera fase de revisión (identificación)



Selección de artículos

1. *Criterios de inclusión y exclusión*

Para la selección de los programas se establecieron criterios de inclusión y exclusión siguiendo las recomendaciones de Sánchez-Meca y Botella (2015) para revisiones sistemáticas, orientadas a aportar una garantía de calidad en la selección. Se siguieron los siguientes criterios:

a. Estudios empíricos publicados entre enero de 2017 y septiembre de 2022.
b. Publicados en inglés o en español.
c. Programa de intervención sobre seguridad y/o alfabetización digital.
d. Artículos con programas implementados.

De este modo, se descartaron todos los registros identificados en las bases de datos que no fueran estudios empíricos, tales como tesis, disertaciones o informes, libros o capítulos de libros, así como revisiones bibliográficas.

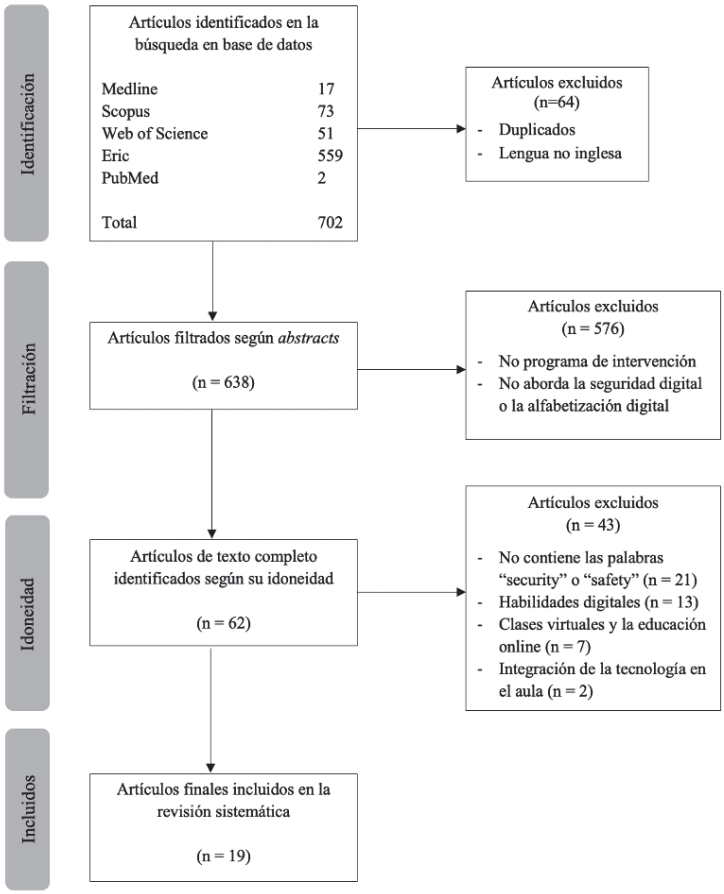
2. *Proceso de identificación, selección e idoneidad*

Una investigadora llevó a cabo la identificación (primera fase) de los artículos a partir de las palabras clave introducidas en las bases de datos (véase Figura 1) descartando aquellos sobre programas educativos que estuvieran duplicados y aquellos que no cumplían el criterio idiomático preestablecido (Criterio *b*), es decir, los artículos no disponibles en inglés o español. Seguidamente, en la segunda fase (filtración), en una revisión por pares cuatro autores realizaron la filtración de los artículos a partir de la lectura de sus resúmenes, siguiendo los criterios de inclusión del programa de intervención: que abordara la seguridad digital y/o la alfabetización digital (Criterio *c*) y que estuviera implementado (Criterio *d*). En la tercera

fase (idoneidad), se realizó la selección final mediante la lectura completa de los artículos seleccionados en la fase anterior, verificando que los diferentes programas abordaran la seguridad digital y excluyendo los artículos que no cumplían los criterios de inclusión. En la Figura 2 se detallan los motivos específicos de exclusión (n= 43). Finalmente, en la fase de codificación, también mediante una revisión por pares de los cuatro autores, se realizó la lectura completa de los artículos obtenidos (n= 19) para la codificación de las siguientes variables de estudio: población diana, duración del programa, contenido del programa, y evaluación y resultados del programa, incluyendo el tipo de metodología utilizada y la muestra.

En la Figura 2 se detalla el diagrama de flujo del proceso de revisión, así como los artículos incluidos y excluidos, siguiendo la propuesta del modelo PRISMA (Urrútia y Bonfill, 2010).

Figura 2. Diagrama de flujo PRISMA de la búsqueda de artículos y procedimiento de inclusión/exclusión para la revisión sistemática



3. Artículos incluidos

Como se puede observar en la Figura 2, se identificaron un total de 702 artículos extraídos de las bases de datos a través de las palabras clave introducidas, de los cuales 64 fueron eliminados al ser duplicados o no estar disponibles en lengua inglesa o española. Posteriormente, en la fase de filtración se revisaron por parejas de revisores/as los abstracts de 638 artículos, de los cuales 62 fueron seleccionados por su idoneidad. Finalmente, en la fase de inclusión, se revisaron los textos completos, incluyendo un total de 19 artículos en la revisión sistemática.

4. Acuerdo intercodificadores

Para analizar el nivel de acuerdo entre los pares de revisores, se calculó el índice Kappa (Cohen, 1960) mediante el recuento de coincidencias y discrepancias para cada par de revisores/as. El resultado obtenido mostró que tanto el primer par de revisoras (κ= ,907) como el segundo par de revisores (κ= ,843) obtuvieron un nivel de concordancia muy bueno en la fase de filtración.

En cuanto a la tercera fase (idoneidad), los mismos dos equipos de investigadores realizaron la codificación de la mitad de los artículos cada uno. El resultado obtenido del análisis de acuerdo intercodificadores demuestra que tanto el primer par de revisoras (κ= ,887) como el segundo par de revisores (κ= ,940) obtuvieron un nivel de concordancia muy bueno.

Los resultados obtenidos en ambas Kappas demuestra que, tanto en la selección de artículos para su revisión (filtración) como en la selección final de artículos para su inclusión (idoneidad), la concordancia interjueces fue superior a la debida por azar, lo cual aporta rigor metodológico a lo largo de todo el proceso de revisión. Por ende, la selección, inclusión y codificación de los artículos de la presente revisión gozan de una buena fiabilidad.

Resultados

Un total de 19 artículos (véase Figura 1) publicados entre 2017 y 2022 fueron considerados para el presente estudio. Sus respectivos programas fueron implementados principalmente en España (36,8%) y Estados Unidos (15,8%). A continuación se describen las principales características de los artículos incluidos en la revisión (véase Tabla 1) teniendo en cuenta cada uno de los tres objetivos de esta revisión.

Tabla 1. Resumen de las características de cada estudio incluido en la revisión sistemática

ESTUDIO (PAÍS)	POBLACIÓN DIANA (EDAD MEDIA)	OBJETIVO	DURACIÓN	MUESTRA	DISEÑO	EVALUACIÓN
1. Agila-Palacios *et al.*, 2021 (España)	Joven (M= 33,01)	Analizar la influencia del Aprendizaje Orientado a Proyectos (AOP) y el Aprendizaje Basado en Casos (ABC) como dos metodologías activas en el desarrollo de competencias digitales utilizando dispositivos móviles.	16 semanas	N= 178 n_{post}= 38	Cuasi-experimental longitudinal	Pre-post
2. Alemany *et al.*, 2020 (España)	Adolescente (M= 13,04)	Investigar el impacto del género y la edad en los usuarios adolescentes en relación con el aprendizaje sobre privacidad y las características de la red social, así como la participación en la red social gamificada.	4 semanas 3 sesiones	N= 387	Cuasi-experimental transversal	Encuesta
3. Antunes *et al.*, 2021 (Portugal)	Adolescente (M= 12,39)	Presentar una estrategia integrada de ciberseguridad y concienciación sobre la misma compuesta por tres ejes: (1) evaluación de actitudes y comportamientos en ciberseguridad, (2) autodiagnóstico y (3) actividades de enseñanza/aprendizaje.	3 sesiones de 90 mins.	N= 164	Cuasi-experimental transversal	Encuesta
4. Aydin y Çelik, 2020 (Turquía)	Profesorado	Evaluar la eficacia del curso de alfabetización digital impartido a estudiantes universitarios sobre las "competencias de ciudadanía digital" de los profesores de ciencias sociales.	8 semanas	N= 30	Cuasi-experimental longitudinal	Pre-post
5. Bickham *et al.*, 2020 (EE. UU.)	Adolescente (M= 12,20)	Determinar la eficacia del programa Screenshots para aumentar los conocimientos en ciudadanía digital y seguridad online en interacciones sociales. Examinar la existencia de efectos diferentes en las estrategias de resolución de conflictos y acoso escolar en hombres y mujeres.	16 semanas	N= 163 n_{exp}= 92 $n_{control}$= 71	Experimental longitudinal	Pre-post

[CONTINÚA EN LA PÁGINA SIGUIENTE]

Tabla 1. Resumen de las características de cada estudio incluido en la revisión sistemática

ESTUDIO (PAÍS)	POBLACIÓN DIANA (EDAD MEDIA)	OBJETIVO	DURACIÓN	MUESTRA	DISEÑO	EVALUACIÓN
6. Brandau *et al.*, 2022 (EE. UU.)	Preadolescente (M= 11,70)	Evaluar la eficacia de un programa de ciudadanía digital para aumentar los conocimientos sobre esta competencia y reducir el ciberacoso y las agresiones en línea en el alumnado de una región económicamente desfavorecida.	5 semanas 5 sesiones de 90 mins.	N= 27	Cuasi-experimental longitudinal	Pre-post
7. Fernández-Montalvo *et al.*, 2017 (España)	Preadolescente (M= 11,00)	Evaluar la efectividad de un programa de alfabetización digital en estudiantes de Educación Primaria.	3 sesiones	N= 364 n_{exp}= 190 $n_{control}$= 174	Experimental longitudinal	Pre-post y follow-up
8. Frydenberg y Lorenz, 2020 (Estonia)	Adulta	Describir el contenido de tres sesiones interactivas ofrecidas a estudiantes de informática dirigidas a sensibilizar en ciberseguridad. Los resultados son evaluados mediante la opinión de los estudiantes tras la finalización del curso.	1 mes 3 sesiones de 80 mins.	N= 20	Cuasi-experimental transversal	Encuesta
9. Gamito *et al.*, 2017 (España)	Preadolescente (M= 11,00)	Presentar el diseño, implementación y evaluación de una intervención didáctica sobre los riesgos de Internet y la identidad digital en el tercer ciclo de educación primaria.	3 sesiones de 45 mins.	N= 153	Cuasi-experimental transversal	Encuesta
10. Gordillo *et al.*, 2021 (España)	Profesorado de educación primaria (M= 42,6)	Examinar la utilidad de una red social simulada (*SocialLab*) como herramienta educativa para mejorar la competencia digital del profesorado en el ámbito del uso seguro y responsable de la tecnología.	10 semanas	N= 70 30 horas	Cuasi-experimental transversal	Encuesta
11. Gordillo *et al.*, 2019 (España)	Profesorado universitario	Examina la efectividad instruccional de tres cursos con formato Massive Open Online Course (MOOC) para la formación del profesorado en el uso seguro y responsable de las TIC mediante el análisis de tres cursos oficiales diferentes.	7 semanas	N= 809 n_{CursoA}= 200 n_{CursoB}= 535 n_{CursoC}= 74	Cuasi-experimental longitudinal	Pre-post

[CONTINÚA EN LA PÁGINA SIGUIENTE]

Tabla 1. Resumen de las características de cada estudio incluido en la revisión sistemática

ESTUDIO (PAÍS)	POBLACIÓN DIANA (EDAD MEDIA)	OBJETIVO	DURACIÓN	MUESTRA	DISEÑO	EVALUACIÓN
12. Holguin-Álvarez *et al.*, 2021 (Perú)	Preadolescente (M= 11,51) Adulta (M= 56,50)	Determinar los efectos de la transferencia de competencias digitales en dos tipos de interacción: estudiantes universitarios-adultos, adultos-niños.	1 año 70 sesiones	N= 201 $n_{pread.}$= 125 n_{adulta}= 76	Cuasi-experimental longitudinal	Pre-post
13. Kapitány-Fövényab *et al.*, 2022 (Hungría)	Preadolescente (M= 11,25)	Explorar las diferencias de género y el posible papel mediador de la edad, la impulsividad y el uso problemático de Internet en relación con los resultados de un programa de ciberacoso en educación primaria.	4 sesiones de 45 mins.	N= 933 $n_{f\text{-}up}$= 536	Cuasi-experimental longitudinal	Post-follow-up
14. King-Man Chong y Shing Pao, 2021 (Hong-Kong)	Profesorado de educación secundaria	Investigar la eficacia de un proyecto de desarrollo profesional sobre educación para la ciudadanía digital (ECD).	6 sesiones	N= 12	Cuasi-experimental longitudinal	Pre-post
15. Kowalska-Chrzanowska, *et al.*, 2021 (Polonia)	Adulta (M= 47,08)	Describir las formaciones sobre competencia digital impartidas en el marco del proyecto "E-Active Residents of the Kuyavian-Pomeranian and Łódź Voivodeships" y evaluación de su eficacia.	28 semanas	N= 837	Cuasi-experimental longitudinal	Pre-post
16. Martin *et al.*, 2020 (EE. UU.)	Profesorado	Examinar las experiencias de los educadores en relación con un curso de posgrado sobre ciudadanía digital en competencias de ciberbullying, netiqueta digital, huella digital, privacidad digital e identidad digital.	1 año	N= 45 n_{post}= 10	Cuasi-experimental longitudinal	Pre-post
17. Martzoukou, 2020 (Reino Unido)	Preadolescente (M= 12,04)	Describe el diseño y el estudio piloto basado en una serie de dibujos animados para el desarrollo de la alfabetización digital, la resiliencia digital y la ciudadanía digital, abordando el compromiso activo y la participación colaborativa a través de vídeos de dibujos animados.	1 hora	N= 24	Cuasi-experimental transversal	Encuesta

[CONTINÚA EN LA PÁGINA SIGUIENTE]

Tabla 1. Resumen de las características de cada estudio incluido en la revisión sistemática

ESTUDIO (PAÍS)	POBLACIÓN DIANA (EDAD MEDIA)	OBJETIVO	DURACIÓN	MUESTRA	DISEÑO	EVALUACIÓN
18. Maqsood y Chiasson, 2021 (Canadá)	Preadolescente (M= 11,44)	Evaluar una herramienta gamificada sobre ciberseguridad, privacidad y alfabetización digital impartida en el contexto educativo	1 semana	N= 84 $n_{pread.}$= 63 n_{prof}= 21	Cuasi-experimental longitudinal	Pre-post
19. Vogt y Hollestein, 2021 (Suiza)	Infantil (M= 5,21)	Explorar el potencial del juego de simulación para que los niños adquieran las competencias necesarias para la transformación digital. Formación previa al profesorado para la implementación del curso.	14 semanas	N= 15	Cualitativa. Análisis de interacción multimodal	Observacional

Características de los programas dirigidos a la comunidad educativa que abordan el uso responsable de Internet

De los 19 artículos incluidos, el 68,4% iban dirigidos al alumnado, entre los cuales se encuentran niños/as y preadolescentes hasta 13 años (n= 9) (Alemany *et al.*, 2020; Antunes *et al.*, 2021; Bickham *et al.*, 2021; Brandau *et al.*, 2022; Fernández-Montalvo *et al.*, 2017; Gamito *et al.*, 2017; Holguin-Álvarez *et al.*, 2021; Martzoukou, 2020; Vogt y Hollestein, 2021), adolescentes (n= 2) (Alemany *et al.*, 2020; Kapitány-Fövényab *et al.*, 2022) y jóvenes universitarios (n= 2) (Agila-Palacios *et al.*, 2021; Frydenberg y Lorenz, 2020 B); otros iban dirigidos al profesorado de primaria (n= 2) (Aydin y Çelik, 2020; Gordillo *et al.*, 2021), al profesorado de educación secundaria (n= 1) (King-Man Chong y Shing Pao, 2021), al profesorado universitario (n= 1) (Gordillo *et al.*, 2019), y a profesorado sin especificación de curso académico (n= 1) (Martin *et al.*, 2020). Finalmente, se contó con un artículo (Kowalska-Chrzanowska *et al.*, 2021) dirigido a la población general de edades comprendidas entre los 20 y 86 años.

En relación con la duración de los programas, algunos artículos refirieron su número de sesiones, mientras que otros reportaron su duración en semanas, meses o años. En concreto, se hallaron programas que consistieron en una sesión (n= 1) (Martzoukou, 2020), en 3 sesiones (n= 5) (Alemany *et al.*, 2020; Antunes *et al.*, 2021; Fernández-Montalvo *et al.*, 2017; Frydenberg y Lorenz, 2020; Gamito *et al.*, 2017), en 4 sesiones (n= 1) (Kapitány-Fövényab *et al.*, 2022), en 5 sesiones (n= 1) (Brandau *et al.*, 2022) y en 6 sesiones (n= 1) (King-Man Chong y Shing Pao, 2021). También, programas que consistieron en 1 semana (n= 1) (Maqsood y

Chiasson, 2021), 8 semanas (n= 1) (Aydin y Çelik, 2020), 10 semanas (n= 1) (Gordillo *et al.*, 2021) y 16 semanas (n= 1) (Agila-Palacios *et al.*, 2021). En relación con los programas que reportaron su duración en meses, se hallarón programas de 3,5 meses (n= 1) (Vogt y Hollestein, (2021), 4 meses (n= 1) (Bickham *et al.*, 2021), 6 meses (n= 1) (Martin *et al.*, 2020) y 7 meses (n= 1) (Kowalska-Chrzanowska *et al.*, 2021). Finalmente, uno de ellos tuvo una duración de un año (n= 1) (Holguin-Álvarez *et al.*, 2021) y otro de dos años (n= 1) (Gordillo *et al.*, 2019).

Riesgos del uso de Internet abordados en los programas educativos

De los 19 programas evaluados, la mayoría de ellos (57,9%) sí mencionaron la ciberviolencia (n= 11), todos ellos haciendo referencia explícita al ciberacoso (n= 11). También se abordaron otros riesgos como *sexting* (n= 5) (Brandau *et al.*, 2022; Fernández-Montalvo *et al.*, 2017; Gamito *et al.*, 2017; Gordillo *et al.*, 2021; Gordillo *et al.*, 2019), privacidad digital (n= 5) (Alemany *et al.*, 2020; Gamito *et al.*, 2017; Gordillo *et al.*, 2021; Martin *et al.*, 2020; Maqsood y Chiasson, 2021), *grooming* (n= 4) (Fernández-Montalvo *et al.*, 2017; Gamito *et al.*, 2017; Gordillo *et al.*, 2021; Gordillo *et al.*, 2019), suplantación de identidad (n= 3) (Frydenberg y Lorenz, 2020; Gordillo *et al.*, 2021; Gordillo *et al.*, 2019), información falsa (n= 3) (King-Man Chong y Shing Pao, 2021; Martzoukou, 2020; Maqsood y Chiasson, 2021), uso problemático de Internet (n= 2) (Gamito *et al.*, 2017; Kapitány-Fövényab *et al.*, 2022), *phishing* e ingeniería social (n= 2) (Antunes *et al.*, 2021; Frydenberg y Lorenz 2020), identidad digital y reputación *online* (n= 2) (Martin *et al.*, 2020; Martzoukou, 2020), compartir excesiva información (n= 2) (Antunes *et al.*, 2021; Gordillo *et al.*, 2021), *spam* y correos no deseados (n= 2) (Antunes, 2021; Frydenberg y Lorenz 2020), netiqueta digital (n= 1) (Martin *et al.*, 2020) y, finalmente, fraude (n= 1) (Kapitány-Fövényab *et al.*, 2022). Ninguno de los programas abordó la temática del consumo de pornografía *online*.

Las redes sociales fueron específicamente mencionadas sólo en tres artículos (n= 3) (Alemany *et al.*, 2020; Gordillo *et al.*, 2019; Holguin-Álvarez *et al.*, 2021) pero sin ser tratadas como un riesgo digital en sí mismas, sino como un medio a través del cual abordar los riesgos digitales. En el estudio llevado a cabo por Alemany *et al.* (2020) se utilizó una red social *gamificada* para comprobar si, a través del dinamismo del juego, los adolescentes eran capaces de aprender de manera efectiva los conceptos de privacidad y compromiso *online* en las redes sociales. Asimismo, en el estudio de Gordillo *et al.* (2019) se hizo uso de una red social simulada a través de la cual se formó al profesorado en competencias digitales, aunque sin incidir en las redes sociales. Finalmente, Holguin-Álvarez *et al.* (2021)

hicieron uso de las redes sociales, sin especificar cuáles ni de qué tipo, para evaluar la transferencia del conocimiento en competencias digitales entre dos tipos de interacción: estudiantes universitarios versus adultos y adultos versus niños y niñas escolarizados.

Características de la evaluación y resultados de su implementación en la comunidad educativa

De los 19 artículos incluidos, el 57,9% evaluaron el programa de forma longitudinal, mediante medidas repetidas pre-post (n= 11) (Agila-Palacios *et al.*, 2021; Aydin y Çelik, 2020; Bickham *et al.*, 2021; Brandau *et al.*, 2022; Fernández-Montalvo *et al.*, 2017; Gordillo *et al.*, 2021; Gordillo *et al.*, 2019; Holguin-Álvarez *et al.*, 2021; Kapitány-Fövényab *et al.*, 2022; King-Man Chong y Shing Pao, 2021; Martin *et al.*, 2020). De ellos, únicamente 2 programas realizaron una medida de seguimiento o *follow-up* (Fernández-Montalvo *et al.*, 2017; Kapitány-Fövényab *et al.*, 2022). Por otro lado, el 36,8% restante realizaron mediciones transversales, mediante encuestas de opinión (n= 6) (Alemany *et al.*, 2020; Antunes *et al.*, 2021; Frydenberg y Lorenz, 2020; Gamito *et al.*, 2017; Gordillo *et al.*, 2021; Martzoukou, 2020) y a través de la observación del comportamiento de los menores (n= 1) (Vogt y Hollestein, 2021).

En relación con la muestra, se hallaron tres programas que presentaron discrepancias entre el número de participantes y el número de personas que realizaron el post-test o el seguimiento (Agila-Palacios *et al.*, 2021; Kapitány-Fövényab *et al.*, 2022; Martin *et al.*, 2020). Además, en nueve programas la muestra fue inferior a 100 participantes (Aydin y Çelik, 2020; Brandau *et al.*, 2022; Frydenberg y Lorenz, 2020; Gordillo et al, 2021; King-Man Chong y Shing Pao, 2021; Martin *et al.*, 2020; Martzoukou, 2020; Maqsood y Chiasson, 2021; Vogt y Hollenstein, 2021), siete con una muestra de entre 150 y 400 participantes (Agila-Palacios *et al.*, 2021; Alemany *et al.*, 2020; Antunes *et al.*, 2021; Bickham *et al.*, 2021; Fernández-Montalvo *et al.*, 2017; Gamito *et al.*, 2017; Holguin-Álvarez *et al.*, 2021) y tres con una muestra de entre 800 y 1.000 (Gordillo *et al.*, 2019; Kapitány-Fövényab *et al.*, 2022; Kowalska-Chrzanowska *et al.*, 2021).

Respecto a los resultados de los programas evaluados, tres de ellos (Gordillo *et al.*, 2019; King-Man Chong y Shing Pao, 2021; Martin *et al.*, 2020) reportaron una mejora en los conocimientos digitales del profesorado y su enseñanza sobre los mismos. Específicamente, hallaron mejoras en los conocimientos sobre ingeniería social, su preparación para prevenir ataques cibernéticos y su comprensión de los diferentes riesgos asociados al uso de Internet (Gordillo *et al.*, 2019),

así como también en la transferencia de la información sobre ciudadanía digital (Martin *et al.*, 2020) y enseñanzas dirigidas a las leyes digitales, comercio digital y seguridad digital a la hora de enseñar ciudadanía digital (King-Man Chong y Shing Pao, 2021).

Otros programas reportaron mejoras en el estudiantado en relación con la seguridad de su comportamiento *online* (n= 2) (Bickham *et al.*, 2021; Holguin-Álvarez *et al.*, 2021), incrementándose su rechazo a las actitudes negativas *online*, así como su consistencia en las conductas dirigidas a la seguridad *online* y a la resolución de conflictos de manera no agresiva (Bickham *et al.*, 2021). Otros concluyeron que los estudiantes presentaron mejoras en la alfabetización y las competencias digitales (n= 2) (Fernández-Montalvo *et al.*, 2017; Kowalska-Chrzanowska *et al.*, 2021), entre las cuales se incluían: el uso de herramientas de búsqueda, recursos digitales, servicios de administración electrónica y herramientas para la ciberseguridad (Kowalska-Chrzanowska *et al.*, 2021); el conocimiento sobre conceptos como red social, *ciberbullying*, identidad digital y privacidad, así como las conductas de bloqueo de mensajes y configuración de los ajustes de privacidad en redes sociales (Fernández-Montalvo *et al.*, 2017). Dos trabajos (n= 2) (Agila-Palacios *et al.*, 2021; Aydin y Çelik, 2020) señalaron que, a partir de los programas implementados, hubo una mejora en la implicación y la participación digital por parte de los estudiantes, que aumentaron así sus competencias de interacción, compartir, colaboración y netiqueta (Agila-Palacios *et al.*, 2021), y en el profesorado su rol activo en la toma de decisiones dentro de una red social para incrementar la interacción entre los usuarios (Aydin y Çelik, 2020). Un estudio afirmó que el alumnado mejoró en competencias de ciudadanía digital (n= 1) (Brandau *et al.*, 2022) como la privacidad y seguridad, la identidad y huella digital, la comunicación y el bienestar *online*. Finalmente, cabe destacar que únicamente un programa (Kapitány-Fövényab *et al.*, 2022) concluye que los componentes implicados en el acoso *online*, como la empatía hacia la víctima, los conocimientos sobre la búsqueda de ayuda y la percepción del riesgo *online*, están sujetos al género.

Discusión

En primer lugar, esta revisión sistemática ha evidenciado la escasez de estudios empíricos publicados sobre programas educativos existentes que aborden los retos del espacio digital y evalúen sus resultados. Este resultado parece especialmente relevante dada la creciente necesidad de incluir estos contenidos en el ámbito educativo, tal y como señalan organismos internacionales como la OMS (WHO, 2016) o Unicef (Brossard *et al.*, 2021).

Tras analizar los programas educativos sobre seguridad digital, cabe señalar que ninguno de ellos se ha dirigido a familiares o cuidadores/as, quienes deben desempeñar un papel activo en la educación de los menores. Para que las familias estén implicadas en la ciberseguridad de los jóvenes, primero deben formarse, ya que aún no tienen suficientes conocimientos para transmitirlos ni para tomar medidas que ayuden a prevenir riesgos en Internet. Además, de los 19 programas analizados, sólo cinco han tenido como objetivo la formación del profesorado y su capacidad para transmitir conocimientos. Tanto docentes como familias deben dar ejemplo de un comportamiento *online* seguro y, por lo tanto, deben estar capacitados en habilidades digitales (Aznar-Martínez *et al.*, 2023; Rodríguez Román, 2022).

La ciberviolencia es el riesgo digital que más se ha abordado en los programas educativos sobre seguridad digital y uso responsable de Internet. El riesgo que más frecuentemente ha aparecido en estos programas es el ciberacoso, ya que supone una de las principales situaciones de riesgo porque, al darse a través de medios tecnológicos, hay una alta invasión del espacio personal de la víctima sin que ésta tenga descanso (Observatorio de la Infancia e INCIBE, 2019; Pascual *et al.*, 2020).

Los otros riesgos abordados en los programas son el *sexting* y el *grooming*, en los que es necesario evaluar los riesgos con instrumentos de evaluación que tengan propiedades psicométricas rigurosas (Peris y Maganto, 2018) ya que la población joven es particularmente vulnerable a convertirse en víctima de violencia o abuso en línea (Peris *et al.*, 2021). También se han incluido otros retos, como la privacidad digital, la identidad digital y la netiqueta. Otras problemáticas que han abordado estos programas son la suplantación de la identidad, la ingeniería social y el *phishing*. El uso problemático de Internet también ha aparecido en los programas, ya es un riesgo relevante porque puede conllevar un comportamiento adictivo (Labrador *et al.*, 2018; Pascual *et al.*, 2020) y es una preocupación creciente entre padres, docentes, investigadores y la sociedad en general (Peris *et al.*, 2020). Otros riesgos abordados han sido reputación *online*, *spam* y correos no deseados, compartir excesiva información y el fraude.

Por otro lado, ningún programa ha incluido el consumo de pornografía *online*. Como indican los estudios previos, el 27% de menores de entre 7 y 12 años han estado expuestos a contenido pornográfico (Kaspersky, 2019), cifra que se eleva a más del 90% en el caso de los adolescentes de entre 13 y 18 años (Ballester *et al.*, 2023). Además, los organismos internacionales señalan la pornografía *online* como una de las mayores problemáticas actuales a las que se debe hacer frente (WHO, 2016), ya que representa la principal fuente de educación sexual en la juventud (Ballester *et al.*, 2021; Román *et al.*, 2021). Estos datos contrastan con los resultados obtenidos, ya que en este contexto cabría esperar que los programas de seguridad digital abordaran el tema

de la pornografía online, dada la importancia que se ha otorgado a esta cuestión y el impacto que ha evidenciado tener en la salud afectivo-sexual de los menores. También sería interesante incluir la seguridad digital en programas de educación afectivo-sexual o viceversa, es decir, incluir temáticas sobre educación afectivo-sexual en el abordaje del consumo de pornografía dentro del marco de la seguridad *online*. Es importante remarcar que, aunque todavía no hay programas estructurados y validados, sí hay literatura sobre intervenciones específicas (Ballester *et al.*, 2022b; Prats *et al.*, 2018).

Las redes sociales son el medio a través del cual se da la mayor parte de la interacción *online* entre la juventud y se utilizan para la construcción de su identidad (Labrador *et al.*, 2018; Peris *et al.*, 2013). Además, a través de las redes sociales también puede haber intercambio de contenido sexual y, aunque en la mayoría de ellas haya restricción de publicar fotografías o vídeos con gente desnuda, existen maneras de evitar la censura (Díaz-Altozano *et al.*, 2020; Save the Children, 2020). Las redes sociales como Instagram, Facebook o TikTok tienen establecidos los 13 años como edad mínima para crearse un perfil, pero el control sobre esta normativa es bajo y cualquier persona puede obtenerlo (Childnet, 2021). Dado que las redes sociales son el medio principal a través del cual adolescentes y jóvenes se exponen a los peligros *online* de los que se ha hablado, es importante concienciar a los menores sobre los riesgos que pueden tener y cómo proceder si se da alguna situación problemática, ya que muchas tienen su propio apartado de denuncias (Childnet, 2021; Labrador *et al.*, 2018). Por tanto, parece imprescindible seguir formando a los menores en este aspecto.

En términos de evaluación del programa, la mayoría han sido evaluados a través de la aplicación de un post-test, y uno de ellos a través de la observación del comportamiento de los menores en el entorno digital, pero solamente dos de los programas han realizado un seguimiento a los participantes. Esto último sería deseable para evaluar si los conocimientos obtenidos permanecen en el tiempo y son interiorizados y aplicados por los participantes, hecho que resultaría óptimo para la correcta evaluación de la eficacia de las intervenciones.

En los programas analizados se ha observado una adaptación de las actividades en función del colectivo al que se dirigen y, en el caso de los menores de edad, también según la etapa del desarrollo. En este sentido, los programas dirigidos a niños y niñas han incluido juegos educativos para adquirir habilidades en el espacio digital, mientras que los programas dirigidos al profesorado han abordado temas sobre la enseñanza y transmisión de competencias necesarias para una práctica educativa óptima.

La literatura científica destaca la necesidad de promover escuelas seguras a través de la participación de toda la comunidad educativa (Ferrer-Cascales *et al.*,

2019; Prats *et al.*, 2018); por ende, se trata de un factor que hay que tener en cuenta y que ninguno de los programas evaluados ha incluido. Debería plantearse un currículum transversal, dirigido tanto a docentes y familias como a estudiantes. Se debería formar a docentes y familias no sólo en habilidades digitales, sino también en cómo transmitir ese conocimiento a los menores y cómo establecer un ambiente seguro y de confianza para abordar cualquier problemática que surja. Por lo tanto, proponemos la implementación de programas escolares en los que docentes y familias sean evaluados longitudinalmente en sus habilidades digitales y en la forma de transmitir sus conocimientos relativos a la seguridad digital a las personas jóvenes. De este modo, planteamos una evaluación de tres medidas (pre-post-seguimiento) para analizar la adquisición de estos conocimientos por parte del alumnado, docentes y familias a corto y a largo plazo. Consideramos fundamental esta tercera medida de seguimiento para garantizar que el alumnado haya interiorizado estas habilidades, que tendrán un papel activo en su propio aprendizaje sobre el espacio digital a través del pensamiento crítico (Rodríguez Román, 2022).

En cuanto al contenido, estos programas deberían tratar los riesgos del espacio digital mencionados, incluyendo el fomento de un uso adecuado de las redes sociales, así como la pornografía, dentro de un marco que englobe también la educación afectivo-sexual. El objetivo es que el alumnado llegue a autorregularse en cuanto al uso que hace del espacio digital, para que dispongan de los conocimientos necesarios sobre las consecuencias que puede tener su mal uso, la capacidad de identificar riesgos o situaciones peligrosas, así como la posibilidad de pedir ayuda en caso de encontrarse ante una amenaza.

Conclusiones

En lo que se refiere al objetivo establecido, analizar los programas educativos que abordan el uso responsable de Internet para gestionar los diversos retos y riesgos del espacio digital, se ha visto que solamente 19 programas de los 702 (2,7%) encontrados en la primera búsqueda implementaron programas educativos sobre seguridad digital. De estos, solamente 5 iban dirigidos a profesorado, ninguno a las familias y los 14 restantes a alumnado, incluyendo niños y niñas, adolescentes y estudiantes universitarios. En lo que respecta al contenido del programa, 11 de ellos abordan la ciberviolencia, donde aparecen temáticas como el ciberacoso y también aparecen otros retos que comporta Internet, como el *sexting* y el *grooming*, el uso problemático de Internet, la privacidad digital, la suplantación de identidad, la ingeniería social y el *phishing*, la información falsa, la compartición excesiva de información, los correos no deseados y *spam*, la identidad digital, la netiqueta digital y el fraude.

El consumo de pornografía *online* no se aborda en ningún programa. En cuanto a la duración del programa, muchos de ellos consistían en algunas sesiones o en pocas semanas, mientras que solamente 2 duraban un año o más. Como se puede observar, existe una clara falta de homogeneidad en la duración de los programas. En la evaluación, 11 siguieron un diseño pos-test, pero solamente 2 de ellos realizaron una medida de seguimiento a largo plazo. Además, simplemente 3 programas cuentan con una muestra amplia de participantes superior a 500 personas. Por otra parte, todos los programas evaluados muestran resultados positivos después de la implementación del programa, asegurando una mejoría en los conocimientos digitales del profesorado, en el comportamiento *online* seguro de los estudiantes, en su alfabetización y competencias digitales, en la implicación digital y en la ciudadanía digital.

En cuanto a las implicaciones prácticas, el análisis de los programas destaca la escasez de programas enfocados a la seguridad digital y la necesidad de medidas preventivas para proteger a los menores de los riesgos en Internet. A partir de esta revisión, se identifican los puntos fuertes de los programas para repetirlos en el futuro y las carencias para reforzarlos, como la necesidad de programas que involucren a toda la comunidad educativa y aborden la problemática del consumo de pornografía *online*, totalmente ausente en estos programas en la actualidad. El objetivo es implementar programas completos y eficaces.

Esta revisión sistemática ha permitido evidenciar la necesidad de mayor consenso en la comunidad educativa y científica en relación a los programas de seguridad digital. El uso responsable de las tecnologías digitales debe ser un aprendizaje básico para toda la comunidad educativa. Además, sería interesante incluir los potenciales peligros de Internet como prevención primaria, poniendo especial énfasis en los riesgos de tipo sexual y las redes sociales.

A pesar de que en la Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación (2020) se hace referencia explícita al abordaje de la seguridad digital y el uso responsable de Internet en el Currículum de Educación Básica (Primaria y Secundaria), hacen falta directrices claras sobre su aplicación, y para ello es necesario que se lleven a cabo más programas sobre la temática estudiada y se evalúen los resultados. Esperamos que esta revisión sistemática permita abrir un diálogo en la comunidad educativa para fomentar nuevos programas que incluyan los aspectos de mejora identificados en esta investigación.

Fecha de recepción del original: 5 de mayo de 2023
Fecha de aceptación de la versión definitiva: 5 de diciembre de 2023

Referencias

*Agila-Palacios, M. V., García-Valcárcel, A. y Ramírez-Montoya, M. S. (2021). Influence of active methodologies: Projects and cases in the development of digital competences with mobile devices. *Journal of Applied Research in Higher Education*, *14*(3), 1007-1020. https://doi.org/10.1108/JARHE-05-2020-0149

*Alemany, J., del Val, E. y García-Fornes, A. (2020). Assessing the Effectiveness of a Gamified Social Network for Applying Privacy Concepts: An Empirical Study With Teens. *Transactions on Learning Technologies*, *13*(4), 777-789. https://doi.org/10.1109/TLT.2020.3026584

Andrade, B., García, I., Boubeta, A. y Suárez, F. (2021). *Impacto de la tecnología en la adolescencia: relaciones, riesgos y oportunidades. Un estudio comprensivo e inclusivo hacia el uso saludable de las TRIC.* Unicef España.

Andrie, E., Ikbale, I., Tzavela, E., Richardson, C. y Tsitsika, A. (2021). Adolescents' Online Pornography Exposure and Its Relationship to Sociodemographic and Psychopathological Correlates: A Cross-Sectional Study in Six European Countries. *Children*, *8*, 2-16. https://doi.org/10.3390/children8100925

*Antunes, M., Silva, C. y Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Science*, *11*(23), 11269. https://doi.org/10.3390/app112311269

Arunkumar, K. y Premalatha, T. (2021). Social Media: Do the Prospective Teachers Use it with Awareness? *Journal of Educational Technology*, *18*(3), 54-62. https://doi.org/10.26634/jet.18.3.18277

Avast (2023). *Ingeniería social y cómo protegerse*. https://www.avast.com/es-es/c-social-engineering

Avast (2023). *Netiqueta: normas y directrices*. https://www.avast.com/es-es/c-netiquette

*Aydin, C. y Çelik, T. (2020). Impact of the digital literacy courses taken by the prospective social studies teachers by distance learning on digital citizenship skills. *Research on Education and Media*, *12*(1), 42-57. https://doi.org/10.2478/rem-2020-0006

Aznar-Martínez, B., Casarramona, A., Lorente-De-Sanz, J., Grané, J., Castillo Garayoa, J., Vall, B. y Pérez-Testor, C. (2023). Formas telemáticas de control de acceso a la pornografía para menores y abordaje integral de los retos del espacio digital. En V. Milano (Dir.), *Estudio sobre pornografía en las Islas Baleares: acceso e impacto sobre la adolescencia, derecho internacional y nacional aplicable y soluciones tecnológicas de control y bloqueo* (pp. 28-287). Institut Balear de la Dona.

Ballester Brague, L., Orte Socías, C. y Rosón Varela, C. (2022). A survey study on pornography consumption among young Spaniards and its impact on

interpersonal relationships. *Net Journal of Social Sciences*, *10*(3), 71-86. https://doi.org/10.30918/NJSS.103.22.023

Ballester, L., Rosón, C., Facal, T. y Gómez, R. (2021). Nueva pornografia y desconexión empàtica. *Revista Internacional de Estudios Feministas*, *6*(1), 67-105. https://dx.doi.org/10.17979/arief.2021.6.1.7075

Ballester, L., Rosón, C., Noya, M. y Calderón-Cruz, B. (2022b). Characteristics of Online Pornography and Interventions Against its Negative Effects in Young People: Results from an International Delphi Panel. *Journal of Rational-Emotive & Cognitive-Behavior Therapy*, *40*(3), 634-646. https://doi.org/10.1007/s10942-021-00425-z

Ballester, L., Sedano, S., Aznar-Martínez, B., Cabellos, A., Lorente-De-Sanz, J. y Nadal, M. (2023). Diagnóstico sobre acceso, consumo e implicaciones de la nueva pornografía en línea en las Islas Baleares. En V. Milano (Dir.), *Estudio sobre pornografía en las Islas Baleares: acceso e impacto sobre la adolescencia, derecho internacional y nacional aplicable y soluciones tecnológicas de control y bloqueo* (pp. 28-287). Institut Balear de la Dona.

*Bickham, D., Moukalled, S., Inyart, H. y Zlokower, R. (2021). Evaluating a Middle-School Digital Citizenship Curriculum (Screenshots): Quasi-Experimental Study. *JMIR Mental Health*, *8*(9). hhtps://doi.org/10.2196/26197

*Brandau, M., Dilley, T., Schaumleffel, C. y Himawan, L. (2022). Digital citizenship among Appalachian middle schoolers: The common sense digital citizenship curriculum. *Health Education Journal*, *81*(2), 157-169. https://doi.org/10.1177/00178969211056429

Brossard, M., Carnelli, M., Chaudron, S., Di-Gioia, R., Dreesen, T., Kardefelt-Winther, D., Little, C. y Yameogo, J. L. (2021). *Digital Learning for every child: closing the gaps for an inclusive and prosperous future*. Unicef. https://www.unicef.org/media/113896/file/Digital%20Learning%20for%20Every%20Child.pdf

Chaudron, S., Di Gioia, R. y Gemo, M. (2018). *Young children (0-8) and digital technology – A qualitative study across Europe*. Publications Office of the European Union. https://data.europa.eu/doi/10.2760/294383

Childnet (2021). *Helping make the Internet a great and safe place for children and young people*. https://www.childnet.com

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, *20*(1), 37-46.

Díaz-Altozano, P., Padilla-Castillo, G. y Requeijo-Rey, P. (2020). Sexualización de niñas en redes sociales: la necesidad de inteligencia semántica en Instagram. *Investigaciones Feministas*, *12*(1), 31-45. https://doi.org/10.5209/infe.69559

Feijóo, S., O'Higgins-Norman, J., Foody, M., Pichel, R., Braña, T., Varela, J. y Rial, A. (2021). Sex Differences in Adolescent Bullying Behaviours. *Psychosocial Intervention*, *30*(2), 95-100. https://doi.org/10.5093/pi2021a1

*Fernández-Montalvo, J., Peñalva, A., Irazabal, I. y López-Goñi, J. J. (2017). Efectividad de un programa de alfabetización digital para estudiantes de Educación Primaria. *Cultura y Educación*, *29*(1), 1-30. https://doi.org/10.1080/11356405.2016.1269501

Ferrer-Cascales, R., Albaladejo-Blázquez, N., Sánchez-SanSegundo, M., Portilla-Tamarit, I., Lordan, O. y Ruiz-Robledillo, N. (2019). Effectiveness of the TEI program for bullying and cyberbullying reduction and school climate improvement *International Journal of Environmental Research and Public Health*, *16*(4), 580. https://doi.org/10.3390/ijerph16040580

*Frydenberg, M. y Lorenz, B. (2020). Lizards in the Street! Introducing Cybersecurity Awareness in a Digital Literacy Context. *Information Systems Education Journal*, *18*(4), 33-45.

*Gamito, R., Aristizabal, P., Olasolo, M. y Vizcarra, M. T. (2017). La necesidad de trabajar los riesgos de internet en el aula. *Profesorado. Revista de Currículum y Formación de Profesorado*, *21*(3), 409-426.

Godaert, E., Aesaert, K., Voogt, J. y van Braak, J. (2022). Assessment of students' digital competences in primary school: a systematic review. *Education and Information Technologies*, *27*(4), 9953-10011. https://doi.org/10.1007/s10639-022-11020-9

*Gordillo, A., Barra, E., Garaizar, P. y López-Pernas, S. (2021). Use of a Simulated Social Network as an Educational Tool to Enhance Teacher Digital Competence. *Revista Iberoamericana de Tecnologías del Aprendizaje*, *16*(1), 107-114. hhttps://doi.org/10.1109/RITA.2021.3052686

*Gordillo, A., López-Pernas, S. y Barra, E. (2019). Efectividad de los MOOC para docentes en el uso seguro de las TIC. *Revista Comunicar*, *26*(61), 103-112. https://doi.org/10.3916/C61-2019-09

Hatch, G., Esplin, C., Aaron, S., Dowdle, K., Fincha, F., Hatch, D. I. y Braithwaite, S. (2020). Does pornography consumption lead to intimate partner violence perpetration? Little evidence for temporal precedence. *The Canadian Journal of Human Sexuality*, *23*(3), 289-296. https://doi.org/10.3138/cjhs.2019-0065

Heru, W., Banu, N., Piang, B. y Sumardjoko, B. (2021). Digital citizenship trend in educational sphere: A systematic review. *International Journal of Evaluation and Research in Education*, *10*(4), 1192-1201. https://doi.org/10.11591/ijere.v10i4.21767

*Holguin-Álvarez, J., Garay-Rodríguez, P., Amasifuén-Sánchez, V., Huaita,

D. M., Luza, F. F., Cruz-Montero, J. y Ledesma-Pérez, F. (2021). Digital Competences in the Elderly and University Students: Didactic Interaction from the Use of Social Networks. *International Journal of Emerging Technologies in Learning (iJET)*, *16*(4), 188-200. https://doi.org/10.3991/ijet.v16i04.18519

Hornor, G. (2020). Child and Adolescent Pornography Exposure. *Pediatric Health Care*, *34*, 191-199. https://doi.org/10.1016/j.pedhc.2019.10.001

INCIBE (2023). *Phishing*. https://www.incibe.es/aprendeciberseguridad/phishing

International Child Development (2021). *CYBERSAFE Guide for Workshop Facilitators: Addressing the issue of online violence against girls in a classroom setting*. https://www.stoponlineviolence.eu/wp-content/uploads/2021/11/CYBERSAFE-Guide-for-workshop-facilitators_FINAL-with-design-2.pdf

Internet Segura for Kids (2022). *Herramientas de control parental*. https://www.is4k.es

James, C., Weinstein, E. y Mendoza, K. (2021). *Teaching Digital Citizens in Today's World: Research and Insights Behind the Common Sense Digital Citizenship Curriculum*. Common Sense. https://www.commonsense.org/system/files/pdf/2021-08/common-sense-education-digital-citizenship-research-backgrounder.pdf

Jiménez-Hernández, D., Muñoz Sánchez, P. y Sánchez Jiménez, F. S. (2021). La Competencia Digital Docente una revisión sistemática de los modelos más utilizados. *Revista Interuniversitaria de Investigación en Tecnología Educativa*, *10*, 105-120. https://doi.org/10.6018/riite.472351

*Kapitány-Fövényab, M., Lukács, A., Takács, J., Kitzinger, I., Soósné Kiss, Z., Szabó, G., Falus, A. y Judit Feith, H. (2022). Gender-specific pathways regarding the outcomes of a cyberbullying youth education program. *Personality and Individual Differences*, *186*. https://doi.org/10.1016/j.paid.2021.111338

Kaspersky (2019). *Parents fear for kids' online safety but aren't putting time in to talk about it.* https://media.kasperskydaily.com/wp-content/uploads/sites/92/2019/09/12065947/family-campaign-report-final.pdf

*King-Man Chong, E. y Shing Pao, S. (2021). Promoting digital citizenship education in junior secondary schools in Hong Kong: supporting schools in professional development and action research. *Asian Education and Development Studies*, *11*(4), 677-690. https://doi.org/10.1108/AEDS-09-2020-0219

*Kowalska-Chrzanowska, M., Krysiński, P. y Paweł Karwowski, M. (2021). Digital competences of residents in Kuyavian-Pomeranian Voivodeship in the light of the polish training project "E-active" . *Education and Information Technologies*, *26*, 3427-3444. https://doi.org/10.1007/s10639-020-10411-0

Labrador Encinas, F., Requesens Moll, A. y Helguera Fuentes, M. (2018). *Guía*

para padres y educadores sobre el uso seguro de Internet, móviles y videojuegos. Fundació Gaudium.

Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación". *Boletín Oficial del Estado*, nº 340, 122868-122953.

*Martin, F., Tuba, G., Wei Chao, W., Teresa, P. y Chuang, W. (2020). Examining K-12 educator experiences from digital citizenship professional development. *Journal of Research on Technology in Education*, *54*(1), 143-160. https://doi.org/10.1080/15391523.2020.1815611

*Martzoukou, K. (2020). "Maddie is online": an educational video cartoon series on digital literacy and resilience for children. *Journal of Research in Innovative Teaching & Learning*, *15*(1), 64-82. https://doi.org/10.1108/JRIT-06-2020-0031

*Maqsood, S. y Chiasson, S. (2021). Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Transactions on Privacy and Security*, *24*(4), 1-37. https://doi.org/10.1145/3469821

Mestre-Bach, G., Villena-Moya, A. y Chiclana-Actis, C. (2023). Pornography use and violence: a systematic review of the last 20 years. *Trauma, Violence, & Abuse*. https://doi.org/10.1177/152483802311736

Observatorio de la Infancia e Instituto Nacional de Ciberseguridad (2019). *Guía de uso seguro y responsable de Internet para profesionales de servicios de protección a la infancia.* https://observatoriodelainfancia.mdsocialesa2030.gob.es/productos/pdf/Guia_Internet_Accesible_2_Con_cubiertas_alta_resolucion.pdf

Pascual, A., Fernández, S., Casero, A., Etxenagusia, P., Fuente, D., Guerrero, I., Lamas, N., Ramajo, M. V., Rodríguez, J. y Vieira, A. (2020). *Guía para familias: acompañando a niños, niñas y adolescentes en el uso seguro y responsable de las TRIC.* FAPMI-ECPAT. https://www.observatoriodelainfancia.es/ficherosoia/documentos/7051_d_FAPMI-TRIC.pdf

Paslakis, G., Chiclana, C. y Mestre-Bach, G. (2020). Associations between pornography exposure, body image and sexual body image: A systematic review. *Journal of Health Psychology*, *27*(3), 1-18. https://doi.org/10.1177/1359105320967085

Peris, M. y Maganto, C. (2018). *Sexting, sextorsión y grooming. Identificación y prevención*. Pirámide.

Peris, M., Maganto, C. y Kortabarria, L. (2013). Body self-esteem, virtual image in social networks and sexuality in adolescent. *European Journal of Investigation in Health, Psychology and Education*, *3*(2), 171-180. https://doi.org/10.1989/ejihpe.v3i2.34

Peris, M., de la Barrera, U., Schoeps, K. y Montoya-Castilla, I. (2020). Psychological Risk Factors that Predict Social Networking and Internet Addiction in

Adolescents. *International Journal of Environmental Research and Public Health*, *17*(12), 4598. https://doi.org/10.3390/ijerph171245987

Peris-Hernández, M., Schoeps, K., Maganto, C. y Montoya-Castilla, I. (2021). The risk of sexual-erotic online behavior in adolescents-Which personality factors predict sexting and grooming victimization? *Computers in Human Behavior*, 114, 106569. https://doi.org/10.1016/j.chb.2020.106569

Potyrała, K. y Tomczyk, L. (2021). Teachers in the lifelong learning process: examples of digital literacy. *Journal of Education for Teaching*, *47*(2), 255-273. https://doi.org/10.1080/02607476.2021.1876499

Prats, M. A., Torres-Rodríguez, A., Oberst, U. y Carbonell, X. (2018). Diseño y aplicación de talleres educativos para el uso saludable de Internet y redes sociales en la adolescencia: descripción de un estudio piloto. *Pixel-Bit. Revista de Medios y Educación*, (52), 111-124. https://doi.org/10.12795/pixelbit.2018.i52.08

Rial Boubeta, A. (Dir.) (2021). *Impacto de la tecnología en la adolescencia. Relaciones, Riesgos y Oportunidades.* Unicef España.

Richardson, J., Martin, F. y Sauers, N. (2021). Systematic review of 15 years of research on digital citizenship: 2004-2019. *Learning, Media and Technology*, *46*(4), 498-514. https://doi.org/10.1080/17439884.2021.1941098

Rodríguez Román, M. (2022). Día de la seguridad en Internet: navegar seguro, una asignatura pendiente. *Radio Televisión Española*, 8 de febrero. https://www.rtve.es/noticias/20220208/dia-internacional-seguridad-internet/2285180.shtml

Román García, O., Bacigalupe, A. y Vaamonde, C. (2021). Relación de la pornografía mainstream con la salud sexual y reproductiva de los/las adolescentes. Una revisión de alcance. *Revista Española de Salud Pública*, *95*.

Sánchez-Meca, J. y Botella, J. (2015). *Meta-análisis en ciencias sociales y de la salud*. Síntesis.

Save the Children (2020). *(Des)Información sexual: pornografía y adolescencia*. https://www.savethechildren.es/sites/default/files/2020-11/Informe_Desinformacion_sexual-Pornografia_y_adolescencia.pdf

Save the Children (2022). *Ciberacoso o ciberbullying.* https://www.savethechildren.es/donde/espana/violencia-contra-la-infancia/ciberacoso-ciberbullying

Síndic de Greuges (2022). *La protección de los niños y los adolescentes en el entorno digital.* https://www.sindic.cat/site/unitFiles/9018/Informe%20redes%20digitales_cast_def.pdf

Silber-Varod, V., Eshet-Alkalai, Y. y Geri, N. (2019). Tracing research trends of 21st-century learning skills. *British Journal of Educational Technology*, *50*(6), 3099-3118. http://dx.doi.org/10.1111/bjet.12753