COVER PAGE IN ENGLISH

Technological Cybersecurity Strategies for the Digital Protection of Adolescents: A Systematic Review

Geovanna Tacuri Gutierrez, Bach., Zatta Silva Cesar Augusto, master[2]
[1,2]Universidad Tecnológica del Perú, Perú, *U20240020@utp.edu.pe, c20237@utp.edu.pe*

Abstract – The growing exposure of adolescents to digital risks—such as cyberbullying, loss of privacy, information manipulation, and contact with strangers—has prompted the development of specific technological strategies to protect them in virtual environments. This Systematic Literature Review (SLR) aims to identify, classify, and analyze cybersecurity strategies designed to safeguard adolescents, evaluating their characteristics, underlying technologies, effectiveness levels, and application contexts. Method: Following the PICOC framework and PRISMA guidelines, a systematic search was conducted in the Scopus database for articles published between 2020 and 2025. After applying inclusion and exclusion criteria, 30 relevant studies were selected and analyzed. Results: The strategies identified leveraged technologies such as artificial intelligence, automated parental control, educational gamification, and adaptive authentication systems. Conclusions: The most effective solutions combined pedagogical and technological approaches, emphasizing personalization, real-time monitoring, and active engagement of both adolescents and responsible adults. Future research should adopt longitudinal designs with broader geographic diversity, and public policies should reinforce digital literacy and child safety in online environments.

Keywords: adolescents; cybersecurity; technological strategies; digital protection.

Estrategias Tecnológicas de Ciberseguridad para la Protección Digital de Adolescentes: Una Revisión Sistemática

Geovanna Tacuri Gutierrez, Bach., Zatta Silva Cesar Augusto, master[2]
[1,2]Universidad Tecnológica del Perú, Perú, *U20240020@utp.edu.pe, c20237@utp.edu.pe*

Resumen– ***La creciente exposición de los adolescentes a riesgos digitales como el ciberacoso, la pérdida de privacidad, la manipulación informativa y el contacto con desconocidos ha motivado el desarrollo de estrategias tecnológicas específicas para su protección en entornos virtuales. Esta Revisión Sistemática de la Literatura (RSL) tiene como objetivo identificar, clasificar y analizar las estrategias de ciberseguridad diseñadas para salvaguardar a los adolescentes, evaluando sus características, tecnologías utilizadas, niveles de efectividad y contexto de aplicación. Método: se aplicó el modelo PICOC y los lineamientos PRISMA para realizar una búsqueda sistemática en la base de datos Scopus, incluyendo artículos publicados entre 2020 y 2025. Tras aplicar criterios de inclusión y exclusión, se seleccionaron 30 estudios relevantes. Resultados: Las estrategias identificadas se basaron en tecnologías como inteligencia artificial, control parental automatizado, gamificación educativa y sistemas de autenticación adaptativa. Conclusiones: Las soluciones más efectivas integraron enfoques pedagógicos y tecnológicos, priorizando la personalización, el monitoreo en tiempo real y la participación activa de adolescentes y adultos responsables. Se destaca la necesidad de investigaciones futuras con diseños longitudinales y mayor diversidad geográfica, así como de políticas públicas que fortalezcan la alfabetización digital y la seguridad infantil en el entorno virtual.***

Palabras clave-- ***adolescentes, ciberseguridad, estrategias tecnológicas, protección digital.***

I. INTRODUCCIÓN

En la era digital contemporánea, los adolescentes se han convertido en uno de los grupos más activos y, al mismo tiempo, más vulnerables dentro de los entornos en línea. Su interacción constante con redes sociales, videojuegos, plataformas de mensajería y entornos educativos virtuales les ofrece oportunidades significativas para el aprendizaje y la socialización. Sin embargo, esta exposición también los enfrenta a riesgos digitales cada vez más complejos, como el ciberacoso, la exposición a contenidos inapropiados, el contacto con desconocidos, el robo de datos personales y la manipulación algorítmica [1], [2]. Según un informe de UNICEF, uno de cada tres usuarios de Internet en el mundo es menor de edad, y muchos de ellos carecen de los conocimientos y habilidades necesarios para proteger su privacidad y seguridad en línea [3].

Este escenario plantea un problema crítico para la sociedad contemporánea: la falta de estrategias tecnológicas de ciberseguridad diseñadas específicamente para el perfil emocional, cognitivo y social de los adolescentes. Si bien existen múltiples herramientas de supervisión parental y monitoreo, muchas de estas han sido desarrolladas desde una perspectiva adultocéntrica, sin considerar principios fundamentales de accesibilidad, participación juvenil y usabilidad efectiva [4], [5]. Asimismo, los enfoques tienden a estar fragmentados, con predominio de soluciones técnicas centradas en el control externo, en detrimento de estrategias integradoras basadas en la alfabetización digital, la prevención y el desarrollo de habilidades socioemocionales [6], [7].

Frente a esta realidad, diferentes investigaciones han subrayado la urgencia de implementar estrategias de ciberseguridad que no se limiten únicamente al control o la vigilancia, sino que promuevan la autonomía digital, la autorregulación, la participación activa del adolescente y una comprensión crítica del entorno digital [8], [9]. La literatura evidencia una proliferación de soluciones parciales (aplicaciones, algoritmos, programas educativos), pero persiste una carencia de estudios integradores que sistematicen estas propuestas, evalúen su efectividad y definan estándares de calidad, aplicabilidad y sostenibilidad a largo plazo [10], [11].

En este contexto, la presente Revisión Sistemática de Literatura (RSL) tuvo como objetivo identificar, clasificar y evaluar críticamente las estrategias tecnológicas de ciberseguridad desarrolladas o implementadas para la protección digital de adolescentes, con base en estudios científicos publicados entre 2020 y 2025 en bases de datos indexadas como Scopus. La finalidad es ofrecer una visión panorámica, rigurosa y actualizada del estado del arte, resaltando tanto las fortalezas como las debilidades de las soluciones existentes, y proporcionando lineamientos para su mejora y aplicación contextualizada.

Este documento se organiza de la siguiente manera: en la sección 2, Metodología, se detalla el diseño de la RSL, incluyendo el planteamiento de preguntas de investigación según el modelo PICOC, así como los criterios de búsqueda,

inclusión y exclusión de estudios, y el protocolo utilizado para el análisis cualitativo y cuantitativo. La sección 3, Resultados, presenta los hallazgos derivados del análisis de los estudios primarios seleccionados. En la sección 4, Discusión, se interpretan los resultados obtenidos, contrastándolos con investigaciones previas y discutiendo sus implicancias técnicas, educativas y sociales. Finalmente, la sección 5, Conclusión, sintetiza los principales hallazgos, señala las limitaciones de la investigación y propone líneas futuras para el desarrollo e implementación de estrategias más eficaces y contextualizadas.

I. METODOLOGÍA

Esta investigación se desarrolló como una Revisión Sistemática de Literatura (RSL), con enfoque cualitativo y sin metaanálisis, siguiendo los lineamientos metodológicos del modelo PRISMA. El objetivo fue identificar, clasificar y analizar las estrategias tecnológicas de ciberseguridad dirigidas a la protección digital de adolescentes, a partir de estudios científicos publicados entre los años 2020 y 2025.

La estrategia de búsqueda se fundamentó en el modelo PICO*C (Población, Intervención, Comparación, Resultado y Contexto)*, que permitió estructurar la pregunta principal y sus subcomponentes de forma lógica y coherente. La pregunta de investigación formulada fue: ¿Qué estrategias tecnológicas de ciberseguridad han sido investigadas y propuestas en la literatura científica para la protección digital de los adolescentes? A partir de esta se definieron las siguientes subpreguntas:

RQ1: ¿Qué características y riesgos enfrentaron los adolescentes en entornos digitales?
RQ2: ¿Qué tecnologías de ciberseguridad se utilizaron en las estrategias para proteger digitalmente a los adolescentes y cómo funcionaron?
RQ3: ¿Qué estrategias se utilizaron en los entornos educativos tradicionales para prevenir el acoso de adolescentes?
RQ4: ¿Qué niveles de efectividad se reportaron en los estudios en relación con la protección digital de adolescentes?

TABLA 1 - Componentes Pico

PICOC	Terms
P *Población*	Adolescentes expuestos a ciberacoso, grooming, phishing, etc.
I *Intervención*	Estrategias tecnológicas de ciberseguridad para la protección digital.
C *Comparación*	Estrategias no tecnológicas aplicadas en contextos educativos tradicionales
O *Resultados*	Efectividad de las estrategias tecnológicas en la protección digital de adolescentes.
C *Contexto*	Literatura científica y estudios académicos relacionados con entornos digitales o educativos.

La selección cuidadosa de palabras clave es esencial para garantizar la precisión y pertinencia de los resultados de una investigación. Al elegir términos adecuados, se puede enfocar la búsqueda en información específica y descartar resultados irrelevantes. Asimismo, estas comunican el alcance y los objetivos del estudio a otros investigadores, lo que contribuye a delimitar el tema de investigación y optimizar la búsqueda, selección y análisis de la literatura pertinente. La Tabla 2 presenta las estrategias de búsqueda para cada componente, utilizando las palabras clave del acrónimo PICOC.

TABLA 2 - Concatenación de la Cadena de Búsqueda

PALABRAS CLAVE		***CADENA DE BÚSQUEDA***
P	adolescentes, jóvenes, nativos digitales, usuarios en línea, estudiantes	*Adolescents OR teenagers OR youth OR "digital natives" OR "online users" OR students*
I	Estrategias de ciberseguridad, tecnologías de ciberseguridad, herramientas de seguridad en línea, estrategias de protección digital, monitoreo basado en IA, software de control parental, sistemas de autenticación.	*"cybersecurity strategies" OR "cybersecurity technologie" OR "online safety tools" OR "digital protection strategies" OR "AI-based monitoring" OR "parental control software" OR "authentication systems"*
C	Estrategias no tecnológicas, intervenciones escolares, programas de prevención tradicionales, educación presencial, programas antibullying, estrategias educativas.	*"non-technological strategies" OR "school-based interventions" OR "traditional prevention programs" OR "offline education" OR "anti-bullying programs" OR "educational strategies"*
O	eficacia, impacto, resultados, reducción de riesgos, seguridad digital, concienciación sobre ciberseguridad, resiliencia digital	*"effectiveness, impact" OR outcomes, "risk reduction" OR "digital safety" OR "cybersecurity awareness" OR "digital resilience"*
C	literatura científica, estudios académicos, contexto educativo, entorno digital, ciberespacio, entorno escolar	*"scientific literature" OR "academic studies" OR "educational context" OR "digital environment" OR cyberspace OR "school setting"*

Con el fin de realizar una revisión sistemática exhaustiva, se seleccionó la base de datos Scopus como principal fuente de información. Esta base de datos permite localizar estudios relevantes sobre el tema de investigación. Scopus ofrece un amplio acceso a información científica de calidad, así como herramientas para analizar la producción académica, rastrear citas y evaluar el impacto de las investigaciones. Investigadores, académicos y diversas organizaciones utilizan Scopus para apoyar sus investigaciones facilitando el proceso para la toma de decisiones.

Tomando como referencia la pregunta de investigación formulada en las Tablas 3 y 4, se definieron los siguientes criterios para la selección de artículos.

TABLA 3 - CRITERIOS DE INCLUSIÓN

CI 1	Publicaciones que abordan estrategias tecnológicas de ciberseguridad enfocadas en la protección digital de adolescentes.

CI 2	Publicaciones centradas en adolescentes (10-19 años) o estudiantes de secundaria
CI 3	Artículos que exploren la protección digital, privacidad, ciberacoso o gestión de datos
CI 4	Investigaciones que incluyan características, enfoques o niveles de efectividad
CI 5	Publicaciones revisadas por pares (peer-reviewed): artículos, revisiones sistemáticas, estudios de caso, etc.
CI 6	Artículos publicados en los últimos 5 años (2020-2025)
CI 7	Artículos en inglés

Estos parámetros de inclusión y exclusión delimitaron el alcance del estudio y aseguraron la pertinencia de la información examinada.

TABLA 4 - CRITERIOS DE EXCLUSIÓN

CI 1	Estudios que no se centren en tecnologías o estrategias de ciberseguridad
CI 2	Investigaciones que traten únicamente sobre adultos, niños menores de 10 años o ancianos
CI 3	Artículos puramente teóricos o reflexivos sin aplicación tecnológica concreta
CI 4	Trabajos que solo aborden competencias digitales generales sin relación con la seguridad
CI 5	Literatura gris (tesis, blogs, ponencias no publicadas, informes sin revisión)
CI 6	Publicaciones fuera del rango de años 2020-2025
CI 7	Artículos en idiomas distintos al inglés.

Se llevó a cabo una Revisión Sistemática de la Literatura (RSL) siguiendo la metodología PRISMA, con el objetivo de identificar estudios relevantes relacionados con estrategias tecnológicas de ciberseguridad orientadas a la protección digital de adolescentes.

Esta búsqueda permitió recopilar un conjunto inicial de 394 publicaciones científicas a partir de la base de datos Scopus. A continuación, se aplicaron filtros para acotar los resultados: primero, se restringió el rango de publicación entre 2020 y 2025, reduciendo el total a 263 documentos. Luego, se seleccionaron únicamente artículos científicos, revisiones y conferencias (article, review, conference paper), quedando 231 registros. Al limitar la búsqueda al idioma inglés, se obtuvieron 227 publicaciones. Posteriormente, se filtró por área temática relevante, lo cual redujo el número a 160 documentos. Al aplicar el criterio de acceso abierto (Open Access), se conservaron 53 publicaciones.

Después, se realizó una revisión de los títulos y resúmenes (mediante la opción Show abstract), seleccionando 39 artículos con potencial relevancia. Posteriormente, tras analizar las introducciones y aplicar los criterios de inclusión y exclusión previamente definidos, se seleccionaron 30 artículos finales para formar parte de la Revisión Sistemática de la Literatura (RSL). Estos estudios cumplen con los criterios establecidos, priorizando investigaciones empíricas, revisiones sistemáticas y artículos revisados por pares que abordan directamente el diseño, implementación o evaluación de estrategias tecnológicas de ciberseguridad aplicadas a adolescentes.

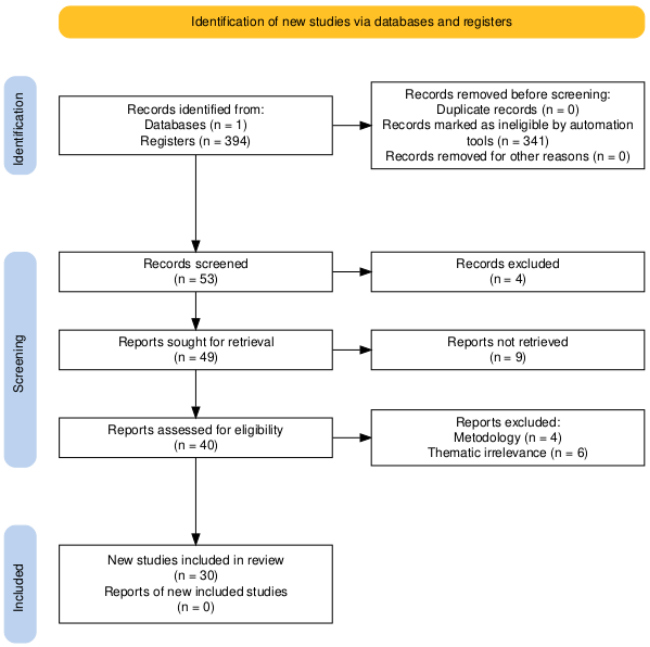

Fig. 1 Flujograma PRISMA

II. RESULTADOS

A continuación, se presenta el análisis de los artículos seleccionados tras la aplicación de las metodologías PICOC y PRISMA, con el propósito de identificar los términos clave más vinculados al tema de investigación, así como las principales contribuciones de los autores, los enfoques metodológicos utilizados, las métricas e indicadores implementados, y la valoración de las respuestas obtenidas en función del enfoque PICOC. Todo ello con el fin de identificar las estrategias tecnológicas de ciberseguridad investigadas y propuestas para la protección digital de adolescentes.

A. Panorama general de los estudios seleccionados

La investigación en torno al desarrollo de estrategias tecnológicas de ciberseguridad orientadas a la protección digital de los adolescentes ha experimentado una evolución significativa en los últimos cinco años, tal como lo reflejan los 30 estudios seleccionados para este análisis. Estos trabajos comprenden el periodo 2020–2025, destacando un notable incremento en la producción académica durante el año 2024, en el que se identificaron 12 publicaciones, seguido por el año 2023 con 8 estudios relacionados.

La distribución anual de los artículos muestra una tendencia creciente en el interés por esta temática durante los años 2023 y 2024. Este fenómeno podría estar relacionado con el avance de tecnologías emergentes aplicadas a la ciberseguridad y con una creciente conciencia global sobre la importancia de proteger a los adolescentes en entornos

digitales. Tal incremento evidencia la urgencia de diseñar e implementar estrategias tecnológicas eficaces que respondan a los riesgos cibernéticos que enfrentan los jóvenes como población especialmente vulnerable (véase Fig. 2).

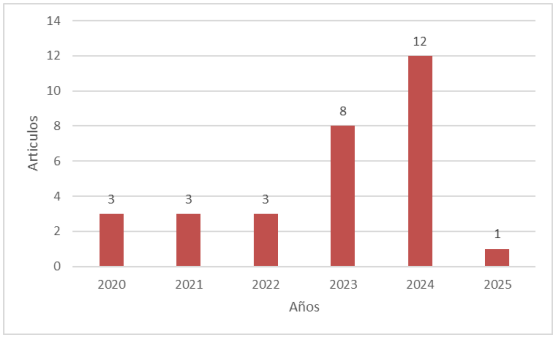

Fig. 2 Artículos incluidos en la revisión sistemática según año

A partir de un estudio Bibliométrico basado en el análisis de co-ocurrencia de términos, se identificó la frecuencia de aparición de palabras clave indexadas mediante la herramienta VOSviewer, utilizando como fuente los 30 artículos seleccionados previamente.

El análisis se efectuó considerando que la búsqueda se realizó en la base de datos Scopus, extrayéndose la información directamente desde dicha fuente para su posterior incorporación al flujo de trabajo de la herramienta tecnológica. Esto permitió detectar los términos técnicos más significativos y su grado de asociación temática. La Figura 2 presenta el Mapa de co-ocurrencia de palabras clave generado por VOSviewer, el cual evidencia las relaciones entre los términos más utilizados en los estudios analizados. En este mapa, cada circulo representa una palabra clave y su tamaño refleja la frecuencia con la que aparece; las líneas de conexión indican cuán frecuentemente se presentan juntas, mientras que los colores agrupan términos con vínculos temáticos similares, permitiendo así identificar subtemas recurrentes en la investigación. Este enfoque facilita la visualización de patrones y relaciones específicas entre los conceptos clave.

Entre los términos más representativos se encuentran: social media, cybersecurity, adolescent, privacy y adolescent online safety lo que confirma la orientación investigativa y aplicada en el campo de estudio.

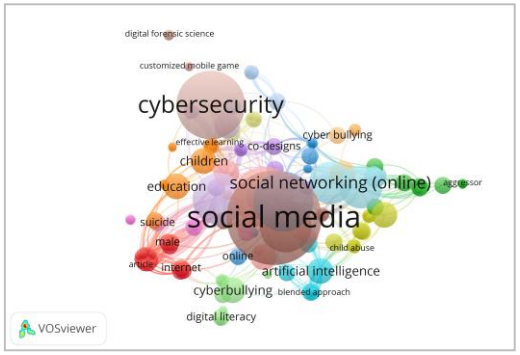

Fig. 3 Artículos incluidos según palabras claves

B. *Procedencia de los articulos por país*

Se llevó a cabo un análisis detallado sobre los países de procedencia de los artículos incluidos en la revisión, con el fin de profundizar en la dimensión geográfica de la investigación. Los resultados se representan en la Figura 3 mediante un gráfico de barras que muestra la distribución de los 30 estudios seleccionados.

La mayoría de las publicaciones analizadas provienen de estudios realizados en Estados Unidos, con un total de 12 artículos. Asimismo, se observa que Australia y el Reino Unido cuentan con 3 estudios cada uno, mientras que Hungría y España registran 2 publicaciones respectivamente. Por otro lado, Afganistán, Alemania, Arabia Saudita, Bangladesh, Irlanda, Malasia, Ruanda y Tailandia presentan un único estudio cada uno, evidenciando así una participación más limitada en la producción científica sobre el tema. Esta dispersión geográfica pone en evidencia que la ciberseguridad en adolescentes constituye una preocupación de alcance global. Ello resalta la necesidad común entre países de desarrollar e implementar soluciones tecnológicas efectivas que contribuyan a mitigar las amenazas cibernéticas en el ámbito de las tecnologías de la información (véase Fig. 4).

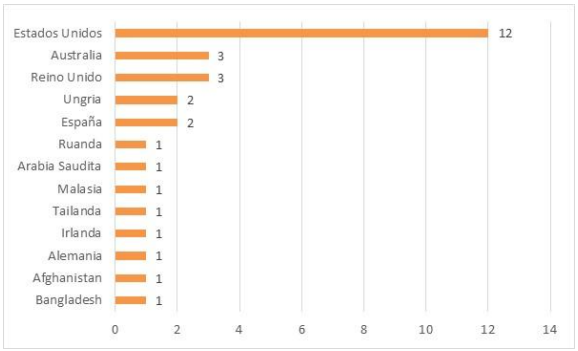

Fig. 4 Artículos incluidos según países o región.

C. *Resultados de las preguntas relacionadas:*

En el marco del análisis realizado en la revisión sistemática, surgieron interrogantes relevantes vinculados al tema de investigación como resultado de la aplicación de la metodología PICOC. En consecuencia, se formularon las siguientes preguntas, cuyas respuestas fueron construidas a partir de la evidencia extraída de los estudios seleccionados.

RQ1: ¿Qué características y riesgos enfrentan los adolescentes en entornos digitales? Los adolescentes presentan características particulares que los hacen especialmente vulnerables en entornos digitales. Diversos estudios coinciden en que están altamente expuestos a riesgos como el ciberacoso, la exposición involuntaria de datos personales, la sextorsión, el contacto con desconocidos, la adicción al uso de redes sociales y la manipulación algorítmica [12], [13], [14].

Una de las principales características distintivas es el uso intensivo de plataformas digitales, especialmente redes sociales y servicios de mensajería. Esta exposición constante, combinada con niveles variables de alfabetización digital, genera condiciones de riesgo [15], [14]. Además, la necesidad de socialización y validación grupal entre los adolescentes puede llevarlos a compartir información sensible sin considerar adecuadamente los posibles riesgos [16], [17].

El estudio [18] introduce el concepto de "dilemas de privacidad", en los cuales los adolescentes deben equilibrar la necesidad de visibilidad social con la protección de su identidad digital. Sin embargo, muchos carecen de las herramientas necesarias para tomar decisiones informadas sobre su seguridad en línea. Investigaciones como las de Martínez-Gómez [19] señalan que los adolescentes tienden a reconocer los riesgos de manera general, pero subestiman su propia vulnerabilidad, lo cual reduce su nivel de precaución en línea. Esta percepción errónea puede estar influida por una confianza excesiva en sus habilidades digitales o una falta de orientación efectiva por parte de adultos. Factores sociodemográficos como la edad, el género y el nivel educativo de los padres también inciden en el nivel de riesgo percibido y en los comportamientos digitales de los adolescentes. Por ejemplo, los adolescentes más jóvenes y con menor supervisión parental suelen ser más vulnerables a situaciones como el contacto no deseado, el grooming o prácticas como el sharenting [20], [21].

En síntesis, los adolescentes se caracterizan por un uso activo y emocional de las tecnologías digitales, acompañado de una alfabetización digital limitada en términos de privacidad y seguridad. Esta combinación los expone a una amplia gama de riesgos digitales, que deben abordarse desde una perspectiva tanto educativa como tecnológica, considerando su contexto social, emocional y cognitivo.

Fig. 5 Características y riesgos en entornos digitales

RQ2: ¿Qué tecnologías de ciberseguridad se han utilizado en las estrategias para proteger digitalmente a los adolescentes y cómo funcionan? La literatura científica revisada identifica diversas tecnologías aplicadas en estrategias de ciberseguridad para proteger a los adolescentes en entornos digitales. Estas combinan enfoques de prevención, monitoreo, educación y control de acceso, y operan tanto en dispositivos personales como en plataformas educativas y redes sociales. Incorporan tecnologías como inteligencia artificial, aprendizaje automático, gamificación, y diseño centrado en el usuario.

Una de las tecnologías más utilizadas es el control parental inteligente, basado en el monitoreo automatizado del contenido y las actividades en línea. Estas soluciones detectan comportamientos inapropiados como el contacto con desconocidos, lenguaje ofensivo o intentos de compartir información sensible mediante algoritmos de procesamiento de lenguaje natural. Por ejemplo, el chatbot propuesto por Wisniewski proporciona asistencia preventiva mediante interacciones adaptadas al contexto adolescente [18]. Otro enfoque son las aplicaciones educativas basadas en gamificación, diseñadas para mejorar el conocimiento de los adolescentes sobre ciberseguridad. Estas herramientas presentan simulaciones interactivas sobre amenazas como el phishing y el rastreo, promoviendo una toma de decisiones informada. El estudio de Agbo reporta mejoras significativas en la conciencia sobre riesgos digitales tras el uso de una app educativa personalizada [16]. También se han desarrollado tecnologías de detección automática de ciberacoso, mediante modelos de machine learning que analizan patrones de comunicación en plataformas sociales o educativas. Estos sistemas pueden generar alertas, bloquear mensajes ofensivos o notificar a los administradores antes de que ocurra un daño psicológico al usuario [22].

Las interfaces de privacidad adaptativa representan otra innovación clave. Estas interfaces ajustan dinámicamente el nivel de información y los controles según la edad, madurez digital y contexto de uso, facilitando una experiencia personalizada que equilibra el control parental con la autonomía progresiva del adolescente[17]. Además, algunas plataformas de aprendizaje (LMS), como Microsoft Teams o Moodle, han incorporado módulos de alfabetización digital y seguridad, que incluyen guías, avisos contextuales y ejercicios prácticos sobre protección de datos y configuración de privacidad, como parte del aprendizaje remoto[13].

En síntesis, las tecnologías aplicadas en estrategias de ciberseguridad para adolescentes van desde herramientas automatizadas hasta soluciones pedagógicas adaptativas. Su efectividad no depende únicamente de su complejidad técnica, sino también de su capacidad para adaptarse al perfil del usuario adolescente y fomentar una cultura de autoprotección desde edades tempranas.

TABLA 5 - TECNOLOGÍAS DE CIBERSEGURIDAD

Tecnologías de ciberseguridad	Artículos (DOI)	Año(s)
Controles parentales inteligentes con IA	2	2021–2023

Aplicaciones móviles educativas / gamificadas	2	2022–2024
Sistemas de detección automática de ciberacoso	2	2021–2022
Interfaces de privacidad adaptativa	1	2022
Extensiones o módulos en LMS para privacidad y seguridad	1	2023
Chatbots de educación digital segura	1	2023
Diseño participativo de herramientas de seguridad (co-diseño)	2	2022–2023
Monitoreo de huella digital y reputación en línea	1	2023
Tecnologías combinadas (educación + IA + monitoreo + participación)	2	2023–2024

RQ3: ¿Qué estrategias se utilizan en los entornos educativos tradicionales para prevenir el acoso de adolescentes? En los entornos educativos tradicionales, la prevención del acoso adolescente incluido el ciberacoso se aborda mediante enfoques pedagógicos, psicosociales y normativos, con énfasis en la formación en valores, la participación de toda la comunidad escolar y el desarrollo de competencias socioemocionales.

Una de las estrategias más implementadas es la educación en habilidades sociales y emocionales, centrada en la empatía, la resolución de conflictos y la comunicación asertiva. Estas iniciativas, integradas en programas curriculares o talleres extracurriculares, buscan reducir comportamientos agresivos y promover relaciones respetuosas [19]. Por ejemplo, Martínez-Gómez evidencian que los adolescentes entrenados en autorregulación emocional tienen menor propensión a conductas de acoso. Asimismo, las campañas de sensibilización escolar constituyen una herramienta clave en la prevención. Estas campañas incluyen charlas, teatro escolar, afiches informativos y dinámicas grupales que visibilizan el bullying y fomentan la cultura de denuncia. El estudio de Fernández-Batanero y Reyes-Rebollo reporta que estas acciones incrementan la percepción del problema y fortalecen la participación estudiantil [23].

Otra estrategia destacada es la formación docente en detección e intervención temprana. A través de programas de capacitación, los docentes adquieren herramientas para identificar señales de acoso y aplicar protocolos institucionales. Esta preparación es crítica, dado que muchos casos no se reportan si los adultos no están sensibilizados [12]. También se han reforzado las normativas de convivencia escolar, que establecen sanciones claras frente al acoso y definen mecanismos de mediación. Algunos centros educativos han implementado programas de mediación entre pares, donde estudiantes capacitados actúan como facilitadores en conflictos menores, promoviendo una resolución pacífica y reduciendo la reincidencia de conductas agresivas [24]. Sin embargo, estas estrategias encuentran limitaciones frente al acoso digital, que ocurre fuera del horario escolar y con frecuencia pasa desapercibido. Por ello, diversos estudios proponen enfoques híbridos que integren la intervención presencial con tecnologías digitales, como sistemas de monitoreo, plataformas de denuncia anónima o módulos de formación online [22]. En conclusión, las escuelas tradicionales previenen el acoso mediante acciones educativas, normativas y participativas. No obstante, la evolución del acoso hacia el entorno digital exige articulaciones con estrategias tecnológicas, adaptadas al ecosistema digital en el que los adolescentes interactúan diariamente.

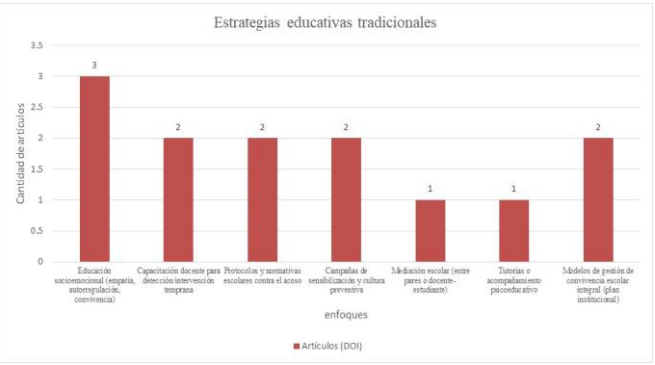

Fig. 6 Tipos de estrategias tecnológicas

RQ4: ¿Qué niveles de efectividad se reportan en los estudios en relación con la protección digital de adolescentes? Los estudios revisados en esta Revisión Sistemática de Literatura (RSL) reportan niveles variados de efectividad en las estrategias tecnológicas implementadas para la protección digital de los adolescentes. Esta efectividad se evalúa generalmente mediante indicadores como la reducción de riesgos digitales, la mejora del conocimiento en ciberseguridad, los cambios en el comportamiento digital, y el nivel de uso o aceptación de la tecnología empleada.

Una de las estrategias con mayor efectividad reportada es el uso de aplicaciones educativas gamificadas. Estas herramientas, que utilizan juegos y simulaciones para enseñar prácticas seguras en línea, han demostrado mejorar significativamente la conciencia digital de los adolescentes. En el estudio de Agbo, por ejemplo, se reporta que más del 80 % de los participantes mejoraron su desempeño en simulaciones sobre phishing y contraseñas tras utilizar una aplicación móvil personalizada [16].

Otra tecnología destacada son las herramientas de control parental basadas en inteligencia artificial, las cuales permiten el monitoreo proactivo de mensajes y comportamientos en línea. Badillo-Urquiola indican que estos sistemas lograron detectar señales de riesgo en comunicaciones con una precisión superior al 90 % [24]. En cuanto a las interfaces de privacidad adaptativas, diseñadas para ajustarse al nivel de comprensión del usuario adolescente, Wisniewski encontraron que el 73 % de los adolescentes y cuidadores valoraron

positivamente estas herramientas, considerándolas útiles para aprender a gestionar su información personal [18]. Sin embargo, varios estudios señalan que la efectividad se reduce cuando las tecnologías no se integran con componentes pedagógicos o contextos educativos. Las soluciones puramente técnicas, sin mediación educativa ni adaptación al perfil del adolescente, presentan baja adherencia o escasa comprensión por parte del usuario [22]. Además, se identifica una limitación metodológica en cuanto al número reducido de estudios con evaluaciones longitudinales. Aunque algunos trabajos, como el de Martínez-Gómez, documentan mejoras sostenidas en la percepción de seguridad digital después de intervenciones educativas, la mayoría de los estudios analizados presentan resultados preliminares o de corto plazo[19].

Los métodos de evaluación varían entre los estudios revisados e incluyen pruebas piloto, encuestas antes y después de la intervención, entrevistas cualitativas y métricas algorítmicas de precisión. Si bien los hallazgos reportan resultados prometedores, se evidencia una necesidad de investigaciones más robustas y longitudinales para validar la efectividad de estas estrategias a gran escala.

TABLA 6- Niveles de Efectividad

Niveles de efectividad	Artículos (DOI)
Alta efectividad (>75 %) en resultados de aprendizaje digital (uso de apps educativas, gamificadas)	2
Precisión técnica alta (>90 %) en detección de riesgos (ciberacoso, lenguaje ofensivo, grooming)	2
Mejora en la percepción de privacidad y seguridad digital	2
Cambio positivo en comportamiento digital (uso responsable de redes, menor exposición de datos personales)	2
Moderada efectividad cuando no hay componente educativo o contextual	2
Resultados mixtos (dependen del contexto de aplicación, aceptación o edad del usuario)	3
Evidencia longitudinal de impacto sostenido en percepción de seguridad y competencias digitales	1
Evaluación por usuarios (usabilidad, utilidad percibida alta en adolescentes y padres)	2

III. DISCUSIONES

En esta revisión sistemática, se observó que los adolescentes presentaron una alta exposición a riesgos digitales como el ciberacoso, el contacto con desconocidos, la pérdida de privacidad, la adicción a redes sociales y la manipulación algorítmica. Estos riesgos fueron más frecuentes entre usuarios con baja alfabetización digital y fuerte necesidad de validación social, fenómeno descrito ampliamente en estudios como los de Agbo [16] y Wisniewski [18]. La exposición intensiva a plataformas digitales se consideró un factor determinante de vulnerabilidad, especialmente cuando no existía un acompañamiento adulto adecuado [15], [14]. A diferencia de estudios previos donde se enfatizaba el desconocimiento técnico, esta revisión identificó que muchos adolescentes sí eran conscientes de los riesgos generales, pero subestimaban su propia vulnerabilidad [19]. Este hallazgo contradijo parcialmente lo reportado por Qiao, quienes plantearon una asociación directa entre desconocimiento y exposición a riesgos [25]. Además, se encontró que factores sociodemográficos como edad, supervisión parental y género influían significativamente en la percepción del riesgo, hallazgo que coincidió con lo reportado en [20] y [21]. Asimismo, el concepto de "dilemas de privacidad" introducido por Wisniewski [18], permitió entender cómo los adolescentes priorizaron la visibilidad social sobre la seguridad, reproduciendo patrones de exposición no intencionada. Estos resultados destacaron la necesidad de estrategias educativas diferenciadas, que consideren los contextos emocionales y sociales en los que se da el uso de la tecnología.

En esta revisión, se identificó que las estrategias tecnológicas más utilizadas para proteger digitalmente a los adolescentes incluyeron aplicaciones educativas gamificadas [16], chatbots conversacionales [18], sistemas de detección automática de riesgo [22] y plataformas de privacidad adaptativa [17]. Estas soluciones operaron en diversos entornos familiares, escolares y digitales con un enfoque preventivo o correctivo, según el tipo de amenaza abordada. A diferencia de tecnologías tradicionales centradas en el control externo, esta revisión evidenció una tendencia hacia el diseño centrado en el usuario adolescente, con interfaces adaptativas que permitieron una mayor apropiación de la herramienta por parte del joven [17]. El estudio de Agbo [16], por ejemplo, demostró que el uso de juegos personalizados mejoró significativamente la comprensión de amenazas como el phishing. Los sistemas de control parental basados en inteligencia artificial fueron capaces de detectar señales de ciberacoso y grooming con tasas de precisión superiores al 90 %, según lo reportado en [24], resultado que superó lo documentado en estudios previos que empleaban métodos manuales o semiautomáticos. Este hallazgo corroboró la evolución tecnológica en el monitoreo conductual, aunque también se señaló que la efectividad de estas herramientas dependía de su integración con componentes educativos [22]. En comparación con investigaciones anteriores centradas exclusivamente en aspectos técnicos, esta revisión resaltó la importancia de combinar funcionalidades tecnológicas con estrategias pedagógicas, una visión compartida por [13] y [14].

Los estudios revisados mostraron que las estrategias más efectivas en entornos educativos tradicionales para prevenir el acoso incluyeron la formación en habilidades socioemocionales, las campañas escolares de sensibilización y los programas de mediación entre pares[19], [23], [24]. Estas intervenciones apuntaron tanto a la prevención como a la intervención temprana de situaciones de acoso, incluyendo su manifestación digital. De manera similar a lo hallado por Catarino en entornos clínicos [26], donde las intervenciones

combinadas aumentaban la sensibilidad diagnóstica, en este estudio se observó que las estrategias que articulaban la formación docente, la normativa institucional y la participación estudiantil fueron más eficaces para reducir los incidentes de acoso [12]. El estudio de Martínez-Gómez [19] reveló que los adolescentes que participaron en talleres de autorregulación emocional presentaron una menor propensión a conductas de acoso, resultado que coincidió con investigaciones previas en contextos europeos. No obstante, la efectividad de las estrategias se redujo en el caso del acoso digital, que ocurre fuera del entorno escolar formal y con menor supervisión. En contraste con enfoques unidimensionales, esta revisión mostró que los enfoques híbridos que combinaron acciones presenciales con herramientas digitales ofrecieron una mejor cobertura ante los nuevos escenarios de riesgo, hallazgo confirmado en [22].

Esta revisión sistemática evidenció que los niveles de efectividad de las estrategias de protección digital variaron ampliamente entre los estudios. Se reportaron mayores tasas de efectividad en herramientas gamificadas educativas y en sistemas de inteligencia artificial para monitoreo de riesgos, con tasas de éxito superiores al 80 % y 90 % respectivamente [16], [24]. A diferencia de lo observado por Arbyn [27] en intervenciones clínicas con alta consistencia metodológica, esta revisión mostró una baja frecuencia de estudios con diseños longitudinales. De los artículos revisados, solo unos pocos, como el de Martínez-Gómez [19], incluyeron seguimiento a mediano plazo, revelando mejoras sostenidas en la percepción de seguridad digital tras programas escolares de alfabetización. Por otro lado, las soluciones exclusivamente tecnológicas sin acompañamiento educativo reportaron menor adherencia, fenómeno atribuido a la falta de personalización y escaso entendimiento de los adolescentes[22]. Estos resultados coincidieron con los reportes de Catarino [26], donde la falta de integración entre herramientas técnicas y el entorno reducía el impacto general de la estrategia. Los métodos de validación variaron entre pruebas piloto, encuestas pre y post, entrevistas y métricas algorítmicas, siendo estos últimos los más comunes en soluciones basadas en IA. A pesar de los avances, se concluyó que la evidencia empírica a gran escala aún es limitada, lo cual exige nuevas investigaciones con mayor rigor metodológico y diversidad geográfica.

IV. CONCLUSIONES

Esta investigación identificó las principales estrategias tecnológicas de ciberseguridad dirigidas a la protección digital de los adolescentes, evidenciando una diversidad de enfoques que abordan tanto la prevención como la intervención ante riesgos en entornos digitales. Entre los principales hallazgos, se destacan las aplicaciones educativas gamificadas, las herramientas de control parental inteligente, las interfaces de privacidad adaptativas y los modelos de detección automática de amenazas digitales, como el ciberacoso y el contacto con desconocidos.

Las estrategias basadas en gamificación y diseño centrado en el usuario mostraron ser altamente efectivas en la mejora del conocimiento en ciberseguridad y en la modificación de conductas digitales de riesgo, alcanzando niveles de aceptación superiores al 70 % en adolescentes y cuidadores. Por su parte, los sistemas basados en inteligencia artificial lograron tasas de detección superiores al 90 % en contextos de monitoreo preventivo, especialmente en plataformas de mensajería y redes sociales. Sin embargo, también se identificó que aquellas soluciones que carecen de un componente educativo presentan niveles de adherencia significativamente más bajos.

En cuanto a las implicaciones prácticas, los hallazgos de esta revisión sugieren orientaciones relevantes para diversos actores vinculados con la protección digital de adolescentes. Para los padres, resulta esencial promover un acompañamiento activo basado en el diálogo y la educación en competencias socioemocionales, evitando enfoques meramente restrictivos y fomentando el uso de aplicaciones interactivas como espacios de aprendizaje conjunto. En el ámbito educativo, se recomienda la incorporación de contenidos de alfabetización digital y privacidad en el currículo escolar, así como la capacitación docente en la detección temprana de riesgos y el uso pedagógico de herramientas digitales de seguridad. Por su parte, los desarrolladores de software deben priorizar el diseño de plataformas con interfaces de privacidad adaptativa, transparencia algorítmica y procesos de co-diseño participativo que incluyan a adolescentes y cuidadores, garantizando tanto la usabilidad como la pertinencia cultural de las soluciones. De manera general, los resultados indican que las estrategias más efectivas serán aquellas que logren integrar pedagogía y tecnología, equilibren la protección con la autonomía progresiva del adolescente y se adapten a contextos sociales diversos, constituyendo así una base sólida para el diseño futuro de herramientas de ciberseguridad con impacto educativo y social.

La contribución de esta RSL a la literatura existente radica en ofrecer una visión integral, actualizada y sistematizada (2020–2025) sobre las tecnologías emergentes y sus aplicaciones en el ámbito de la ciberseguridad adolescente, así como en visibilizar el rol del contexto educativo, familiar y cultural en la efectividad de dichas estrategias. Esta revisión también resalta la importancia de integrar la voz de los adolescentes en el diseño de soluciones tecnológicas, promoviendo enfoques participativos e inclusivos.

Entre las principales limitaciones de esta revisión se encuentra el uso exclusivo de la base de datos Scopus, lo que podría haber excluido estudios relevantes disponibles en otras bases

académicas como Web of Science, IEEE Xplore o ACM Digital Library. Asimismo, la restricción al idioma inglés y el acceso abierto limitó la diversidad lingüística y geográfica de las investigaciones incluidas.

Finalmente, para futuras investigaciones, se recomienda: (1) ampliar el análisis a través de estudios longitudinales que permitan evaluar el impacto sostenido de las estrategias tecnológicas en el tiempo; (2) explorar el desarrollo e implementación de modelos híbridos que integren ciberseguridad y bienestar emocional; y (3) fomentar la investigación en contextos subrepresentados, como América Latina, África y zonas rurales, a fin de generar soluciones más contextualizadas y equitativas.

AGRADECIMIENTO

A mis padres e hijos, por su amor, paciencia y apoyo incondicional; y a mis tutores del curso, por su guía, dedicación y valiosas enseñanzas que hicieron posible la culminación de este trabajo académico.

REFERENCIAS

[1] X. Zhang *et al.*, «Analysis of deviant behaviors and family functions in the population at risk of internet addiction among primary and secondary school students in Chengdu city, Sichuan province of China», *Front. Public Health*, vol. 12, nov. 2024, doi: 10.3389/fpubh.2024.1498466.

[2] A. Lau-Zhu, C. Anderson, y M. Lister, «Assessment of digital risks in child and adolescent mental health services: A mixed-method, theory-driven study of clinicians' experiences and perspectives», *Clin. Child Psychol. Psychiatry*, vol. 28, n.º 1, pp. 255-269, ene. 2023, doi: 10.1177/13591045221098896.

[3] *Estado mundial de la infancia 2017: niños en un mundo digital*. Nueva York: UNICEF, 2017.

[4] M. C. Buchan, J. Bhawra, y T. R. Katapally, «Navigating the digital world: development of an evidence-based digital literacy program and assessment tool for youth», *Smart Learn. Environ.*, vol. 11, n.º 1, p. 8, feb. 2024, doi: 10.1186/s40561-024-00293-x.

[5] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, y J. M. Carroll, «Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?», en *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, Portland Oregon USA: ACM, feb. 2017, pp. 51-69. doi: 10.1145/2998181.2998352.

[6] S. B. Jackson, K. T. Stevenson, L. R. Larson, M. N. Peterson, y E. Seekamp, «Outdoor Activity Participation Improves Adolescents' Mental Health and Well-Being during the COVID-19 Pandemic», *Int. J. Environ. Res. Public. Health*, vol. 18, n.º 5, p. 2506, mar. 2021, doi: 10.3390/ijerph18052506.

[7] X. Zhu y D. T. L. Shek, «Parental Control and Adolescent Delinquency Based on Parallel Process Latent Growth Curve Modeling», *Int. J. Environ. Res. Public. Health*, vol. 18, n.º 17, p. 8916, ago. 2021, doi: 10.3390/ijerph18178916.

[8] Y. Peng, Y. Wang, S. Liu, y X. Hu, «Parenting and mobile phone addiction tendency of Chinese adolescents: The roles of self-control and future time perspective», *Front. Psychol.*, vol. 13, oct. 2022, doi: 10.3389/fpsyg.2022.985608.

[9] K. Badillo-Urquiola, C. Chouhan, S. Chancellor, M. De Choudhary, y P. Wisniewski, «Beyond Parental Control: Designing Adolescent Online Safety Apps Using Value Sensitive Design», *J. Adolesc. Res.*, vol. 35, n.º 1, pp. 147-175, 2020, doi: 10.1177/0743558419884692.

[10] T. Qiu, S. Wang, D. Hu, N. Feng, y L. Cui, «Predicting Risk of Bullying Victimization among Primary and Secondary School Students: Based on a Machine Learning Model», *Behav. Sci.*, vol. 14, n.º 1, p. 73, ene. 2024, doi: 10.3390/bs14010073.

[11] E. A. Nina-Gutiérrez, J. E. Pacheco-Alanya, y J. C. Morales-Arevalo, «SocialBullyAlert: A Web Application for Cyberbullying Detection on Minors' Social Media», *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, n.º 7, 2024, doi: 10.14569/ijacsa.2024.0150776.

[12] Y. Al-Saggaf y J. Maclean, «Smartphone Privacy and Cyber Safety among Australian Adolescents: Gender Differences», *Inf. Switz.*, vol. 15, n.º 10, 2024, doi: 10.3390/info15100604.

[13] S. Khan *et al.*, «Teaching Middle Schoolers about the Privacy Threats of Tracking and Pervasive Personalization: A Classroom Intervention Using Design-Based Research», en *Conf Hum Fact Comput Syst Proc*, Association for Computing Machinery, 2024. doi: 10.1145/3613904.3642460.

[14] M. J. Rubio Hurtado, R. Vilà Baños, y T. Donoso Vazquez, «Evaluation of a Training Program Aimed At Young Lawbreakers to Prevent Gender-Based Cyber Violence», *Rev. Cercet. Si Interv. Sociala*, vol. 88, pp. 7-22, 2025, doi: 10.33788/rcis.88.1.

[15] A. Lavis y R. Winter, «#Online harms or benefits? An ethnographic analysis of the positives and negatives of peer-support around self-harm on social media», *J. Child Psychol. Psychiatry*, vol. 61, n.º 8, pp. 842-854, 2020, doi: 10.1111/jcpp.13245.

[16] A. M. R. Alsobeh, I. Alazzam, A. M. J. Shatnawi, y I. Khasawneh, «Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors», *Online J. Commun. Media Technol.*, vol. 13, n.º 2, 2023, doi: 10.30935/ojcmt/12942.

[17] N. Chatlani, A. Davis, K. Badillo-Urquiola, E. Bonsignore, y P. Wisniewski, «Teen as research-apprentice: A restorative justice approach for centering adolescents as the authority of their own online safety», *Int. J. Child-Comput. Interact.*, vol. 35, 2023, doi: 10.1016/j.ijcci.2022.100549.

[18] D. Buckingham, «Epilogue: Rethinking digital literacy: Media education in the age of digital capitalism», *Digit. Educ. Rev.*, n.º 37, pp. 230-239, 2020, doi: 10.1344/DER.2020.37.230-239.

[19] M. Dorasamy, M. Kaliannan, M. Jambulingam, I. Ramadhan, y A. Sivaji, «Parents' awareness on online predators: Cyber grooming deterrence», *Qual. Rep.*, vol. 26, n.º 11, pp. 3685-3723, 2021, doi: 10.46743/2160-3715/2021.4914.

[20] T. Milosevic *et al.*, «Effectiveness of Artificial Intelligence–Based Cyberbullying Interventions From Youth Perspective», *Soc. Media Soc.*, vol. 9, n.º 1, 2023, doi: 10.1177/20563051221147325.

[21] R. M. Chandrima *et al.*, «Adolescent problematic internet use and parental mediation: A Bangladeshi structured interview study», *Addict. Behav. Rep.*, vol. 12, 2020, doi: 10.1016/j.abrep.2020.100288.

[22] M. Bendechache *et al.*, «AI in My Life: AI, Ethics & Privacy Workshops for 15-16-Year-Olds», en *ACM Int. Conf. Proc. Ser.*, Association for Computing Machinery, 2021, pp. 34-39. doi: 10.1145/3462741.3466664.

[23] X. V. Caddle, N. Naher, Z. P. Miller, K. Badillo-Urquiola, y P. J. Wisniewski, «Duty to Respond: The Challenges Social Service Providers Face When Charged With Keeping Youth Safe Online», *Proc. ACM Hum.-Comput. Interact.*, vol. 7, n.º GROUP, 2023, doi: 10.1145/3567556.

[24] S. Iqbal, R. Zakar, y F. Fischer, «Extended Theoretical Framework of Parental Internet Mediation: Use of Multiple Theoretical Stances for Understanding Socio-Ecological Predictors», *Front. Psychol.*, vol. 12, 2021, doi: 10.3389/fpsyg.2021.620838.

[25] J. Turvey, D. McKay, S. T. Kaur, N. Castree, S. Chang, y M. S. C. Lim, «Exploring the Feasibility and Acceptability of Technological Interventions to Prevent Adolescents' Exposure to Online Pornography: Qualitative Research», *JMIR Pediatr. Parent.*, vol. 7, 2024, doi: 10.2196/58684.

[26] T. I. Tanni, M. Akter, J. Anderson, M. J. Amon, y P. J. Wisniewski, «Examining the Unique Online Risk Experiences and Mental Health Outcomes of LGBTQ+ versus Heterosexual Youth», en *Conf Hum Fact Comput Syst Proc*, Association for Computing Machinery, 2024. doi: 10.1145/3613904.3642509.

[27] M. Kapitány-Fövény *et al.*, «Gender-specific pathways regarding the outcomes of a cyberbullying youth education program», *Personal. Individ. Differ.*, vol. 186, 2022, doi: 10.1016/j.paid.2021.111338.

[28] S. A. Aljasir y M. O. Alsebaei, «Cyberbullying and cybervictimization on digital media platforms: the role of demographic variables and parental mediation strategies», *Hum. Soc. Sci. Comm*, vol. 9, n.º 1, 2022, doi: 10.1057/s41599-022-01318-x.

[29] E. Roehrer, P. Pokawinkoon, P. Watters, J. D. Sauer, y J. Scanlan, «Adolescent-Centric Design of an Online Safety Chatbot», *J. Comput. Inf. Syst.*, 2024, doi: 10.1080/08874417.2024.2401991.

[30] J. Henriksen-Bulmer, E. Rosenorn-Lanng, S. Corbin-Clarke, S. Ware, D. Melacca, y L.-A. Fenge, «Using game-based learning to teach young people about privacy and online safety», *Interact. Learn. Environ.*, vol. 32, n.º 10, pp. 6430-6450, 2024, doi: 10.1080/10494820.2023.2265424.

[31] V. Chang, L. Golightly, Q. A. Xu, T. Boonmee, y B. S. Liu, «Cybersecurity for children: an investigation into the application of social media», *Enterp. Inf. Syst.*, vol. 17, n.º 11, 2023, doi: 10.1080/17517575.2023.2188122.

[32] D. Freed *et al.*, «Understanding Digital-Safety Experiences of Youth in the U.S.», en *Conf Hum Fact Comput Syst Proc*, Association for Computing Machinery, 2023. doi: 10.1145/3544548.3581128.

[33] Z. Agha *et al.*, «Tricky vs. Transparent: Towards an Ecologically Valid and Safe Approach for Evaluating Online Safety Nudges for Teens», en *Conf Hum Fact Comput Syst Proc*, Association for Computing Machinery, 2024. doi: 10.1145/3613904.3642313.

[34] A. Alluhidan, M. Akter, A. Alsoubai, J. Katie Park, y P. Wisniewski, «Teen Talk: The Good, the Bad, and the Neutral of Adolescent Social Media Use», *Proc. ACM Hum. Comput. Interact.*, vol. 8, n.º CSCW2, 2024, doi: 10.1145/3686961.

[35] I. Alam, A. Basit, y R. A. Ziar, «Utilizing Age-Adaptive Deep Learning Approaches for Detecting Inappropriate Video Content», *Hum. Behav. Emerg. Technol.*, vol. 2024, 2024, doi: 10.1155/2024/7004031.

[36] E. Casey, J. Jocz, K. A. Peterson, D. Pfeif, y C. Soden, «Motivating youth to learn STEM through a gender inclusive digital forensic science program», *Smart Learn. Environ.*, vol. 10, n.º 1, 2023, doi: 10.1186/s40561-022-00213-x.

[37] J. M. Takács y M. Pogátsnik, «The Presence of Cybersecurity Competencies in the Engineering Education of Generation Z», *Acta Polytech. Hung.*, vol. 21, n.º 6, pp. 107-127, 2024, doi: 10.12700/APH.21.6.2024.6.6.

[38] A. Cohen, A. Bendelow, T. Smith, C. Cicchetti, M. M. Davis, y M. Heffernan, «Parental Attitudes on Social Media Monitoring for Youth: Cross-Sectional Survey Study», *JMIR Pediatr. Parent.*, vol. 6, n.º 1, 2023, doi: 10.2196/46365.

[39] K. Sriwisathiyakun, «CRAFTING DIGITAL MICRO-STORYTELLING FOR SMARTER THAI YOUTH: A NOVEL APPROACH TO BOOST DIGITAL INTELLIGENT QUOTIENT», *J. Inf. Technol. Educ.*, vol. 23, 2024, doi: 10.28945/5273.

[40] S. Abascal-Peiró *et al.*, «Digital Platform for the Prevention of Suicidal Behaviour and Non-Suicidal Self-Injuries in Adolescents: The SmartCrisis-Teen Study Protocol», *Behavioral Sciences*, vol. 14, n.º 9, 2024, doi: 10.3390/bs14090740.

[41] R. C. T. Panga, J. Marwa, y J. D. Ndibwile, «A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania», *J. Cybersecur. Priv.*, vol. 2, n.º 3, pp. 466-489, 2022, doi: 10.3390/jcp2030024.