COMPARATIVE ANALYSIS OF DIGITAL SAFETY TRAINING PROGRAMS FOR MINORS

Marcos Gómez-Puerta
Universidad de Alicante
marcos.gomez@ua.es
Esther Chiner
Universidad de Alicante
Andrea Oliver-Ridaura
Universidad de Alicante

Estos autores contribuyeron por igual en este trabajo

Received: 13 abril 2025
Revised: 17 abril 2025
Evaluator 1 report: 23 abril 2025
Evaluator 2 report: 27 abril 2025
Accepted: 20 mayo 2025
Published: mayo 2025

RESUMEN

Aunque el entorno digital ofrece numerosas oportunidades para el aprendizaje, la comunicación y el ocio de los menores también implica riesgos como el ciberacoso, la exposición a contenidos inadecuados, los problemas de privacidad o la dependencia de las pantallas. Esta situación plantea un reto a los centros educativos y a las políticas públicas, que deben prevenir dichos riesgos y promover un uso seguro y responsable de la tecnología. La educación para la competencia digital debe ir más allá del dominio técnico, integrando también la comprensión crítica de los entornos digitales y la participación ética en ellos. En este contexto, se presenta un análisis comparado de nueve programas de formación en seguridad digital para menores, desarrollados en distintos países y promovidos por entidades públicas, académicas y del tercer sector. El objetivo es identificar patrones comunes, divergencias y vacíos que permitan orientar futuras líneas de acción en alfabetización digital crítica y prevención de riesgos online. El análisis de contenido se ha basado en temas y categorías previamente definidos, examinando objetivos, población destinataria, contenidos, metodología, implementación, evaluación, accesibilidad, inclusión y sostenibilidad. Los programas analizados incluyen iniciativas consolidadas como KiVa, eSafety Commissioner o IS4K, así como propuestas más recientes como CODI, Demo Days, Cyberprogram 2.0, Safety.Net, ConRed y Líderes Digitales. Los resultados evidencian una convergencia en el enfoque preventivo y en la atención al ciberacoso, la privacidad y el uso seguro de redes sociales, con la formación docente como pilar esencial. Sin embargo, se detectan diferencias en el alcance territorial, la inclusión de alumnado vulnerable y el tratamiento de riesgos emergentes. Se concluye la necesidad de avanzar hacia programas más inclusivos, evaluables y participati-

vos, donde también los estudiantes sean protagonistas activos de la construcción de entornos digitales seguros, éticos e inclusivos.

Palabras clave: competencia digital; programas formativos; riesgos online; mediación; centros educativos

ABSTRACT

Comparative analysis of digital safety training programs for minors. Although the digital environment offers numerous opportunities for learning, communication, and leisure for minors, it also presents risks such as cyberbullying, exposure to inappropriate content, privacy issues, or screen dependency. This situation poses a challenge for educational institutions and public policies, which must prevent these risks and promote safe and responsible use of technology. Digital literacy education must go beyond technical proficiency, also integrating critical understanding of digital environments and ethical participation within them. In this context, a comparative analysis of nine digital safety training programmes for minors, developed in various countries and promoted by public, academic, and third-sector entities, is presented. The aim is to identify common patterns, divergences, and gaps that will help guide future actions in critical digital literacy and online risk prevention. The content analysis has been based on predefined themes and categories, examining objectives, target population, content, methodology, implementation, evaluation, accessibility, inclusion, and sustainability. The programmes analysed include established initiatives such as KiVa, eSafety Commissioner, and IS4K, as well as newer proposals such as CODI, Demo Days, Cyberprogram 2.0, Safety.Net, ConRed, and Líderes Digitales. The results reveal a convergence in the preventive approach and focus on cyberbullying, privacy, and safe use of social networks, with teacher training as a key pillar. However, differences in territorial scope, the inclusion of vulnerable students, and the treatment of emerging risks are identified. The need to move towards more inclusive, evaluable, and participatory programmes is concluded, where students also play an active role in building safe, ethical, and inclusive digital environments.

Keywords: digital literacy; training programmes; online risks; mediation; educational institutions

INTRODUCCIÓN

El entorno digital ofrece a los menores una amplia gama de oportunidades para el aprendizaje, la comunicación y el ocio. Sin embargo, junto con estos beneficios, también surgen una serie de riesgos asociados al uso de las tecnologías, como el ciberacoso, la exposición a contenidos inapropiados, los problemas de privacidad o la adicción a las pantallas, entre otros. Estos riesgos pueden tener consecuencias negativas para el bienestar emocional y físico de los menores, afectando su desarrollo social y académico (Finkelhor, Walsh et al., 2021). A medida que la conectividad digital se expande, los centros educativos y las políticas públicas enfrentan el desafío de ofrecer una formación adecuada que no solo prevenga estos riesgos, sino que también promueva un uso responsable y seguro de la tecnología. En este contexto, la alfabetización digital se ha consolidado como un componente esencial en la educación moderna.

No obstante, la competencia digital del estudiantado debe trascender el simple dominio técnico de las herramientas digitales e incluir una comprensión crítica de los entornos digitales para promover la participación ética de los estudiantes en estos espacios (Walsh et al., 2022). Como señalan Finkelhor, Walsh et al. (2021), un aspecto clave de la educación digital es proporcionar a los menores las herramientas necesarias para navegar de manera segura por internet, sensibilizándolos sobre los riesgos potenciales y enseñándoles estrategias efectivas de protección, así como pautas adecuadas de comportamiento online para evitar comportamientos inadecuados. Aunque la alfabetización digital tradicionalmente ha priorizado la privacidad como una habilidad clave, estudios recientes han cuestionado este enfoque. Finkelhor, Jones et al. (2021) argumentan que enseñar a los menores solo sobre privacidad no es suficiente para prevenir los riesgos más graves ya que no se abordan adecuadamente problemas como el acoso sexual en línea o el fraude. Así, los programas deben centrarse en enseñar a los menores a reconocer y gestionar los riesgos específicos que enfrentan, como el ciberacoso o la manipulación en línea. Además, la enseñanza de habilidades socioemocionales, como la toma de decisiones informadas, la empatía y la

gestión de emociones, es fundamental para prevenir comportamientos inseguros en la red. Estos enfoques, orientados al manejo de situaciones específicas de riesgo, son más eficaces para proteger a los menores en comparación con los enfoques centrados exclusivamente en la privacidad.

Asimismo, la implementación de programas de seguridad digital para menores presenta varios desafíos. En primer lugar, los programas deben ser inclusivos, accesibles y adaptados a las diversas realidades de los estudiantes, incluidos aquellos con necesidades específicas de apoyo educativo (Sâglam et al., 2023). Además, los enfoques deben ser actualizados de manera constante para abordar los riesgos emergentes que surgen con el avance de las tecnologías y las nuevas formas de interacción digital (Finkelhor et al., 2020). Esto subraya la importancia de basar la educación digital en un enfoque integral, que no solo se limite a la formación técnica, sino que también abarque aspectos éticos, sociales y de salud relacionados con el uso de las tecnologías (Walsh et al., 2022).

Consecuentemente, este trabajo se propuso realizar un análisis crítico y comparado de nueve programas de formación en seguridad digital para menores, desarrollados en diversos contextos internacionales y promovidos por entidades públicas, académicas y del tercer sector. A través de este análisis, se busca identificar patrones comunes, divergencias y vacíos en las estrategias de alfabetización digital que puedan guiar futuras líneas de acción en la prevención de riesgos online. De este modo se espera proporcionar una evaluación crítica de las metodologías empleadas, la efectividad de los programas y su capacidad para incluir a los menores más vulnerables. Los objetivos específicos de este análisis son los siguientes:

Identificar las características comunes y las diferencias entre los programas analizados.

Examinar cómo los programas abordan la inclusión y los riesgos emergentes.

Describir posibles lagunas en el abordaje de la formación de la seguridad digital en menores.

MÉTODO

Diseño de la investigación

Este estudio sigue un enfoque cualitativo mediante observación no participante indirecta, centrado en el análisis de contenido disponible públicamente en las webs y documentos relacionados con nueve programas de formación en seguridad digital para menores. El análisis de contenido es una técnica que permite interpretar y extraer patrones significativos de los textos disponibles, facilitando una comprensión más profunda de los enfoques, objetivos y metodologías empleadas en los programas seleccionados. La investigación se basa en una plantilla de temas prefijados, que permite organizar y comparar los programas en función de diversas categorías clave, tales como los objetivos de formación, la metodología utilizada, la accesibilidad, la inclusión y la sostenibilidad.

Contexto y participantes

Los programas analizados están disponibles online y son promovidos por diversas entidades públicas, académicas y del tercer sector. Dado que los programas son accesibles principalmente a través de internet, la investigación se centra en el análisis de la información pública disponible en las plataformas digitales de cada uno de los programas. A través de este análisis, se pretende identificar patrones comunes y diferencias en los enfoques de los programas, sin necesidad de la interacción directa con los participantes o de un enfoque experimental. En la Tabla 1 se presentan los nueve programas seleccionados para este análisis.

Tabla 1. Descripción de los programas de formación en seguridad digital para menores

Programa	Entidad responsable	Enfoque	Población objetivo	Fuente
KiVa	Universidad de Turku	Prevención del ciberacoso	Estudiantes de Primaria y Secundaria	(University of Turku, 2025)
eSafety	Gobierno de Australia	Seguridad en línea, prevención de riesgos	Estudiantes y educadores	(Australian Government, 2019)
IS4K	Instituto Nacional de Ciberseguridad (INCIBE)	Ciberseguridad y protección infantil	Niños, adolescentes y familias	(INCIBE, 2025)
CODI	Generalitat Valenciana	Alfabetización digital y gestión de riesgos	Estudiantes y docentes	(Generalitat Valenciana, 2025)
Demo Days	Junta de Castilla y León (CyL Digital)	Formación práctica en herramientas digitales	Población general	(Junta de Castilla y León, 2025)
Cyberprogram 2.0	Fundación Ciberseguridad	Prevención de riesgos cibernéticos	Estudiantes y educadores	(Garaigordobil Landazabal & Martínez-Valderrey, 2014)
Safety.Net	Fundación Global	Prevención de riesgos en redes sociales	Adolescentes y jóvenes	(Ortega-Barón et al., 2021)
ConRed	Generalitat Valenciana	Prevención de ciberacoso y riesgos online	Estudiantes de Primaria y Secundaria	(Junta de Andalucía, 2020)
Líderes Digitales	Fundación Telefónica	Alfabetización digital y liderazgo online	Jóvenes y educadores	(Plena Inclusión, 2022)

Instrumentos y análisis de contenido

El análisis de contenido temático se realizó atendiendo a unas temáticas prefijadas, que abarcaban las siguientes categorías:

Objetivos del programa. Qué buscan lograr los programas (prevención de riesgos, educación para la competencia digital, etc.).

Metodología. Enfoques educativos, actividades y recursos utilizados (formación presencial, recursos digitales, talleres, etc.).

Población destinataria. A quién está dirigido el programa (estudiantes, familias, docentes).

Evaluación. Métodos de evaluación utilizados para medir la efectividad de los programas.

Accesibilidad e inclusión. Consideración de la accesibilidad para diferentes grupos de estudiantes, incluyendo a aquellos con necesidades educativas especiales.

Sostenibilidad. Estrategias para asegurar la continuidad y/o actualización del programa a largo plazo.

El análisis se basó en la identificación de temas en los documentos y en las páginas web de los programas, para identificar similitudes y diferencias en los enfoques adoptados, y para evaluar cómo abordan las necesidades de los menores en el contexto de la seguridad digital.

Procedimiento y análisis de la información

La localización y análisis de los programas se llevó a cabo durante el primer trimestre de 2025, a través de una revisión exhaustiva de los documentos y recursos disponibles en las plataformas digitales de los programas seleccionados. Cada programa fue analizado en función de los temas prefijados y según el instrumento de recogida de datos (plantilla de temas y categorías) para organizar los datos y así asegurar una comparación coherente entre los diferentes programas. Este estudio se enmarca en el proyecto i-EDUMED, que se realiza respetando los principios éticos y las normativas de investigación de la Universidad de Alicante (ref. UA-2022-10-28), que garantiza que todos los procedimientos se realizan de manera ética y respetuosa con los derechos de los participantes y las instituciones involucradas.

RESULTADOS

Convergencias y divergencias entre los programas formativos analizados

Los nueve programas analizados presentan tanto características comunes como diferencias importantes en su enfoque hacia la seguridad digital para menores. A continuación, se describen los aspectos clave:

Enfoque preventivo y formativo. Todos los programas comparten un enfoque preventivo centrado en la educación de los menores sobre los riesgos en línea, especialmente el ciberacoso, la exposición a contenidos inapropiados y el manejo de la privacidad. Sin embargo, la metodología empleada varía considerablemente. Programas como KiVa y Cyberprogram 2.0 adoptan un enfoque integral que incluye talleres para estudiantes, formación para docentes y estrategias de sensibilización para las familias, mientras que otros, como eSafety y IS4K, priorizan recursos digitales y formación en línea, con un enfoque más autodidacta.

Metodología educativa. Existen diferencias notables en la metodología empleada. Mientras que KiVa se basa en un programa estructurado que implica a toda la comunidad educativa (estudiantes, docentes y familias) en un proceso continuo, otros programas, como Líderes Digitales o ConRed, emplean metodologías participativas que involucran activamente a los estudiantes en la creación de contenidos y en el liderazgo en el ámbito digital.

Accesibilidad y adaptabilidad. La mayoría de los programas, como Safety.Net y CODI, están diseñados para ser fácilmente accesibles, con recursos en línea disponibles en múltiples plataformas. Sin embargo, algunos programas, como Demo Days y Líderes Digitales, se enfocan más en actividades presenciales, lo que puede limitar su alcance en áreas con acceso limitado a recursos tecnológicos.

Cobertura geográfica. Existe una clara diferencia en el alcance territorial de los programas. Algunos, como IS4K y eSafety, tienen una cobertura nacional o internacional, mientras que otros, como ConRed y Líderes Digitales, se concentran principalmente en España o en áreas específicas de ciertos países.

Abordaje de la inclusión y los riesgos emergentes

En cuanto a la inclusión y el tratamiento de los riesgos emergentes, los programas presentan diferentes enfoques y niveles de atención:

Inclusión de estudiantes vulnerables. Algunos programas, como KiVa, Cyberprogram 2.0 o CODI, incluyen mecanismos específicos para abordar las necesidades de los estudiantes más vulnerables, como aquellos con discapacidad intelectual o con dificultades en el acceso a las tecnologías. Estos programas proporcionan recursos y estrategias adaptadas a las diversas necesidades de los estudiantes, garantizando la participación de todos los grupos en el proceso educativo. En contraste, programas como Demo Days y Safety.Net no presentan una mención explícita a la adaptación para grupos vulnerables o bien no se orientan a ellos, lo que podría limitar la accesibilidad y efectividad en contextos más diversos.

Tratamiento de riesgos emergentes. Los riesgos emergentes como el *sexting*, el *grooming* y la adicción a las pantallas son abordados de manera variable. Programas como eSafety y Safety.Net ofrecen recursos específicos para tratar estos temas mediante la sensibilización sobre el comportamiento en línea y la creación de contenido seguro. En cambio, ConRed y Líderes Digitales se centran más en la prevención del ciberacoso y no profundizan tanto en otros riesgos emergentes relacionados con la interacción en redes sociales o plataformas de mensajería.

Preocupación por la gestión de la privacidad. Aunque todos los programas abordan la importancia de la privacidad en línea, algunos, como IS4K y CODI, prestan más atención a la enseñanza de herramientas y recursos para gestionar la privacidad de los menores en plataformas digitales. Sin embargo, otros programas, como Cyberprogram 2.0, abordan la privacidad de manera más general, sin entrar en detalles sobre la gestión de datos personales en plataformas digitales específicas.

Lagunas en el abordaje de la formación de la seguridad digital en menores

A pesar de los avances y esfuerzos de los programas analizados, se han identificado varias lagunas en el abordaje de la formación en seguridad digital para menores:

Falta de formación integral para la comunidad educativa. Aunque muchos programas ofrecen formación para estudiantes, hay una clara falta de estrategias que involucren de manera más directa a toda la comunidad educativa, incluyendo a padres, cuidadores y administradores escolares. Programas como KiVa y Cyberprogram 2.0 han hecho avances en este sentido, pero otros, como Demo Days y Safety.Net, se limitan a intervenciones centradas en los estudiantes o en aplicaciones concretas sin necesariamente proporcionar suficiente formación y recursos para los educadores y las familias.

Enfoque limitado en la diversidad funcional, cultural y social. Los programas analizados no siempre consideran adecuadamente las diversas realidades funcionales, culturales y sociales de los estudiantes, especialmente en contextos internacionales. Programas como Líderes Digitales y ConRed están más enfocados en contextos nacionales específicos (España), lo que puede dificultar su aplicabilidad en otros países con diferentes problemáticas relacionadas con la seguridad digital.

Desactualización frente a riesgos emergentes. Algunos programas presentan una desconexión con los riesgos emergentes más actuales, como la manipulación a través de algoritmos, la desinformación, la inteligencia artificial (IA), o los retos virales en las redes sociales. Aunque se abordan temas como el ciberacoso o la privacidad, la formación no siempre incluye enfoques actualizados sobre las nuevas formas de riesgo en línea que afectan a los menores. Esto indica una laguna en la actualización de los programas frente a las rápidas transformaciones del entorno digital.

Evaluación insuficiente. Muchos programas carecen de sistemas de evaluación formales o presentan evaluaciones limitadas a aspectos técnicos, como la entrega de contenidos o la participación de los estudiantes. Sin embargo, es necesario un enfoque más robusto que evalúe la eficacia y el impacto real de los programas en términos de cambio de comportamientos, conocimientos adquiridos y, lo más importante, la protección real frente a los riesgos digitales.

DISCUSIÓN Y CONCLUSIONES

Discusión

El propósito de este estudio fue realizar un análisis comparado de nueve programas de formación en seguridad digital para menores, con el fin de identificar sus características comunes y diferencias, examinar cómo abordan la inclusión y los riesgos emergentes, y describir las posibles lagunas en su enfoque.

Desde la introducción de este estudio, se resaltó la importancia de un enfoque que no solo se centre en el dominio técnico de las herramientas digitales, sino que también promueva la comprensión crítica de los entornos

digitales y fomente una participación ética de los estudiantes. En este sentido, los resultados obtenidos refuerzan esta premisa ya que la mayoría de los programas adoptan un enfoque preventivo que incluye la sensibilización sobre el ciberacoso y la gestión de la privacidad. Sin embargo, como señalan Finkelhor, Jones et al. (2021), los programas que se centran exclusivamente en estos aspectos tradicionales no son suficientes para abordar los riesgos emergentes. Los programas como Safety.Net y eSafety, que priorizan la formación autodidacta y digital, se alinean mejor con las recomendaciones de Finkelhor, Jones et al. (2021) sobre la necesidad de proporcionar herramientas más prácticas y específicas para la gestión de riesgos

En cuanto a la inclusión, algunos programas han integrado recursos específicos para estudiantes vulnerables, como los de KiVa y Cyberprogram 2.0, lo cual refleja el enfoque inclusivo y accesible que Finkelhor, Walsh et al. (2021) consideran necesario para garantizar que todos los estudiantes, independientemente de su contexto, puedan beneficiarse de una formación efectiva en seguridad digital. Sin embargo, otros programas, como Safety.Net y Demo Days, no presentan un enfoque explícito hacia la inclusión de estudiantes con necesidades especiales o aquellos que enfrentan barreras tecnológicas, lo que puede limitar el impacto de la formación en estos grupos. Respecto al tratamiento de los riesgos emergentes, los programas que abordan el *sexting*, el *grooming* y la adicción a las pantallas, como eSafety y Safety.Net, están en línea con las recomendaciones de Finkelhor, Jones et al. (2021). Sin embargo, algunos riesgos emergentes, como la manipulación de algoritmos, la desinformación o la adicción a la tecnología, no son suficientemente tratados en los programas analizados, lo que refleja una desconexión con los rápidos avances en el entorno digital. En este aspecto, la necesidad de una actualización constante de los programas de seguridad digital se hace patente.

Respecto de las lagunas identificadas, una de las principales es la falta de formación integral para la comunidad educativa, especialmente en programas como Demo Days y Safety.Net, que se centran en los estudiantes sin necesariamente involucrar a sus familias o educadores. Esta falta de enfoque integral va en contra de las recomendaciones de Finkelhor, Walsh et al. (2021), quienes destacan la importancia de que los programas incluyan a todas las partes interesadas en la creación de entornos digitales seguros. Los programas que adoptan un enfoque comunitario, como KiVa y Cyberprogram 2.0, demuestran ser más efectivos en este sentido, ya que implican a estudiantes, docentes y familias en el proceso educativo, lo que favorece una respuesta más cohesionada ante los riesgos en línea. La diversidad funcional, cultural y social de los estudiantes también fue identificada como un aspecto que no siempre se aborda de manera adecuada. Los programas que se centran en contextos nacionales específicos, como Líderes Digitales y ConRed, pueden tener dificultades para ser implementados de manera efectiva en otros países con diferentes realidades. Este aspecto resalta la necesidad de un diseño más flexible de los programas, que permita adaptarse a diversas situaciones y contextos.

Implicaciones

Los programas de formación en seguridad digital deben evolucionar hacia modelos más inclusivos, integrales y dinámicos, que consideren las necesidades y contextos de todos los menores, sin excepción. Actualmente, muchos de los programas evaluados se centran en los estudiantes, pero ignoran a otros actores clave en la educación digital, como las familias y los docentes, omitiendo una recomendación clave en este tipo de intervenciones (Finkelhor, Walsh, et al., 2021). Consecuentemente, las familias y el profesorado deben actuar como mediadores que faciliten el aprendizaje y la integración de la seguridad digital de los menores, intentando lograr la necesaria coherencia y consistencia en las actuaciones. Las familias, en este sentido, resultan aliados esenciales en el proceso educativo, especialmente en la prevención de riesgos como el ciberacoso o la adicción a las pantallas. Por otra parte, los programas de seguridad digital deben ser dinámicos para adaptarse a un entorno digital cambiante. Las amenazas en línea evolucionan rápidamente y los menores enfrentan nuevos tipos de riesgos, como la desinformación, los algoritmos manipuladores y la interacción con contenido generado por IA. Este tipo de riesgos no puede abordarse con enfoques tradicionales o estáticos. Por ende, los programas deben integrar constantemente nuevas estrategias que

incluyan no solo el manejo de herramientas digitales básicas, sino también la alfabetización crítica para que los menores desarrollen un pensamiento reflexivo sobre lo que consumen y cómo interactúan en línea. Para esto, se requiere que los programas se actualicen de manera continua y se adapten a la realidad tecnológica de cada momento. La educación digital debe ser entendida como un proceso continuo y adaptativo, no un evento puntual, para asegurar que los menores estén preparados para afrontar los desafíos digitales presentes y futuros.

Limitaciones y futuras líneas de investigación y desarrollo

Este estudio, de carácter meramente exploratorio y limitado en su alcance, presenta varias limitaciones significativas que deben ser consideradas al interpretar los resultados. Una de las principales limitaciones es la falta de datos empíricos sobre la efectividad real de los programas de formación en seguridad digital. Aunque se ha analizado la información disponible públicamente sobre los programas, no se dispone de datos que midan su impacto directo en los comportamientos y actitudes de los menores. La evaluación de los programas es crucial para determinar si realmente están logrando los objetivos propuestos, como la reducción de riesgos en línea y la mejora en la competencia digital de los estudiantes. Para superar esta limitación, futuros estudios deberían incorporar metodologías más directas, como encuestas a estudiantes, entrevistas a docentes y padres, y análisis longitudinales que permitan observar el cambio en los comportamientos de los menores a lo largo del tiempo. Otra área clave que necesita más atención es el uso de tecnologías emergentes en la educación para la seguridad digital. Por ejemplo, la IA podría desempeñar un papel importante en la personalización de los programas de formación. La IA tiene el potencial de adaptar los contenidos y las estrategias pedagógicas a las necesidades individuales de los estudiantes, lo que aumentaría la efectividad de los programas y permitiría un aprendizaje más eficaz. La personalización de los programas podría también ayudar a abordar los riesgos emergentes de manera más específica, adaptando las intervenciones educativas a los cambios rápidos del entorno digital. Además, la integración de nuevas herramientas de evaluación debería ser un área de investigación clave en el futuro. A medida que los programas educativos en seguridad digital evolucionan, se requieren nuevas métricas de evaluación que vayan más allá de la simple participación de los estudiantes. Los estudios futuros deberían considerar evaluaciones más profundas que midan el impacto real en la protección de los menores y en su comportamiento en línea, así como el nivel de adopción de habilidades digitales críticas.

Conclusiones

Este estudio ha demostrado que los programas de formación en seguridad digital son esenciales para proteger a los menores de los riesgos digitales. Sin embargo, se han identificado áreas de mejora, como la falta de implicación de las familias y los docentes. Los programas deben involucrar a toda la comunidad educativa para ser más efectivos. Además, muchos programas no están suficientemente actualizados para abordar los nuevos riesgos digitales, como la desinformación y los algoritmos manipuladores. Es necesario que los programas se adapten para preparar a los menores ante estos desafíos de manera ética y responsable. También, la mayoría carece de evaluaciones robustas que midan su impacto real, lo que impide medir su efectividad en la prevención de riesgos y la mejora de competencias digitales. Por lo tanto, los programas deben ser más inclusivos y participativos, involucrando activamente a familias y docentes. También deben actualizarse continuamente y tener sistemas de evaluación sólidos para garantizar que no solo protejan a los menores, sino que los empoderen para navegar de manera segura y ética.

Financiación

Esta publicación es parte del proyecto PID2021-122320NA-I00 financiado por MICIU/AEI/10.13039/501100011033/ y FEDER/UE.

REFERENCIAS BIBLIOGRÁFICAS

Australian Government. (2019). *Being safe online*. eSafety Education; Australian Government. https://www.esafety.gov.au/sites/default/files/2020-02/Easy%20English-Being%20Safe%20Online.pdf?v=1746101002145

Finkelhor, D., Jones, L., & Mitchell, K. (2021). Teaching privacy: A flawed strategy for children's online safety. *Child Abuse & Neglect*, *117*. https://doi.org/10.1016/J.CHIABU.2021.105064

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2021). Youth internet safety education: Aligning programs with the evidence base. *Trauma, Violence, & Abuse*, *22*(5), 1233–1247. https://doi.org/10.1177/1524838020916257

Garaigordobil Landazabal, M., & Martínez-Valderrey, V. (2014). *Cyberprogram 2.0. Programa de intervención para prevenir y reducir el ciberbullying*. Pirámide.

Generalitat Valenciana. (2025). *Programa CODI. Programa de competencias digitales para la infancia.* https://ceice.gva.es/es/web/innovacion-calidad/programa-codi#publics-nov

INCIBE. (2025). *is4k - Internet segura for kids*. Menores. https://www.incibe.es/menores/

Junta de Andalucía. (2020). *Programa CONRED Andalucía para la Prevención del Acoso Escolar y el Ciberacoso en Entornos Educativos*. Planes y Programas de La Consejería de Desarrollo Educativo y Formación Profesional. https://www.juntadeandalucia.es/organismos/desarrolloeducativoyformacionprofesional/consejeria/transparencia/planificacion-evaluacion-estadistica/planes/detalle/240680.html

Junta de Castilla y León. (2025). *Demo Days*. CyL Digital. https://www.cyldigital.es/demo-days

Ortega-Barón, J., González-Cabrera, J., Machimbarrena, J. M., & Montiel, I. (2021). Safety.Net: A pilot study on a multi-risk internet prevention program. *International Journal of Environmental Research and Public Health, 18*(8), 4249. https://doi.org/10.3390/IJERPH18084249

Plena Inclusión. (2022). *Uso de internet y seguridad. Líderes Digitales.* https://www.plenainclusion.org/publicaciones/buscador/lideres-digitales-2-uso-de-internet-y-seguridad/

Saglam, R. B., Miller, V., & Franqueira, V. N. L. (2023). A systematic literature review on cybersecurity education for children. *IEEE Transactions on Education*, *66*(3), 274–286. https://doi.org/10.1109/TE.2022.3231019

University of Turku. (2025). *KiVa Program*. https://www.kivaprogram.net/

Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., Serry, E., Trotter, S., Spanos, T., & Rogic, N. (2022). Best practice framework for online safety education: Results from a rapid review of the international literature, expert review, and stakeholder consultation. *International Journal of Child-Computer Interaction*, *33*, 100474. https://doi.org/10.1016/j.ijcci.2022.100474