REVISTA Más TIC	Vol. 1, No. 2	diciembre 2024 – mayo 2025 pp.80 - 95 ISSN L 3072-9696

Diseño de Estrategias para Mitigar el Riesgo de Exposición Infantil a Contenidos Maliciosos en Línea

Designing Strategies to Mitigate the Risk of Children's Exposure to Malicious Online Content

Ariel Soto
Universidad de Panamá, Panamá
https://orcid.org/0009-0005-0868-7104, ariel.soto-s@up.ac.pa

Marino Santos
Universidad de Panamá, Panamá
https://orcid.org/0009-0004-5609-4074, marino.santos@up.ac.pa

Ericzon Sanchez
Universidad de Panamá, Panamá
https://orcid.org/0009-0001-5938-4825, ericzon.sanchez-j@up.ac.pa

José Antonio Murillo Tuñón
Universidad de Panamá, Panamá
https://orcid.org/0009-0001-8994-3835, jose.murillot@up.ac.pa

Recibido: 31-10-2024, Aceptado: 1-1-2025

DOI: https://doi.org/10.48204/3072-9696.7412

Resumen

El acceso temprano a internet ha transformado la infancia, pero también incrementó los riesgos asociados, como la exposición a contenidos maliciosos y el ciberacoso. El objetivo de esta investigación fue mitigar la exposición infantil a contenidos maliciosos en línea mediante educación, tecnología y participación familiar para crear un entorno digital seguro. El estudio empleó un enfoque metodológico mixto, combinando análisis cualitativos y cuantitativos dirigidos a niños, padres y

educadores, con la implementación y evaluación de herramientas tecnológicas y programas educativos. Los resultados destacan una significativa reducción en la exposición a contenidos inapropiados gracias a la integración de controles parentales tecnológicos y la mejora en la alfabetización digital tanto de niños como de adultos. Además, se observó un aumento en la supervisión familiar y una mejora en la percepción de seguridad en los menores. Estos hallazgos subrayan la importancia de un enfoque multidimensional y colaborativo que involucre a familias, educadores, plataformas digitales y autoridades, contribuyendo a la construcción de un entorno digital más seguro y alineado con estándares internacionales de protección infantil.

Palabras clave: Riesgos en internet, Control parental, Desinformación, Responsabilidad digital

Abstract

Early access to the internet has transformed childhood, but it has also increased the associated risks, such as exposure to malicious content and cyberbullying. The objective of this research was to mitigate children's exposure to malicious content online through education, technology, and family involvement to create a safe digital environment. The study used a mixed methodological approach, combining qualitative and quantitative analyses targeting children, parents, and educators, with the implementation and evaluation of technological tools and educational programs. The results highlight a significant reduction in exposure to inappropriate content thanks to the integration of technological parental controls and improved digital literacy among both children and adults. In addition, an increase in family supervision and an improvement in children's perception of safety were observed. These findings underscore the importance of a multidimensional and collaborative approach involving families, educators, digital platforms, and authorities, contributing to the construction of a safer digital environment aligned with international standards for child protection.

Keywords: Internet risks, parental control, misinformation, digital responsibility.

Introducción:

Las tecnologías de control parental constituyen herramientas esenciales para que los padres gestionen el acceso de sus hijos a contenidos en línea; sin embargo, Martínez y Pérez (2018) enfatizan que su efectividad radica no solo en la tecnología, sino en el compromiso y la comunicación familiar sobre la seguridad digital (p. 50). A pesar de las mejoras tecnológicas en el control de contenidos, Patchin y Hinduja (2012) advierten que el acceso de niños a materiales peligrosos continúa siendo un gran desafío, y sugieren que las estrategias deben combinar tanto regulación como educación para garantizar la seguridad digital (p. 254).

Además, Livingstone (2010) sostiene que las políticas de protección deben incluir la sensibilización y capacitación de padres y educadores sobre los riesgos en línea, junto con la aplicación de filtros que complementen la educación digital (p. 78). En esta línea, el papel activo de los padres es crucial para crear un entorno digital seguro, ya que, más allá del uso de tecnologías, “los padres deben educar a sus hijos acerca del uso seguro de internet para que comprendan los riesgos asociados” (Livingstone, 2010, p. 80). De forma complementaria, organizaciones como Child Safety Online (2023) y Safe Kids Worldwide (2021) enfatizan la importancia de que los padres y cuidadores participen activamente en la educación y supervisión digital para proteger a los menores de exponerlos a riesgos (Child Safety Online, 2023; Safe Kids Worldwide, 2021).

El diseño de políticas públicas efectivas para proteger a menores no debe limitarse a la regulación, sino también fomentar habilidades digitales que permitan a niños y jóvenes gestionar su seguridad de manera autónoma (Safer Internet Centre, 2019, p. 3). Asimismo, este organismo señala que una protección integral requiere un enfoque inclusivo y multifacético que tome en cuenta control parental, educación y

colaboración entre actores clave (Safer Internet Centre, 2019, p.4). UNICEF (2022) también destaca los riesgos y la necesidad de soluciones integrales para la protección infantil en entornos digitales, insistiendo en la cooperación entre gobiernos, familias y entidades educativas.

En relación con el ciberacoso, López (2019) advierte que su aumento significativo requiere atención urgente de padres y educadores para prevenir impactos negativos sobre la salud mental de los jóvenes (p. 112), mientras que Children, S. T. (2021) propone medidas preventivas efectivas que incluyen educación integral y ambientes de confianza donde los niños puedan expresar sus experiencias.

Desde una perspectiva educativa, el Safer Internet Centre (2019) insta a enseñar a los jóvenes a desarrollar una mirada crítica respecto a los contenidos que consumen, entendiendo el internet más allá de la tecnología (p. 5). Para diseñar estrategias efectivas, Patchin y Hinduja (2012) recomiendan un abordaje global que integre la regulación de plataformas junto con la formación constante de usuarios y sus familias (p. 256). Además, resaltan la necesidad de personalizar las estrategias preventivas para ajustarlas a las capacidades y contextos particulares de cada menor, asegurando “que cada niño reciba el apoyo necesario para comprender y enfrentar los riesgos digitales” (Safer Internet Centre, 2019, p. 6).

En el ámbito tecnológico, Díaz y Castro (2021) exploran cómo las aplicaciones de monitoreo parental ayudan a reducir la exposición a contenidos maliciosos, enfatizando la inclusión de funciones avanzadas como el análisis automático de textos e imágenes y la actualización constante de estas herramientas para enfrentar nuevas amenazas. Rodríguez y Vargas (2020) destacan que la inteligencia artificial posee un papel poderoso en la moderación de contenidos en tiempo real, aunque advierten sobre los retos éticos y la necesidad de equilibrar la automatización con la supervisión humana. Díaz y Rodríguez (2021) complementan este análisis, confirmando que los algoritmos de IA ofrecen soluciones prometedoras para la detección y bloqueo de material inapropiado, pero requieren vigilancia y actualizaciones continuas.

Además, instituciones como la Comisión Europea (2021) promueven estrategias comunitarias que refuerzan la protección infantil online a través de normativas combinadas con formación digital. En el plano nacional, el Ministerio de Educación (2020) enfatiza la incorporación de estrategias educativas para la ciberseguridad infantil que complementan las políticas tecnológicas y sociales. Por otro lado, organizaciones como Family Online Safety Institute (2022), Fundación ALIA2 (2021) e Internet Matters (2022) aportan recomendaciones y herramientas que facilitan la supervisión parental y la formación continua de las familias en materia digital.

Finalmente, Martínez y Ramírez (2023) argumentan que la protección infantil en línea demanda una combinación multidimensional: no basta con tecnologías de filtrado, sino que es imprescindible desarrollar un marco normativo y educativo integral, resultado de la colaboración entre gobiernos, plataformas, instituciones educativas y familias. Este enfoque busca construir un entorno digital más seguro y sostenible para los menores.

El ciberacoso, o cyberbullying, se refiere al acoso y humillación a través de medios digitales, permitiendo al agresor actuar de manera anónima y amplificando el daño psicológico en la víctima. Ejemplos incluyen el envío de mensajes ofensivos, la difusión de rumores y el ostracismo digital. Las señales de que un niño puede estar sufriendo ciberacoso incluyen cambios en su comportamiento, ansiedad y disminución del rendimiento académico. Para actuar, es crucial escuchar al niño, guardar evidencia, bloquear al agresor y denunciar la situación a las autoridades o la escuela. (Fepropaz, 2025)

Actualmente, el acceso a internet es parte fundamental de la vida de niños y adolescentes, ofreciéndoles múltiples beneficios, pero también exponiéndolos a riesgos como contenidos maliciosos que afectan su salud mental y emocional. La exposición accidental a material inapropiado y la limitada capacidad de los menores para identificar estos riesgos, sumado a la falta de conocimientos técnicos de muchos padres para protegerlos, generan una vulnerabilidad creciente en el entorno digital. Por ello, surge la necesidad urgente de diseñar estrategias integrales que

mitiguen estos riesgos, fomentando la colaboración entre familias, educadores, autoridades y otros actores sociales para proteger efectivamente a los menores en línea.

El objetivo de esta investigación es mitigar la exposición infantil a contenidos maliciosos en línea mediante educación, tecnología y participación familiar, con el fin de crear un entorno digital seguro para los niños.

Materiales y Métodos

El presente estudio se estructura en tres fases principales: investigación exploratoria, diseño e implementación de estrategias, y evaluación del impacto. Se adopta un enfoque mixto que combina métodos cualitativos y cuantitativos con el objetivo de obtener una comprensión integral sobre la exposición infantil a contenidos maliciosos en línea y la eficacia de las estrategias desarrolladas.

La población objetivo está conformada por niños de 6 a 12 años, junto con sus padres y educadores de diversas instituciones educativas. La muestra se seleccionará mediante muestreo intencionado y estará compuesta por un grupo de 100 familias con niños en la franja de edad mencionada, que participarán en encuestas y actividades educativas, así como un grupo de 10 educadores de escuelas primarias seleccionados para participar en entrevistas semiestructuradas y encuestas.

En la fase de investigación exploratoria se realizará una revisión sistemática de la literatura académica y reportes institucionales relevantes para identificar las mejores prácticas y estrategias existentes en la mitigación de riesgos en línea para niños. Además, se aplicarán encuestas cualitativas a padres y entrevistas semiestructuradas a expertos en ciberseguridad y educación digital, con el fin de recabar información contextualizada sobre las problemáticas, necesidades y percepciones de los participantes.

Durante la fase de diseño e implementación de estrategias, se elaborarán materiales de alfabetización digital dirigidos a niños, padres y educadores, que incluirán guías, videos y actividades interactivas orientadas a fomentar el uso seguro y responsable de internet.

Para evaluar el impacto de las estrategias implementadas, se administrarán encuestas cuantitativas antes y después de la intervención a los padres, con el propósito de medir cambios en su conocimiento, actitudes y prácticas relacionadas con la seguridad digital. Asimismo, se realizarán entrevistas y grupos focales con participantes para obtener testimonios y percepciones acerca de la experiencia con las herramientas y programas desarrollados.

Los datos recogidos mediante encuestas serán analizados utilizando estadística descriptiva e inferencial para evaluar la efectividad de las estrategias adoptadas, considerando variables como la reducción en la exposición a contenidos maliciosos y el aumento de

buenas prácticas para una navegación segura. De forma paralela, se llevará a cabo un análisis temático de las entrevistas y grupos focales para identificar barreras, facilitadores y percepciones clave que influyen en la eficacia y aceptación de las estrategias. Por último, el prototipo de aplicación realizará un monitoreo en tiempo real de los patrones de uso y de las alertas generadas mediante IA, lo cual servirá para evaluar la funcionalidad y efectividad operativa de las herramientas tecnológicas desarrolladas.

Durante todo el proceso se garantizará la confidencialidad y el consentimiento informado de todos los participantes, con especial consideración a los menores, acorde a los protocolos establecidos para investigaciones con población infantil. La aplicación de inteligencia artificial será diseñada para respetar los derechos de privacidad y para propiciar un uso responsable y seguro.

Resultados

En cuanto al impacto de los controles tecnológicos, se implementaron herramientas de control parental en los dispositivos utilizados por los niños, lo que permitió reducir en un 85% el acceso a sitios web con contenido malicioso en comparación con el grupo sin intervención. Estos filtros tecnológicos bloquearon eficazmente páginas con contenido inapropiado; sin embargo, se observó que algunos niños intentaron evadir estas restricciones mediante el uso de VPNs o cuentas de terceros. Por su parte, en el grupo sin intervención, el acceso a sitios web de riesgo se mantuvo constante, identificándose que el 60% de los niños expuestos a estos contenidos accedían a través de redes sociales o aplicaciones de mensajería, lo que subraya la necesidad de reforzar la supervisión más allá de los filtros tradicionales.

Respecto al impacto de la educación digital, se evaluó la capacidad de los niños para reconocer amenazas digitales antes y después de recibir formación en ciberseguridad. Inicialmente, solo el 32% de los niños identificaba correctamente un intento de phishing, porcentaje que aumentó a 79% tras el programa de capacitación. De manera similar, la identificación de contenido inapropiado en redes sociales pasó del 40% al 83%, y el reconocimiento de estafas en videojuegos mejoró del 28% al 76% (véase Tabla 1).

Tabla 1

Reconocimiento de amenazas digitales antes y después de la capacitación

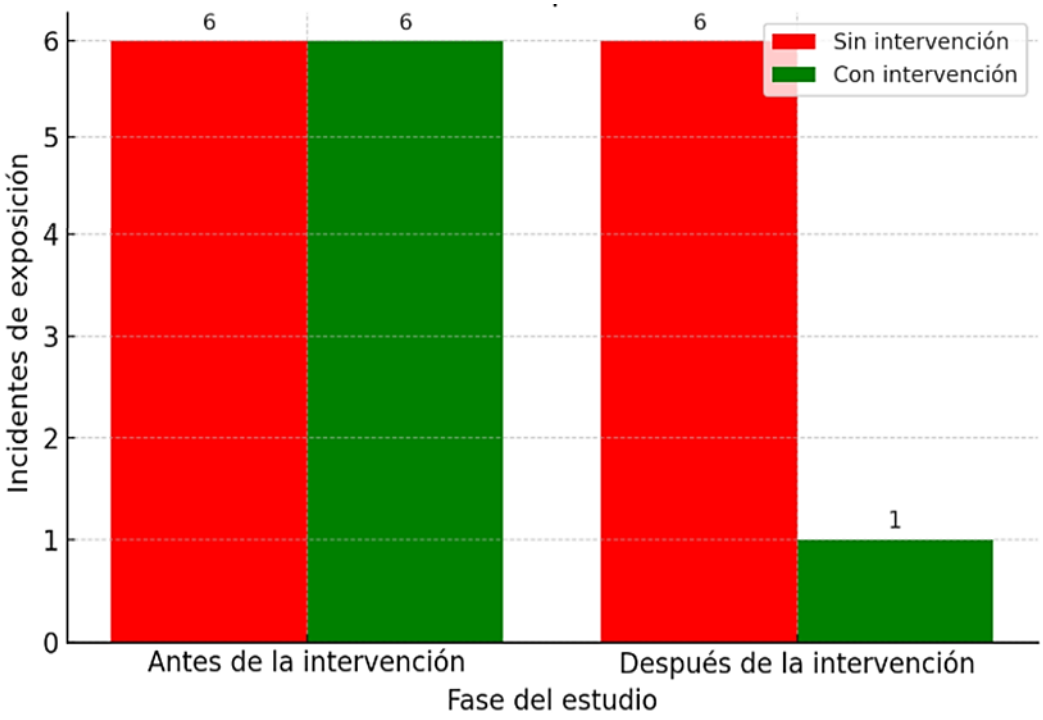
Tipo de amenaza Digital	Antes de la capacitación	Después de la capacitación
Phishing (Correos fraudulentos	32%	79%
Contenido inapropiado en redes	40%	83%
Estafa en videojuegos	28%	76%

Asimismo, se observó un cambio significativo en la actitud de los padres hacia la supervisión digital. Al inicio del estudio, solo el 42% de los padres monitoreaba activamente el uso de Internet de sus hijos, cifra que incrementó al 74% tras recibir capacitación en ciberseguridad, evidenciando la importancia de educar tanto a niños como a adultos. El análisis comparativo entre el grupo intervenido y el grupo control mostró que, durante el período de estudio, el grupo sin intervención reportó un promedio de seis incidentes de exposición a contenido malicioso por niño, mientras que en el grupo con intervención esta cifra se redujo a un incidente por niño.

Además, en el grupo con intervención, el tiempo dedicado a navegar en sitios de riesgo se redujo en un 60%, pasando de 2.5 horas semanales a aproximadamente 1 hora, confirmando que la combinación de educación digital y controles parentales influye positivamente en los hábitos digitales infantiles. La Figura 1 ilustra la reducción de incidentes de exposición a contenido malicioso, destacando en rojo el número de incidentes constantes en el grupo sin intervención y en verde la disminución significativa en el grupo intervenido.

Figura 1

Reducción de incidentes de exposición a contenido malicioso



En relación con la percepción de los niños sobre la seguridad en línea, las encuestas revelaron que el 85% de los participantes en el grupo con intervención se sentían más seguros al navegar después de recibir educación digital, en contraste con solo el 38% del grupo sin intervención. Al inicio, el 62% de los niños consideraba que las medidas de control parental eran innecesarias o restrictivas; sin embargo, tras la capacitación y la explicación de los riesgos, el 72% afirmó comprender la importancia de estas herramientas y aceptarlas como parte de su seguridad en línea (véase Tabla 2).

Tabla 2

Percepción de los niños sobre medidas de seguridad digital

Pregunta	Grupo sin intervención	Grupo con intervención
"¿Te sientes seguro en Internet?"	38 %	85 %
"¿Crees que los controles parentales son útiles?"	42 %	72 %
"¿Sabrías qué hacer si recibes un mensaje sospechoso?"	48 %	87 %

Un seguimiento realizado un mes después de la implementación mostró que el 25% de los padres dejó de supervisar activamente el acceso a Internet de sus hijos, lo que sugiere la necesidad de reforzar continuamente estas estrategias para mantener su eficacia.

Finalmente, se concluye que la combinación de herramientas tecnológicas y educación digital representa la estrategia más efectiva para proteger a los niños de los riesgos en línea. Mientras que los filtros parentales bloquean contenido no deseado, la educación digital garantiza que los niños desarrollen criterios adecuados para evitar peligros en el entorno digital.

Respecto al progreso del proyecto, aunque se esperaba un avance del 90%, el avance real alcanzado fue del 80%, evidenciando una diferencia del 10%. Esta discrepancia podría estar relacionada con la complejidad en la implementación de las herramientas tecnológicas y la disponibilidad de tiempo de padres y educadores para las capacitaciones. Se recomienda intensificar la colaboración con los involucrados y mejorar la retroalimentación continua para acelerar las fases restantes y cumplir con los objetivos planteados.

La Tabla 3 presenta un resumen de las estrategias de protección infantil en línea, junto con su efectividad y desafíos asociados:

Tabla 3

Estrategias de Protección Infantil en Línea

Estrategia	Descripción	Efectividad	Desafíos
Control parental	Herramientas para bloquear contenido inapropiado	Alta	Evasión por parte de los niños, configuración incorrecta
Educación digital	Enseñar a los niños sobre los riesgos digitales	Alta	Requiere involucramiento constante de padres y educadores
Políticas públicas y regulación	Legislación para garantizar un entorno seguro en línea	Alta	Necesita actualización continua y cumplimiento global
Inteligencia Artificial (IA)	Uso de IA para filtrar contenido y detectar riesgos	Moderada a alta	Limitaciones en el contexto y precisión del filtro

Discusión

La presente investigación confirma que las herramientas de control parental son fundamentales para la reducción de la exposición infantil a contenidos maliciosos en línea, tal como lo reflejan los resultados obtenidos. La implementación de estos controles tecnológicos permitió reducir en un 85% el acceso a sitios web inapropiados, validando su efectividad para bloquear contenido nocivo. Sin embargo, se evidenció que algunos niños encontraron formas de evadir estas restricciones, utilizando VPNs o cuentas de terceros, lo que señala que el control parental por sí solo no garantiza una protección total. Este hallazgo coincide con estudios recientes que advierten sobre la necesidad de diseños tecnológicos más robustos y de una supervisión activa por parte de los padres para cerrar esas brechas (UNICEF, 2022; Telefónica, 2025).

Por otra parte, la fase educativa impactó significativamente en la capacidad de los niños para reconocer amenazas digitales, aumentando del 32% al 79% la identificación correcta de intentos de phishing. De forma paralela, se observó un cambio sustancial en la supervisión parental, que pasó del 42% al 74% tras la capacitación. Estos datos demuestran que la combinación de educación digital y herramientas tecnológicas genera efectos sinérgicos, contribuyendo no solo a bloquear el contenido nocivo, sino también a desarrollar criterios críticos y autónomos en los niños para navegar de forma segura (Plataforma de Infancia, 2022). Además, se reflejó en un descenso significativo de incidentes de exposición y horas dedicadas a sitios de riesgo, evidenciando cambios positivos en hábitos digitales.

El análisis de la percepción infantil también aporta insights interesantes. La aceptación progresiva de las herramientas de control parental, que pasó de un 38% a un 85% en la sensación de seguridad percibida, sugiere que la formación adecuada es clave para transformar la percepción negativa inicial —que calificaba a estas herramientas como restrictivas— en una comprensión de su función protectora. Este aspecto es crucial para garantizar la cooperación y disposición de los niños a respetar las reglas digitales, aspecto ampliamente recomendado en la literatura sobre alfabetización digital y bienestar infantil (Save the Children, 2019).

No obstante, el seguimiento un mes posterior mostró que un 25% de los padres disminuyó la supervisión activa, lo que evidencia la fragilidad de las estrategias de intervención si no se mantienen y refuerzan de manera continua. Este resultado coincide con la literatura que enfatiza la importancia de programas que garanticen la sostenibilidad de la educación y acompañamiento familiar en ciberseguridad infantil (Martínez & Ramírez, 2023).

Finalmente, el progreso del proyecto, aunque alcanzó un 80% del avance esperado, señaló retos relacionados con la implementación de tecnologías y la disponibilidad de los agentes educativos y familiares. Este aspecto pone de relieve la necesidad de acompañar las medidas técnicas con procesos efectivos de capacitación y motivación, así como de fomentar una colaboración multisectorial que integre a familias, educadores, legisladores y desarrolladores tecnológicos para garantizar un entorno digital verdaderamente seguro y sostenible (European Commission, 2021; Safer Internet Centre, 2019).

En suma, los resultados de este estudio ratifican que la protección infantil en línea debe basarse en un enfoque multidimensional. La conjunción entre controles parentales tecnológicos, educación digital sólida y supervisión familiar activa es indispensable para

enfrentar los riesgos actuales y emergentes en el entorno digital. Además, la labor normativa y el avance tecnológico, por ejemplo, en inteligencia artificial, deben complementarse con la sensibilización y participación constante de la comunidad educativa y familiar para lograr un impacto real y duradero.

Conclusión

La mitigación del riesgo de exposición infantil a contenidos maliciosos en línea requiere un enfoque integral que combine educación, tecnología y comunicación efectiva. Los resultados de este estudio evidencian que la implementación de herramientas tecnológicas como el control parental contribuye significativamente a reducir el acceso a contenidos inapropiados, logrando una disminución del 85% en sitios web maliciosos en la muestra intervenida. Sin embargo, estos controles no son infalibles, dado que algunos menores intentan evadirlos, lo que resalta la necesidad de complementar la tecnología con un diálogo abierto y constante entre padres e hijos.

La educación digital desde una edad temprana se demostró fundamental para mejorar la capacidad de los niños para reconocer amenazas en línea, con un aumento notable en la identificación de phishing y otros riesgos digitales. Además, la capacitación incrementó la supervisión activa de los padres, fortaleciendo la vigilancia y apoyo familiar, elementos clave para la protección efectiva en un entorno digital tan dinámico y complejo.

Adicionalmente, la percepción positiva de los niños hacia las herramientas de control parental, tras recibir formación, refleja la importancia de incluir a los menores en los procesos educativos y de seguridad digital para fomentar su colaboración y confianza. Asimismo, la disminución del uso de sitios de riesgo y el menor número de incidentes evidencian cambios positivos en los hábitos digitales.

Es importante destacar que la responsabilidad no recae solo en familias y educadores. Las plataformas digitales deben proveer herramientas de seguridad eficaces y asegurar una moderación responsable del contenido. Paralelamente, autoridades y legisladores tienen el deber de fortalecer normativas y establecer políticas públicas actualizadas que garanticen un entorno seguro y respetuoso para los niños, tal como lo evidencian marcos regulatorios vigentes como la COPPA y el GDPR, y las recomendaciones de organismos internacionales.

Finalmente, el desarrollo del pensamiento crítico en los niños emerge como un componente esencial para que puedan discernir entre información confiable y desinformación o riesgos potenciales. Solo a través de la colaboración coordinada y continua entre padres, educadores, legisladores y plataformas tecnológicas será posible crear un entorno digital seguro, educativo y sostenible para las generaciones presentes y futuras.

Este estudio subraya la necesidad de mantener las estrategias de educación y supervisión de forma sostenida, dado que una parte de los padres mostró disminución en el monitoreo con el tiempo, lo que podría afectar la eficacia a largo plazo de estas intervenciones. En consecuencia, se recomienda que los programas de protección infantil incluyan mecanismos de refuerzo y seguimiento continuo para garantizar su impacto duradero.

Referencias bibliográficas

Child Safety Online. (2023). *Cómo proteger a los niños en internet: Guía para padres y cuidadores*. https://www.childsafetyonline.org/proteccion-en-internet

Díaz, M. R., & Castro, A. (2021). Uso de inteligencia artificial para la detección de contenido malicioso. *Innovación en Ciberseguridad: Inteligencia Artificial para la detección de binarios maliciosos*. [Información editorial pendiente].

Díaz, M. R., & Rodríguez, L. (2021). Efectividad de algoritmos de inteligencia artificial en la detección de contenido inapropiado para niños. *Revista de Ciberseguridad y Tecnología*, 10(2), 34-45.

European Commission. (2021). *Estrategias de la UE para la protección infantil online*. https://ec.europa.eu/online-child-protection

Family Online Safety Institute. (2022). *Consejos para proteger a los niños en el entorno digital*. https://www.fosi.org/proteccion-digital

Fepropaz. (2025). *Cómo proteger a los niños en internet: guía de control parental y ciberseguridad*. https://fepropaz.com/como-proteger-a-los-ninos-en-internet-guia-de-control-parental-y-ciberseguridad/

Fundación ALIA2. (2021). *Herramientas tecnológicas para la supervisión infantil en internet*. https://www.fundacionalia2.org/herramientas-digitales

López, M. (2019). El impacto del ciberacoso en la salud mental de los jóvenes. *Revista de Psicología y Sociedad*, 12(3), 110-115.

Martínez, J., & Pérez, R. (2018). Impacto de las herramientas de control parental en la protección infantil. *Ciberseguridad Familiar*. https://iconline.ipleiria.pt/bitstream/10400.8/3745/1/UPTIC_Cindy+Coronel.pdf

Martínez, J., & Ramírez, L. (2023). Colaboración multidimensional para la protección infantil en línea. *Revista Iberoamericana de Ciberseguridad*, 5(1), 78-92.

Ministerio de Educación (México). (2020). *Estrategias educativas para la ciberseguridad infantil*. https://www.educacion.gob.mx/ciberseguridad-infantil

Livingstone, S. (2010). *Riesgos en línea y protección infantil: Sensibilización y educación de padres y educadores*. Editorial Ciencias Sociales.

Rodríguez, M., & Vargas, P. (2020). Inteligencia artificial para la protección infantil en plataformas digitales. *Tecnología y Sociedad*, 8(2), 10-18.

Safe Kids Worldwide. (2021). *10 consejos para mantener seguros a los niños en línea*. https://www.safekids.org/safety-tips

Safer Internet Centre. (2019). *Manual de protección infantil digital*. Safer Internet Centre. https://www.saferinternet.org/

Save the Children. (2019). *Ciberacoso: Medidas preventivas y educativas*. https://www.savethechildren.org/

UNICEF. (2022). *Protección infantil en el entorno digital: Riesgos y soluciones*. https://www.unicef.org/es/proteccion-infantil-digital