Hacia una cultura digital inclusiva: adolescencia y seguridad desde UNESCO, UNICEF y Agenda 2030

Towards an Inclusive Digital Culture: Adolescence and Safety from UNESCO, UNICEF, and the 2030 Agenda

Delia Consuegra Herrera[1], Antonio Sucre Medina[2] y María Mitre Vásquez[3]
[1]Universidad de Panamá, delia.consuegra@up.ac.pa, https://orcid.org/0000-0002-4661-6578, Panamá
[1]Universidad de Panamá, antonio.sucre@up.ac.pa, https://orcid.org/0009-0000-0243-277X, Panamá
[1]Universidad de Panamá, maria.mitrev@up.ac.pa, https://orcid.org/0009-0000-8154-025X, Panamá

Información del Artículo

Trazabilidad:

Recibido 07-09-2025
Revisado 08-09-2025
Aceptado 03-10-2025

Palabras Clave:

Informática
Adolescencia
Seguridad digital
Control parental
Ciberdelitos

RESUMEN

La expansión acelerada de Internet en Panamá y en el mundo ha transformado la vida de niños y adolescentes, incrementando tanto sus oportunidades de aprendizaje como los riesgos asociados a la exposición digital. En la última década, fenómenos como el ciberacoso, el grooming, el sexting y la suplantación de identidad se han visto agravados por nuevas amenazas, entre ellas los *deepfakes*, las adicciones digitales y el uso indiscriminado de herramientas de inteligencia artificial generativa. Ante este panorama, el control parental emerge como una estrategia esencial, no solo a través de aplicaciones especializadas como Qustodio, Bark, Canopy, Kaspersky Safe Kids o Family Link, sino también mediante un acompañamiento educativo que fortalezca la ciudadanía digital responsable. En consonancia con la Agenda 2030, particularmente los Objetivos de Desarrollo Sostenible 4, 10 y 16, organismos internacionales como UNESCO y UNICEF han subrayado la necesidad de promover competencias digitales, proteger los derechos de la infancia en entornos virtuales y garantizar entornos inclusivos y seguros. Este artículo analiza las principales herramientas de control parental, revisa la normativa vigente en Panamá y propone un enfoque integral de seguridad digital que combine tecnología, educación y políticas públicas orientadas a la protección de adolescentes y a la construcción de una cultura digital inclusiva.

Keywords:

Computer science
Adolescence
Digital security
Parental control
Cybercrimes

ABSTRACT

The accelerated expansion of the Internet in Panama and worldwide has transformed the lives of children and adolescents, increasing both their learning opportunities and the risks associated with digital exposure. In the last decade, phenomena such as cyberbullying, grooming, sexting, and identity theft have been aggravated by new threats, including deepfakes, digital addictions, and the unsupervised use of generative artificial intelligence tools. In this context, parental control emerges as an essential strategy, not only through specialized applications such as Qustodio, Bark, Canopy, Kaspersky Safe Kids, or Family Link but also through educational support that strengthens responsible digital citizenship. In line with the 2030 Agenda, particularly Sustainable Development Goals 4, 10, and 16, international organizations such as UNESCO and UNICEF have emphasized the need to promote digital competencies, protect children's rights in virtual environments, and ensure inclusive and safe digital cultures. This article analyzes the main parental control tools, reviews the current regulations in Panama, and proposes a comprehensive digital security approach that combines technology, education, and public policies aimed at protecting adolescents and fostering a safe and inclusive digital culture.

INTRODUCCIÓN

El avance vertiginoso de la cultura digital ha transformado profundamente la manera en que niños y adolescentes se relacionan con la información, la educación y el entretenimiento. En Panamá, más del 75 % de la población accede a Internet de manera regular, con más de 3.2 millones de usuarios activos en redes sociales (Autoridad Nacional para la Innovación Gubernamental [AIG], 2024). Este panorama refleja tanto oportunidades como riesgos: mientras los entornos digitales facilitan la creatividad, el aprendizaje y la participación ciudadana, también exponen a los menores a múltiples amenazas como el ciberacoso, el *grooming*, el *sexting* y la suplantación de identidad.

En los últimos cinco años han surgido, además, riesgos emergentes como los *deepfakes*, el uso de algoritmos con *dark patterns* en videojuegos y aplicaciones, y la exposición temprana a herramientas de inteligencia artificial generativa sin supervisión (UNESCO, 2023). Esta situación exige respuestas integrales que no se limiten al control tecnológico, sino que incorporen educación digital, acompañamiento familiar y políticas públicas robustas.

En este contexto, es importante destacar que la protección digital de niños y adolescentes no solo responde a necesidades familiares o nacionales, sino también a compromisos globales. La Agenda 2030 para el Desarrollo Sostenible establece metas vinculadas a la educación, la equidad y la paz que se relacionan directamente con la ciudadanía digital protegida. En particular, los ODS 4, 9, 10 y 16 señalan la necesidad de garantizar una educación inclusiva y de calidad, cerrar la brecha digital, reducir desigualdades y fortalecer sociedades pacíficas mediante instituciones sólidas (UNESCO, 2023; UNICEF, 2021). En consonancia, organismos como la UNESCO y UNICEF han subrayado que el acceso a Internet debe estar acompañado de entornos seguros y políticas de protección, integrando la alfabetización digital responsable como una competencia clave del siglo XXI.

El presente artículo actualiza el análisis de herramientas de control parental y lo vincula con los marcos internacionales de protección digital, proponiendo un enfoque integral que combine tecnología, educación y políticas públicas para la protección de adolescentes en entornos digitales.

MATERIALES Y MÉTODOS

Este trabajo se desarrolló mediante una revisión documental de enfoque cualitativo, centrada en fuentes publicadas entre 2020 y 2025. Se recopilaron datos de organismos internacionales como UNESCO y UNICEF, informes de la AIG Panamá, literatura académica de revistas indexadas en bases de datos como Scopus y Redalyc, así como reportes de organismos especializados en ciberseguridad.

Los criterios de análisis se organizaron en tres categorías:

1. Panorama de riesgos digitales: identificación de amenazas clásicas (ciberacoso, *grooming*, *sexting*, suplantación de identidad) y emergentes (deepfakes, IA generativa, adicciones digitales).
2. Herramientas de control parental: evaluación de su vigencia, funcionalidades principales (control web, gestión de aplicaciones, geolocalización, límites de uso, detección con IA) y accesibilidad.
3. Marco normativo y ético: revisión de leyes panameñas de ciberseguridad y protección de datos, así como lineamientos internacionales de UNESCO, UNICEF y la Agenda 2030.

Esta metodología permitió contrastar la información más reciente con estudios previos y con el artículo original publicado en 2023, logrando así una actualización crítica y contextualizada al escenario digital actual.

RESULTADOS

Panorama de riesgos digitales en adolescentes (2020–2025)

Los adolescentes panameños y latinoamericanos enfrentan un entorno digital cada vez más complejo. Además de los riesgos tradicionales identificados en estudios previos como el ciberacoso, el *grooming*, el *sexting* y la suplantación de identidad, se observan fenómenos emergentes en los últimos cinco años:

- Deepfakes y manipulación audiovisual: la creación de imágenes y videos falsos aplicados a menores constituye una amenaza creciente para su reputación y privacidad (UNESCO, 2023).
- Dark patterns en videojuegos y aplicaciones: interfaces que inducen a realizar compras, compartir datos o permanecer conectado de manera compulsiva, lo que incrementa la adicción digital.

- Exposición a inteligencia artificial generativa: el acceso a chatbots, generadores de texto e imágenes sin supervisión adulta plantea riesgos de manipulación, desinformación y contacto con desconocidos.
- Ciberdependencia y salud mental: el uso excesivo de pantallas está relacionado con problemas de sueño, ansiedad y aislamiento social (UNICEF, 2021).

Estos riesgos hacen evidente que el control parental no debe limitarse a restringir, sino también a formar competencias de ciudadanía digital responsable.

Tabla 1: Comparativa de herramientas de control parental (actualizada 2020–2025)

Herramienta	Control web	Límite de apps	Límite de uso	Geolocalización	Detección IA / monitoreo avanzado	Modelo gratuito	Vigencia 2025
Qustodio	✓	✓	✓	✓	✓ Reportes avanzados	✗	Vigente
Google Family Link	✓	✓	✓	✓	✗	✓	Vigente
Norton Family	✓	✓	✓	✓	✗	✓	Vigente
Kaspersky Safe Kids	✓	✓	✓	✓	✗	✓	Vigente
Bark	✓	✓	✓	✓	✓ IA para redes sociales	✗ (solo prueba)	Vigente
Canopy	✓	✓	✓	✓	✓ Filtrado IA peligroso en chat	✗	Vigente
Net Nanny (actual.)	✓	✓	✓	✓	✓ Alertas dinámicas	✗	Vigente
Microsoft Family Safety	✓	✓	✓	✓	✗	✓	Vigente (sustituto de Windows Live)
Secure Kids	✓	✓	✓	✓	✗	✓	Vigente
Screen Time	✓	✓	✓	✓	✗	✓	Obsoleta (última actualización 2022)
Kidbox	✓	✗	✗	✗	✗	✓	Obsoleta

Análisis:

- Las herramientas Qustodio, Bark y Canopy destacan por integrar funciones avanzadas con inteligencia artificial.
- Google Family Link y Microsoft Family Safety se consolidan como opciones gratuitas y accesibles para la mayoría de las familias.
- Screem Time y Kidbox han quedado obsoletas, mientras que Windows Live Family Safety fue sustituido por Microsoft Family Safety.

El mercado tiende hacia soluciones integrales que combinan control web, gestión de apps y monitoreo de redes sociales con IA.

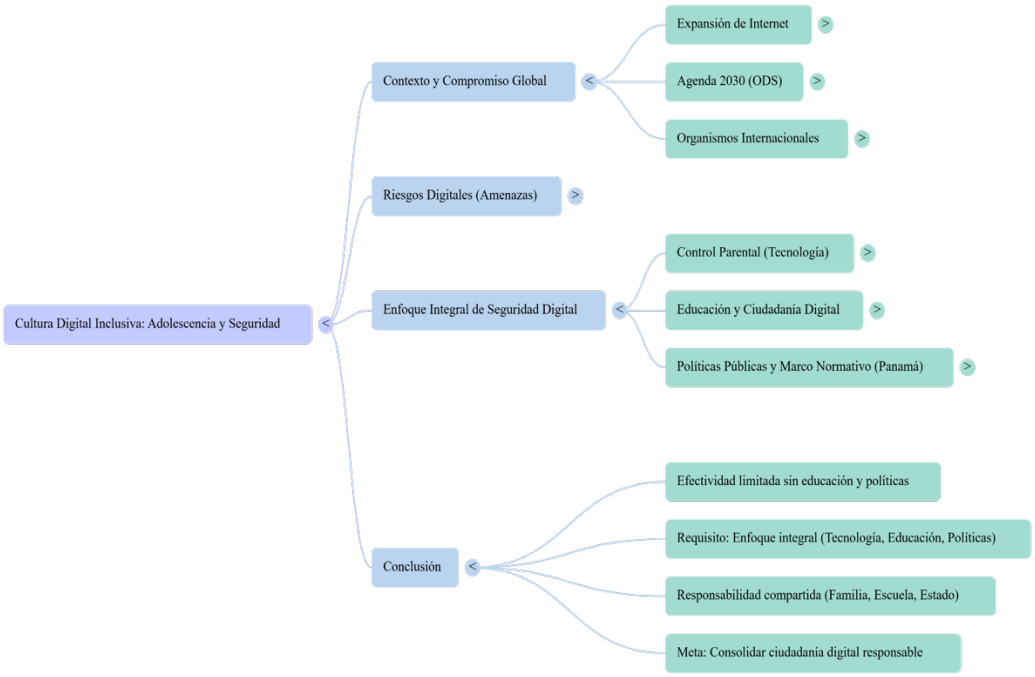

Fig. 1: Mapa conceptual del estudio

DISCUSIÓN

Más allá del software: educación y ciudadanía digital
Si bien las herramientas de control parental son útiles para mitigar riesgos inmediatos, no constituyen una solución integral. La literatura reciente subraya que la supervisión técnica debe complementarse con procesos de alfabetización digital crítica, fomentando en adolescentes la capacidad de reconocer riesgos, proteger su privacidad y ejercer un uso responsable de la tecnología (Delgado-Zambrano, 2023).
En este sentido, el control parental debe entenderse no solo como un filtro, sino como una estrategia educativa que promueva la ciudadanía digital responsable, donde adolescentes aprendan a autorregular su consumo digital y a identificar situaciones de vulnerabilidad.

Relación con los Objetivos de Desarrollo Sostenible (ODS)
La seguridad digital y la protección de adolescentes se vinculan directamente con la Agenda 2030:

- ODS 4 (Educación de calidad): la alfabetización digital responsable forma parte de las competencias del siglo XXI.
- ODS 10 (Reducción de desigualdades): garantizar entornos digitales seguros para todos los adolescentes, especialmente aquellos en situación de vulnerabilidad, contribuye a cerrar la brecha digital.
- ODS 16 (Paz, justicia e instituciones sólidas): prevenir delitos como el *grooming* o el ciberacoso fortalece la convivencia digital pacífica y protege los derechos de la infancia.

Perspectivas de la UNESCO
La UNESCO ha enfatizado que la ética digital y la seguridad de los menores deben considerarse como ejes prioritarios de la política educativa. En su *Recomendación sobre la Ética de la Inteligencia Artificial* (2021, 2023), advierte que la protección infantil debe guiar el diseño y uso de tecnologías basadas en IA. Además, promueve la noción de competencias digitales inclusivas, que combinan habilidades técnicas con valores de respeto, privacidad y derechos humanos (UNESCO, 2023).

Perspectivas de UNICEF
Por su parte, UNICEF ha insistido en que ningún país cuenta con sistemas perfectos para la protección en línea (UNICEF, 2021). En sus informes recientes destaca que los niños acceden a Internet a edades cada vez más tempranas, lo que exige estrategias integrales que incluyan:

- Marco legal y regulatorio sólido.
- Acompañamiento parental informado.
- Plataformas tecnológicas con diseño seguro por defecto (*safety by design*).

De este modo, el control parental debe concebirse como parte de un ecosistema de protección digital, no como un recurso aislado.

Regulaciones en Panamá
El marco normativo panameño ha dado pasos significativos en los últimos años:

- Ley 81 de 2019 sobre protección de datos personales.
- Ley 14 de 2023 sobre regulación de la inteligencia artificial, que incluye restricciones para el uso de IA en menores de edad.
- Iniciativas de la Autoridad Nacional para la Innovación Gubernamental (AIG) orientadas a ciberseguridad y protección de la infancia digital (AIG, 2024).

A pesar de estos avances, organismos como IPANDETEC y la sociedad civil señalan la necesidad de fortalecer las políticas públicas, dotarlas de mecanismos de aplicación más efectivos y articularlas con los lineamientos internacionales de UNESCO y UNICEF.

Ciudadanía digital y Agenda 2030: aportes de los ODS
La ciudadanía digital protegida no puede comprenderse de manera aislada, sino en el marco de los compromisos internacionales de desarrollo sostenible. Los Objetivos de Desarrollo Sostenible ofrecen un marco que conecta la protección de adolescentes en entornos digitales con metas globales de inclusión, equidad y derechos humanos.

- ODS 4 (Educación de calidad): la alfabetización digital y mediática es parte esencial de la educación inclusiva, al preparar a los jóvenes para interactuar de manera segura y crítica en entornos digitales (UNESCO, 2023).
- ODS 9 (Industria, innovación e infraestructura): el acceso universal y asequible a Internet de calidad es indispensable para garantizar igualdad de oportunidades y reducir la vulnerabilidad frente a riesgos digitales (ONU, 2020).
- ODS 10 (Reducción de desigualdades): la brecha digital refuerza desigualdades sociales y de género; por ello, la protección en línea debe considerarse un componente de justicia social (UNICEF, 2021).
- ODS 16 (Paz, justicia e instituciones sólidas): la prevención de ciberdelitos como el *grooming*, el ciberacoso o el fraude digital contribuye a sociedades más pacíficas y resilientes, asegurando que los derechos de los menores sean respetados en espacios digitales (UNESCO, 2021).

De este modo, los ODS refuerzan que la ciudadanía digital protegida no es solo un asunto tecnológico, sino un derecho humano y una condición necesaria para el desarrollo sostenible. La UNESCO insiste en que las competencias digitales deben articularse con valores éticos, mientras que UNICEF promueve el principio de *safety by design* en plataformas tecnológicas para salvaguardar a los menores (UNICEF, 2023). Integrar estas perspectivas en las políticas nacionales, como las leyes de protección de datos y las estrategias de ciberseguridad en Panamá, fortalece la coherencia entre lo local y lo global.

CONCLUSIÓN

El análisis realizado permite afirmar que la protección digital de los adolescentes en Panamá y en la región requiere un enfoque integral que trascienda el uso de aplicaciones tecnológicas. Si bien las herramientas de control parental —como Qustodio, Family Link, Norton Family, Kaspersky Safe Kids, Bark o Canopy— representan un apoyo esencial para la supervisión digital, su efectividad se limita cuando no se acompañan de procesos educativos y políticas públicas coherentes.
En los últimos cinco años se ha evidenciado un aumento en los riesgos emergentes, como los *deepfakes*, los *dark patterns* y la exposición a inteligencia artificial generativa. Esto refuerza la urgencia de construir una cultura digital inclusiva y segura, donde la familia, la escuela y el Estado asuman responsabilidades compartidas.
El alineamiento con la Agenda 2030 y, en particular, con los Objetivos de Desarrollo Sostenible 4, 10 y 16, ofrece un marco para integrar la seguridad digital con la educación de calidad, la reducción de desigualdades

y la promoción de sociedades pacíficas. Tanto la UNESCO como UNICEF han enfatizado que el control parental debe formar parte de un ecosistema de protección digital más amplio, en el que se prioricen los derechos de los niños y adolescentes, la alfabetización digital crítica y la ética en el uso de nuevas tecnologías.

Finalmente, Panamá ha avanzado con la Ley 81 de 2019 sobre protección de datos personales y la Ley 14 de 2023 sobre inteligencia artificial. Sin embargo, aún queda camino por recorrer para garantizar mecanismos de aplicación efectivos y alineados con estándares internacionales. Solo a través de la articulación entre tecnología, educación y políticas públicas será posible consolidar una ciudadanía digital responsable y proteger a las futuras generaciones en entornos cada vez más interconectados.

El mapa conceptual de la Fig. 1. muestra que, aunque la tecnología de control parental es un apoyo crucial, la verdadera protección digital de los adolescentes se logra únicamente integrando la Tecnología, la Educación y las Políticas Públicas, bajo el paraguas de los derechos de la infancia y los Objetivos de Desarrollo Sostenible.

REFERENCIAS

Autoridad Nacional para la Innovación Gubernamental (AIG). (2024). *Informe de conectividad digital en Panamá*. Panamá: AIG.

Delgado-Zambrano, O. (2023). Implementación de aplicativos de control parental en el uso de internet como herramientas tecnológicas de apoyo para el desempeño académico. *Revista Cátedra, 6*(1), 57–77. https://doi.org/10.29166/catedra.v6i1.4078

UNESCO. (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. París: UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000380455

UNESCO. (2023). *Educación digital y competencias para el siglo XXI*. París: UNESCO. https://www.unesco.org/es/digital-competencies-skills?utm_source=chatgpt.com

UNICEF. (2021). *Proteger los derechos de la infancia en tiempos de crisis*. UNICEF. https://www.unicef.org/media/120406/file/UNICEF%20Annual%20Report%202021%20SP.pdf

UNICEF. (2023). *Estado mundial de la infancia 2023: Para cada niño, un futuro digital inclusivo*. UNICEF.

IPANDETEC. (2022). *Ciberseguridad y derechos digitales en Panamá*. Panamá: IPANDETEC