Protección Infantil en Línea en América Latina

Riesgos, Marcos y Respuestas de Política Pública

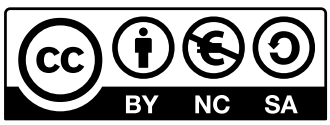
DIGI AMERICAS

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks Google

kriptos LUMU netskope paloalto Resecurity Schneider Electric SISAP SOPHOS

TANIUM tenable Trellix TrendAI whalemate zscaler



Resumen Ejecutivo

La protección infantil en línea (COP, por sus siglas en inglés) se ha convertido en un desafío central de la gobernanza digital en América Latina. A medida que niñas, niños y adolescentes pasan una mayor parte de sus vidas en línea, la región debe ampliar la conectividad significativa y, al mismo tiempo, garantizar que los entornos digitales sean seguros, protegidos, respetuosos de la privacidad y apropiados para la edad. Los riesgos en línea, incluindo el grooming, la explotación y el abuso sexual infantil, los contenidos nocivos, las violaciones de privacidad, la desinformación, el ciberacoso y los daños amplificados algorítmicamente, están creciendo en escala y complejidad, especialmente a medida que la inteligencia artificial y otras tecnologías emergentes transforman el ecosistema digital.

Los países de América Latina no parten de cero. Muchos han adoptado leyes de protección de datos, estrategias de ciberseguridad, programas de alfabetización digital, mecanismos de denuncia e iniciativas de seguridad infantil. Varios países ya han comenzado a mostrar avances importantes, con enfoques que van desde la protección de datos basada en derechos y las campañas educativas hasta marcos más amplios de responsabilidad de plataformas y ciberseguridad. Sin embargo, la implementación sigue siendo desigual, y los enfoques nacionales fragmentados limitan la capacidad de la región para responder eficazmente a daños que son inherentemente transfronterizos.

El informe identifica varias brechas persistentes: definiciones legales inconsistentes, obligaciones divergentes para las plataformas, estrategias de ciberseguridad con atención limitada a riesgos específicos para niñas, niños y adolescentes, capacidades desiguales de aplicación, cooperación transfronteriza lenta y la dificultad de implementar verificación de la edad y moderación de contenidos de manera que protejan la privacidad y la libertad de expresión. Estos desafíos imponen una carga poco realista sobre familias, educadores y comunidades para gestionar riesgos que requieren respuestas coordinadas de carácter legal, técnico, institucional y del sector privado.

Los marcos internacionales de UNICEF, la UIT, la OACNUDH, la CEPAL y otros ofrecen una base sólida para la acción regional. Estos marcos enfatizan los derechos de la niñez, la seguridad desde el diseño y la privacidad desde el diseño, la gobernanza multisectorial, la alfabetización digital, el apoyo a las víctimas y la aplicación coordinada. Los ejemplos de política pública de Australia, la Unión Europea, el Reino Unido e India, así como de países

de América Latina, también ilustran distintos modelos para operacionalizar la responsabilidad de las plataformas, el diseño apropiado para la edad, la verificación de la edad y la supervisión regulatoria.

La conclusión central es que América Latina no necesita un modelo único y uniforme para proteger a niñas, niños y adolescentes en línea, pero sí requiere una mayor armonización. Los países deben preservar la flexibilidad necesaria para reflejar sus sistemas jurídicos y contextos culturales nacionales, al tiempo que se alinean en torno a principios interoperables, estándares técnicos compartidos y mecanismos coordinados de aplicación. Entre las acciones prioritarias se incluyen el desarrollo de un marco modelo, la armonización de definiciones y salvaguardas clave, la creación de estándares regionales de denuncia e intercambio de evidencia, la promoción de mecanismos de verificación de la edad que preserven la privacidad, el fortalecimiento de los procesos de asistencia jurídica mutua, el establecimiento de puntos focales de seguridad en línea, la inversión en laboratorios técnicos compartidos y capacitación, y la incorporación de la gobernanza multisectorial y las evaluaciones de impacto en derechos humanos en la formulación de políticas. Proteger a niñas, niños y adolescentes en línea no es un ejercicio regulatorio único. Es un compromiso continuo de gobernanza que requiere que gobiernos, industria, sociedad civil, educadores, familias e instituciones regionales trabajen conjuntamente. Al combinar interoperabilidad legal, buenas prácticas de ciberseguridad, salvaguardas de privacidad, participación infantil y cooperación regional, América Latina puede construir un enfoque más coherente y sostenible que proteja a niñas, niños y adolescentes frente a daños, al tiempo que les permita beneficiarse plenamente de las oportunidades de la era digital.

Tabla de Contenidos

Introducción

El mundo está cada vez más interconectado, y el acceso a internet sustenta hoy el desarrollo económico, la educación y la participación social. En América Latina, la rápida adopción digital entre las poblaciones jóvenes ha ampliado las oportunidades de aprendizaje, comunicación e inclusión, al tiempo que ha expuesto a niñas, niños y adolescentes a una gama creciente de riesgos en línea, incluido el uso nocivo de redes sociales, el uso indebido de datos y la privacidad, el grooming en línea, la explotación sexual, la exposición a la desinformación y los contenidos amplificados algorítmicamente que pueden afectar negativamente la salud mental y el desarrollo. A pesar de la importancia reconocida de la conectividad, se estima que dos tercios de los niños y niñas en edad escolar del mundo aún carecen de acceso a internet en el hogar, lo que pone de manifiesto desigualdades persistentes que también se reflejan en la región.[1]

Si bien la conectividad digital ofrece importantes beneficios sociales y económicos, sus implicaciones para la salud mental y física, la privacidad, la educación y el bienestar general de niñas, niños y adolescentes siguen siendo desiguales y dependientes del contexto.[2] Durante la última década, el debate de política pública sobre protección infantil en línea ha evolucionado desde un enfoque estrecho centrado en el acceso y la alfabetización digital hacia un énfasis más amplio en la responsabilidad de las plataformas, la protección de datos, la ciberseguridad y el diseño apropiado para la edad, impulsado en gran medida por la creciente evidencia sobre los peligros del mayor uso en línea y sus impactos sociales adversos de largo plazo. Los gobiernos de América Latina han comenzado a responder mediante diversos enfoques, entre ellos el fortalecimiento de marcos de protección de datos para menores, la actualización de estrategias de ciberseguridad, la introducción de obligaciones para plataformas y la expansión de iniciativas de protección infantil y alfabetización digital. Sin embargo, estos esfuerzos siguen estando fragmentados, con variaciones significativas en las definiciones legales, la capacidad de aplicación y la coordinación institucional.

La inteligencia artificial (IA) y otras tecnologías emergentes probablemente amplifican tanto las

[1] https://www.unicef.org/innocenti/reports/childhood-digital-world
[2] https://www.unicef.org/innocenti/reports/childhood-digital-world

oportunidades como los riesgos, y podrían ampliar las brechas existentes si no se abordan de manera proactiva.[3] En América Latina, donde los marcos legales, los enfoques de gobernanza digital y los contextos culturales varían ampliamente, estos desafíos son particularmente complejos y cada vez más transfronterizos.

Este documento examina cómo los países de la región están abordando la protección infantil en línea en la intersección entre la gobernanza digital y la ciberseguridad, destacando desafíos comunes, brechas de política pública y áreas de divergencia. También analiza el papel de los marcos internacionales y la cooperación regional, y propone vías prácticas hacia una mayor armonización, incluidos estándares interoperables, mecanismos de aplicación transfronteriza e iniciativas de fortalecimiento de capacidades. Abordar estos temas requerirá una acción coordinada entre gobiernos, industria y sociedad civil para garantizar que niñas, niños y adolescentes puedan participar en el entorno digital de manera segura, protegida y equitativa.

[3] https://www.cgdev.org/blog/three-reasons-why-ai-may-widen-global-inequality

Brechas y tensiones clave que obstaculizan una COP efectiva en América Latina

El entorno digital se está volviendo cada vez más central para casi todos los aspectos de la vida de niñas, niños y adolescentes, incluida la educación, la interacción social, el acceso a servicios gubernamentales y la participación en la vida cívica.[4] En toda América Latina, los esfuerzos para expandir la conectividad han sido una prioridad de política pública central, reflejando el vínculo ampliamente reconocido entre el acceso a internet y el crecimiento económico, la innovación y la inclusión social.[5] Los operadores de telecomunicaciones y los proveedores de servicios de internet (ISP) han desempeñado un papel fundamental en la ampliación de esta conectividad, invirtiendo en infraestructura y habilitando una mayor participación en la economía digital.[6], [7] De hecho, una conectividad a internet confiable se entiende cada vez más como un indicador clave de desarrollo, ya que permite el acceso a información, mercados y servicios públicos.[8], [9]

Sin embargo, esta rápida expansión del acceso digital no siempre va acompañada de sistemas igualmente robustos para proteger a niñas, niños y adolescentes en línea. Si bien la conectividad genera beneficios económicos y sociales significativos, también introduce un conjunto paralelo de riesgos que afectan de manera desproporcionada a los usuarios más jóvenes.[10] La mayor exposición a redes sociales se ha asociado con resultados negativos para la salud mental, mientras que los entornos en línea han facilitado nuevas formas de daño, incluida la explotación sexual y el grooming, la propagación de desinformación e información errónea, el uso indebido de datos y privacidad, y los contenidos amplificados algorítmicamente que pueden influir en el comportamiento y

---

4 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

5 https://openknowledge.worldbank.org/entities/publication/483cab21-85be-544f-93c6-302e094b2dfe

6 https://publications.iadb.org/en/strategies-and-business-models-improving-broadband-connectivity-latin-america-and-caribbean

7 https://2017-2021.state.gov/u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean/

8 https://www.cepal.org/en/publications/45835-childhood-and-adolescence-digital-age-comparative-report-kids-online-surveys

9 https://blogs.worldbank.org/en/digital-development/can-internet-access-lead-improved-economic-outcomes

10 https://www.unicef.org/documents/keeping-children-safe-online

el desarrollo.[11], [12] Estos riesgos se ven agravados por la escala, la velocidad y la naturaleza transfronteriza de las plataformas digitales.

En muchos casos, los marcos de política pública y regulación de la región han tenido dificultades para mantenerse al ritmo de estos desafíos en evolución. Los enfoques fragmentados y poco desarrollados de protección infantil en línea a menudo han dejado a familias, educadores y comunidades gestionando riesgos complejos con apoyo limitado. La expectativa de que manejen esta situación por sí solos no es realista, dada la sofisticación técnica e institucional necesaria para abordarla de manera efectiva. Como resultado, brechas y tensiones significativas siguen obstaculizando una respuesta regional coherente.

Uno de los desafíos más persistentes es la fragmentación de las definiciones legales y las obligaciones regulatorias entre países, particularmente en relación con las definiciones de restricciones de edad, qué constituye contenido nocivo y cuáles son las responsabilidades de las plataformas y los fabricantes de dispositivos. Esta falta de alineación genera incertidumbre tanto para reguladores como para actores de la industria, complica la aplicación y debilita la rendición de cuentas. Del mismo modo, los regímenes divergentes de protección de datos y privacidad, junto con capacidades limitadas de aplicación, restringen en algunos casos la capacidad de las autoridades para proteger la información personal de niñas, niños y adolescentes y responder eficazmente a las violaciones.

La cooperación transfronteriza sigue siendo otra debilidad crítica. La actividad dañina en línea frecuentemente trasciende fronteras nacionales, pero los mecanismos de asistencia jurídica mutua, intercambio de evidencia y esfuerzos coordinados de remoción o trazabilidad inversa suelen ser lentos, inconsistentes o subutilizados. Para los operadores de red y proveedores de servicios, esta fragmentación genera desafíos operativos al responder a solicitudes legales e implementar medidas de seguridad en múltiples jurisdicciones. Esto se complica aún más por desafíos técnicos, incluida la necesidad de implementar sistemas de verificación o verificación de la edad que no dependan de la recolección intrusiva de datos, así como la dificultad de moderar contenidos a escala en múltiples idiomas, dialectos y contextos culturales presentes en la región.

[11] https://law.stanford.edu/2024/05/20/social-media-addiction-and-mental-health-the-growing-concern-for-youth-well-being/

[12] https://www.hopkinsmedicine.org/health/wellness-and-prevention/social-media-and-mental-health-in-children-and-teens

Al mismo tiempo, los esfuerzos para fortalecer la protección infantil en línea deben equilibrar cuidadosamente derechos y objetivos de política pública en tensión. Regulaciones demasiado amplias o mal diseñadas corren el riesgo de socavar la libertad de expresión, restringir el acceso a la información o incentivar a las plataformas a adoptar medidas contundentes como la remoción excesiva o el bloqueo generalizado de contenidos. Estas tensiones subrayan la necesidad de enfoques matizados y respetuosos de los derechos, capaces de mitigar daños de manera efectiva sin generar consecuencias no deseadas.

En conjunto, estos desafíos apuntan a la necesidad de una mayor coordinación regional e interoperabilidad de políticas. Marcos legales más armonizados, estándares técnicos alineados y mecanismos estructurados de colaboración público-privada pueden ayudar a reducir la fragmentación, mejorar los resultados de aplicación y ofrecer expectativas más claras para los actores de la industria que operan en múltiples jurisdicciones.

Desafíos de ciberseguridad y operativos en la COP

A medida que la conectividad digital se convierte en una característica definitoria de la vida moderna, la protección de niñas, niños y adolescentes en línea está cada vez más determinada no solo por consideraciones sociales y regulatorias, sino también por la seguridad subyacente de los sistemas e infraestructuras digitales. La ciberseguridad y la protección infantil en línea están profundamente interconectadas. Las vulnerabilidades en plataformas, dispositivos y redes pueden ser explotadas para facilitar daños como el grooming, la explotación sexual, las filtraciones de datos que involucran a menores y la manipulación de niñas, niños y adolescentes mediante contenido malicioso o amplificado algorítmicamente. La proliferación de dispositivos conectados, como teléfonos inteligentes, plataformas de videojuegos y juguetes habilitados para internet, ha ampliado aún más la superficie de ataque potencial, introduciendo nuevos riesgos cuando estándares de seguridad débiles

pueden exponer a niñas, niños y adolescentes a vigilancia, explotación o recolección no autorizada de datos. En este contexto, proteger a niñas, niños y adolescentes en línea requiere no solo moderación de contenidos y supervisión regulatoria, sino también prácticas robustas de ciberseguridad incorporadas en todo el ecosistema digital.

A pesar de esta clara intersección, los enfoques nacionales en América Latina varían significativamente en la medida en que las estrategias de ciberseguridad abordan explícitamente riesgos específicos para niñas, niños y adolescentes. Aunque algunos países han comenzado a incorporar elementos de protección infantil en marcos más amplios de ciberseguridad, muchas estrategias siguen centradas en infraestructura crítica, seguridad económica y ciberdelincuencia en general, con atención limitada a las vulnerabilidades únicas de niñas, niños y adolescentes. En el plano operativo, persisten brechas en áreas clave como mecanismos de denuncia seguros y accesibles, preservación efectiva de evidencia y sistemas coordinados de respuesta a incidentes que integren a fuerzas de seguridad, agencias de ciberseguridad y servicios de protección infantil. Fortalecer la protección en este ámbito requerirá una colaboración más estrecha entre gobiernos y sector privado, junto con mejor intercambio de información y protocolos más claros de respuesta intersectorial. Desarrollar estas capacidades es esencial para garantizar que los esfuerzos de ciberseguridad contribuyan de manera significativa a entornos digitales más seguros para niñas, niños y adolescentes en toda la región.

Marcos globales y normas internacionales

Los esfuerzos para abordar la seguridad infantil en línea están cada vez más moldeados por una combinación de marcos internacionales y respuestas de política pública nacionales. Los marcos globales, incluidos los desarrollados por organizaciones como el Fondo de las Naciones Unidas para la Infancia (UNICEF) y la Unión Internacional de Telecomunicaciones (UIT), han establecido principios orientadores para proteger a niñas, niños y adolescentes en entornos digitales, haciendo énfasis en enfoques basados en derechos, gobernanza multisectorial y participación infantil.[13] Estos marcos ofrecen una base importante para los países que buscan equilibrar los beneficios de la conectividad con la necesidad de mitigar daños.

[13] https://www.unicef.org/documents/guidelines-industry-child-online-protection

Al mismo tiempo, los gobiernos de todo el mundo y de América Latina están traduciendo estos principios en políticas nacionales mediante una variedad de medidas legales y regulatorias, incluidas disposiciones específicas de protección de datos para niñas, niños y adolescentes, obligaciones para plataformas, restricciones de edad e iniciativas de alfabetización digital. Sin embargo, la interpretación e implementación de estas normas varía considerablemente entre jurisdicciones, reflejando diferencias en sistemas legales, capacidades institucionales y prioridades sociales.

Este panorama en evolución resalta tanto oportunidades como tensiones. Si bien los marcos internacionales promueven una mayor alineación y estándares compartidos, los enfoques nacionales suelen divergir en la forma en que equilibran objetivos en competencia, como privacidad frente a verificación de la edad efectivo, o libertad de expresión frente a moderación de contenidos y seguridad infantil. Comprender cómo estas normas globales influyen en los contextos nacionales y se adaptan a ellos es fundamental para identificar vías hacia una protección infantil en línea más coherente y efectiva en la región.

Marcos internacionales

Directrices de UNICEF y la UIT para la industria sobre protección infantil en línea[14]

Las Directrices de UNICEF y la UIT para la industria sobre protección infantil en línea ofrecen un marco global reconocido y no vinculante sobre cómo los actores del sector privado —incluidos operadores de telecomunicaciones, proveedores de servicios de internet y plataformas digitales— deben respetar y apoyar los derechos de niñas, niños y adolescentes en el entorno digital. Desarrolladas mediante un proceso multisectorial, las directrices enfatizan un enfoque basado en derechos alineado con la Convención sobre los Derechos del Niño de las Naciones Unidas y los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos.

El marco describe cinco áreas centrales de acción para la industria: integrar los derechos de la niñez en las políticas y la gobernanza corporativa; implementar procesos para detectar y abordar material de abuso sexual infantil; diseñar entornos digitales más seguros y apropiados para la edad; promover la alfabetización digital y el uso responsable entre niñas, niños, adolescentes y sus cuidadores; y

[14] https://www.unicef.org/media/66616/file/industry-guidelines-for-online-childprotection.pdf

aprovechar la tecnología para apoyar la participación infantil y el compromiso cívico.[15]

De manera importante, las directrices reconocen la responsabilidad compartida de los actores de la industria tanto para mitigar daños como para habilitar experiencias positivas en línea, alentando a las empresas a incorporar la protección infantil en el diseño de productos, las prácticas operativas y la colaboración intersectorial. También ofrecen recomendaciones específicas por sector para distintas partes del ecosistema de las TIC, incluidos ISP, operadores móviles, proveedores de contenido y plataformas, reflejando los diversos roles que estos actores desempeñan en la cadena de valor digital. En general, las directrices sirven como un punto de referencia global flexible, que ayuda a alinear las prácticas de la industria con los estándares internacionales de derechos de la niñez, al tiempo que permite la adaptación a distintos contextos regulatorios y regionales.

Comentario General No. 25 (2021) de la OACNUDH sobre los derechos de la niñez en relación con el entorno digital[16]

El Comentario General No. 25 (2021) de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH) sobre los derechos de la niñez en relación con el entorno digital proporciona orientación autorizada sobre cómo se aplica la Convención sobre los Derechos del Niño (CDN) en contextos digitales. Afirma que los derechos de niñas, niños y adolescentes se aplican plenamente en línea, incluidos los derechos a la privacidad, la protección frente a daños, el acceso a la información, la educación y la participación. El marco enfatiza que los Estados tienen la obligación de proteger a niñas, niños y adolescentes frente a riesgos en línea como la explotación, el abuso y los contenidos nocivos, al tiempo que deben garantizar que las medidas adoptadas no restrinjan indebidamente el acceso a la información o la libertad de expresión.

El Comentario General llama a un enfoque holístico y basado en derechos para la gobernanza digital, que incluya regímenes de protección de datos centrados en la niñez, estándares de diseño apropiado para la edad y mecanismos de rendición de cuentas para proveedores de servicios digitales. También subraya la importancia de la responsabilidad empresarial, exigiendo a las compañías realizar debida diligencia para identificar, prevenir y mitigar riesgos para niñas,

[15] https://merlin.obs.coe.int/download/7025/pdf
[16] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

niños y adolescentes. De manera importante, destaca la necesidad de acceso inclusivo, alfabetización digital y participación significativa de niñas, niños y adolescentes en los procesos de formulación de políticas que les afectan. En conjunto, el documento sirve como una referencia global fundamental para orientar a los gobiernos en el equilibrio entre protección, empoderamiento y derechos en el entorno digital.

CEPAL: Infancia y adolescencia en la era digital[17]

La Comisión Económica para América Latina y el Caribe (CEPAL) destaca que la transformación digital de la región presenta tanto oportunidades significativas para la inclusión como desafíos estructurales persistentes, particularmente para niñas, niños, adolescentes y poblaciones vulnerables. Aunque el acceso a internet se ha expandido considerablemente, persisten profundas desigualdades en conectividad, calidad de acceso y habilidades digitales, lo que limita la capacidad de muchos niños, niñas y adolescentes para beneficiarse plenamente del entorno digital. El informe subraya que la inclusión digital debe ir más allá del acceso para abarcar asequibilidad, uso significativo y desarrollo de capacidades digitales, especialmente en educación.

Al mismo tiempo, la CEPAL enfatiza la necesidad de marcos más sólidos de gobernanza digital para abordar riesgos emergentes, incluidos la protección de datos, la ciberseguridad y el uso seguro de plataformas digitales. Llama a enfoques coordinados de política pública, inversión en infraestructura y cooperación regional para cerrar brechas y garantizar que la transformación digital apoye el desarrollo sostenible e inclusivo. El análisis también señala la importancia de alinear las estrategias nacionales con marcos regionales e internacionales más amplios, adaptando al mismo tiempo las políticas a los contextos locales.

En general, el informe refuerza que lograr una inclusión digital equitativa y segura en América Latina requiere políticas integradas que equilibren acceso, protección y fortalecimiento de capacidades, con especial atención a niñas, niños, adolescentes y otros grupos en situación de riesgo.

[17] https://repositorio.cepal.org/server/api/core/bitstreams/51f4dc9b-9bde-4358-bd68-98275f64583d/content

Modelo de Respuesta Nacional de WeProtect para poner fin a la explotación y el abuso sexual infantil en línea[18]

El Modelo de Respuesta Nacional de la Alianza Global WeProtect ofrece un enfoque estructurado para que los gobiernos prevengan y respondan a la explotación y el abuso sexual infantil en línea (CSEA, por sus siglas en inglés). Plantea un modelo integral y sistémico basado en seis dominios clave: política y gobernanza, justicia penal, apoyo a víctimas, participación de la industria, sociedad y prevención, y coordinación y cooperación. El marco enfatiza que una protección infantil en línea efectiva requiere acción integrada entre instituciones, incluidas fuerzas de seguridad, servicios de protección infantil, reguladores y actores del sector privado.

Una característica central del modelo es su enfoque en la colaboración multisectorial y en roles y responsabilidades claramente definidos, asegurando que gobiernos, industria y sociedad civil trabajen de manera coordinada. También resalta la importancia del fortalecimiento de capacidades, el intercambio de datos y la preparación operativa, incluidos mecanismos de denuncia, investigación y apoyo a víctimas. El marco incluye un modelo de madurez que permite a los países evaluar sus capacidades actuales e identificar brechas, apoyando un enfoque gradual para fortalecer las respuestas nacionales. En general, sirve como una herramienta práctica de implementación que ayuda a los países a traducir principios internacionales en sistemas coordinados y accionables para abordar la explotación y el abuso infantil en línea.

Ejemplos de políticas nacionales

Si bien los marcos internacionales establecen un conjunto compartido de principios y expectativas para la protección infantil en línea, su efectividad depende en última instancia de cómo se traducen en leyes, regulaciones y prácticas operativas nacionales. En todo el mundo, los gobiernos están adaptando estas normas internacionales a respuestas de política doméstica que reflejan sus sistemas legales, capacidades institucionales y prioridades sociales. Este proceso ha dado lugar a un panorama diverso de enfoques para proteger a niñas, niños y adolescentes en línea, ofreciendo perspectivas valiosas sobre buenas prácticas emergentes y brechas persistentes en la implementación.

[18] https://www.weprotect.org/resources/frameworks/model-national-response/

Australia: Ley de Seguridad en Línea de 2021[19]

La Ley de Seguridad en Línea de Australia de 2021 establece un marco regulatorio integral para abordar una amplia gama de daños en línea, con un fuerte enfoque en la protección de niñas, niños, adolescentes y usuarios vulnerables. La legislación otorga poderes ampliados a la eSafety Commissioner para exigir la remoción rápida de contenidos nocivos, incluido material de ciberacoso dirigido a niñas, niños y adolescentes, abuso basado en imágenes y contenido ilegal o seriamente dañino.[20] Introduce estándares exigibles de seguridad en línea para plataformas y proveedores de servicios, requiriendo que adopten medidas proactivas para reducir la exposición a material dañino y mejorar los mecanismos de denuncia y respuesta.

La ley también incluye un marco de Basic Online Safety Expectations, que establece requisitos de referencia para proveedores de servicios digitales en materia de seguridad de usuarios, transparencia y rendición de cuentas. De manera importante, crea vías para abordar daños emergentes como el grooming en línea, la explotación sexual y la difusión no consentida de imágenes íntimas, al tiempo que apoya a las víctimas mediante mecanismos de denuncia y reparación. La legislación refleja un enfoque sistémico y basado en riesgos, que combina supervisión regulatoria, obligaciones de la industria y protecciones para usuarios con el fin de mitigar daños y mantener el acceso a servicios digitales.

En general, la ley se considera ampliamente un modelo práctico y exigible para operacionalizar la protección infantil en línea, demostrando cómo los gobiernos pueden traducir principios de alto nivel en herramientas regulatorias concretas y autoridad institucional.

Unión Europea: Resolución del Parlamento Europeo 2693/2026[21]

El Parlamento Europeo ha solicitado una acción más fuerte a nivel de la Unión Europea para combatir el ciberacoso, en particular para proteger mejor a niñas, niños y jóvenes en línea. La iniciativa enfatiza la necesidad de marcos legales más claros, mayor responsabilidad de las plataformas y mejores mecanismos de denuncia y apoyo para las víctimas. Aborda daños como el acoso en línea, el

[19] https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation

[20] https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/esafety-commissioner

[21] https://www.europarl.europa.eu/news/en/press-room/20260423IPR41845/parliament-wants-stronger-action-against-cyberbullying-in-the-eu

abuso psicológico y la difusión de contenidos nocivos, al tiempo que promueve acciones coordinadas entre los Estados miembros. La propuesta también destaca la importancia de medidas de prevención, alfabetización digital y cooperación transfronteriza, reflejando un enfoque más proactivo y armonizado para abordar el ciberacoso en la UE.

Unión Europea: Tecnologías de verificación de edad a escala de la UE[22]

El enfoque común de la Comisión Europea sobre tecnologías de verificación de edad a escala de la UE plantea un marco coordinado para proteger a menores del acceso a contenidos inapropiados para su edad en línea, particularmente en el marco de la Ley de Servicios Digitales (DSA). La iniciativa promueve el desarrollo y despliegue de soluciones de verificación de la edad que preserven la privacidad, con el objetivo de verificar si una persona usuaria está por encima o por debajo de determinada edad sin requerir una recolección excesiva de datos personales. Este enfoque busca mitigar daños como la exposición a contenido nocivo o inapropiado, el grooming en línea y la explotación, al tiempo que aborda preocupaciones sobre protección de datos y privacidad del usuario.
El marco enfatiza la interoperabilidad y estandarización en toda la UE, alentando el uso de sistemas de identidad digital confiables y credenciales reutilizables para garantizar consistencia entre plataformas y servicios. También refleja un enfoque basado en riesgos y proporcional, que exige a las plataformas implementar salvaguardas apropiadas según la naturaleza de sus servicios y los riesgos que plantean para menores. De manera importante, la iniciativa equilibra los objetivos de protección infantil con los derechos fundamentales, particularmente la privacidad y la minimización de datos, promoviendo tecnologías que reduzcan el rastreo y la elaboración de perfiles.

El enfoque de la UE demuestra cómo los gobiernos pueden avanzar soluciones escalables y técnicamente viables para la verificación de la edad que se alineen con marcos regulatorios más amplios, ofreciendo un modelo para integrar la protección infantil en sistemas de identidad digital y gobernanza de plataformas.

[22] https://digital-strategy.ec.europa.eu/en/library/commission-sets-out-common-approach-eu-wide-age-verification-technologies

Reino Unido: Ley de Seguridad en Línea de 2023[23]

La Ley de Seguridad en Línea del Reino Unido de 2023 establece un régimen regulatorio integral orientado a reducir los daños en línea, con un fuerte énfasis en la protección de niñas, niños y adolescentes. La legislación impone deberes de cuidado estatutarios a las plataformas en línea, exigiéndoles evaluar y mitigar proactivamente los riesgos asociados con contenido nocivo, particularmente para menores. Las plataformas deben implementar medidas de seguridad apropiadas para la edad, incluidas una moderación de contenidos más sólida, configuraciones de seguridad predeterminadas para niñas, niños y adolescentes, y mecanismos para prevenir la exposición a material dañino como pornografía, contenido de autolesión y abuso en línea.

La ley otorga al regulador de comunicaciones, Ofcom, una autoridad significativa de supervisión y aplicación, incluida la capacidad de establecer estándares de seguridad, exigir informes de transparencia e imponer multas sustanciales por incumplimiento. También introduce requisitos para que las plataformas aborden contenido

[23] https://www.legislation.gov.uk/ukpga/2023/50

ilegal y daños prioritarios, incluida la explotación y el abuso sexual infantil, el grooming y el ciberacoso, al tiempo que mejora los mecanismos de denuncia y reparación para usuarios.

De manera importante, la legislación adopta un enfoque basado en riesgos y proporcional, exigiendo a las empresas adaptar las protecciones según la escala y naturaleza de sus servicios. Al mismo tiempo, busca equilibrar la protección infantil con consideraciones de libertad de expresión y privacidad, incorporando salvaguardas para prevenir excesos. En general, la ley representa un modelo operativo robusto para traducir principios de protección infantil en línea en obligaciones exigibles para plataformas y supervisión regulatoria.

India: Reglas de Tecnología de la Información (Directrices para Intermediarios y Código de Ética de Medios Digitales), 2021 (actualizadas en 2023)[24]

Las Reglas de Tecnología de la Información de India (Directrices para Intermediarios y Código de Ética de Medios Digitales), 2021 (modificadas en 2023), establecen un marco regulatorio para intermediarios en línea, con disposiciones que abordan daños que afectan a niñas, niños, adolescentes y usuarios vulnerables.

Las reglas imponen obligaciones de debida diligencia a las plataformas, exigiéndoles retirar contenido ilícito dentro de plazos específicos, incluido material relacionado con abuso sexual infantil, explotación y otros contenidos dañinos. Los intermediarios también deben implementar mecanismos de reparación de quejas, designar oficiales de cumplimiento y permitir que los usuarios denuncien contenido dañino de manera eficiente.

El marco introduce obligaciones adicionales para plataformas más grandes, incluidas medidas de monitoreo proactivo y requisitos de trazabilidad para ciertos tipos de contenido, orientados a abordar cuestiones como abuso en línea, desinformación y explotación. También incluye disposiciones para restringir el acceso a contenido no apropiado para la edad y fortalecer la rendición de cuentas de los editores de medios digitales mediante un código de ética y una estructura de supervisión.

Si bien las reglas buscan mitigar daños como la explotación en línea, la difusión de contenido dañino y el abuso, también han suscitado debates importantes sobre privacidad, cifrado y libertad de expresión, particularmente en relación con los requisitos de trazabilidad. En general, el marco representa un modelo impulsado

[24] https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

por el cumplimiento que enfatiza la responsabilidad de las plataformas, la remoción rápida de contenidos y la supervisión gubernamental como herramientas clave para abordar daños en línea.

Panorama regional: cómo abordan los países de América Latina la COP

Los marcos internacionales y ejemplos nacionales mencionados demuestran una creciente convergencia en torno a principios centrales como la gobernanza basada en derechos, la coordinación multisectorial, la seguridad desde el diseño y la responsabilidad de las plataformas. Sin embargo, su implementación varía significativamente entre regiones. En América Latina, los países se encuentran en diferentes etapas de madurez política e institucional, reflejando disparidades en marcos legales, capacidad regulatoria, infraestructura digital y disponibilidad de recursos. Como resultado, los enfoques de protección infantil en línea en la región siguen siendo desiguales, con algunos países avanzando en estrategias integrales mientras otros aún desarrollan políticas fundamentales. A pesar de estas diferencias, existe una clara oportunidad —y necesidad— de que todos los países se alineen con estos principios globales compartidos, adaptándolos a contextos locales mientras trabajan hacia enfoques más consistentes, efectivos e interoperables para proteger a niñas, niños y adolescentes en línea. Los siguientes países se encuentran entre aquellos que han comenzado a abordar estos temas.

Argentina

El enfoque de Argentina hacia la protección infantil en línea se apoya en su marco establecido de protección de datos y se complementa con legislación penal específica, iniciativas de concientización pública y una estrategia emergente de ciberseguridad. La Ley No. 25.326 de Protección de Datos Personales proporciona la base legal central, estableciendo principios como consentimiento, limitación de finalidad y seguridad de datos, que se aplican a los datos de menores pero no crean un régimen plenamente diferenciado y específico para la niñez.[25], [26] La autoridad nacional de protección de datos (AAIP) ha buscado cubrir esta brecha mediante orientación

[25] https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790
[26] https://termly.io/resources/articles/argentinas-personal-data-protection-act/

no vinculante e iniciativas públicas, en particular su programa "Nuestro Mundo Digital", que promueve la alfabetización digital, conciencia sobre privacidad y salvaguardias prácticas para niñas, niños, adolescentes, familias y educadores.[27] La AAIP también ha emitido pronunciamientos sobre verificación de la edad y privacidad infantil que enfatizan proporcionalidad, minimización de datos y alineación con estándares regionales e internacionales, reflejando un enfoque cauteloso y basado en derechos para implementar salvaguardas técnicas.[28]

En el ámbito penal y preventivo, la Ley No. 27.590 (la "Ley Mica Ortega") desempeña un papel central al exigir programas de educación y concientización sobre grooming en línea, señalando un énfasis de política en la prevención mediante escuelas y campañas públicas más que en una regulación centrada en plataformas.[29] Desde la perspectiva de ciberseguridad, las capacidades de Argentina se estructuran en torno a CERT.ar, que proporciona respuesta nacional a incidentes, monitoreo de amenazas y coordinación entre sectores, formando la columna vertebral operativa para abordar riesgos digitales, incluidos los que afectan a menores.[30] Estos esfuerzos se contextualizan además en el plan federal de prevención de ciberdelitos y gestión estratégica de la ciberseguridad para 2025–2027, que integra gestión de riesgos cibernéticos, coordinación institucional y fortalecimiento de capacidades, aunque sin un enfoque específico robusto en la niñez.[31]

En general, la postura de Argentina se caracteriza por una base de protección de datos basada en derechos, complementada por medidas de seguridad infantil impulsadas por educación y concientización, así como infraestructura general de ciberseguridad. En comparación con modelos más prescriptivos, depende en mayor medida de orientación, iniciativas de política pública y herramientas de derecho penal, con menor énfasis en obligaciones vinculantes para plataformas o marcos regulatorios integrales específicos para la niñez.

---

[27] https://www.argentina.gob.ar/aaip/nuestro-mundo-digital-guia-pedagogica-y-guia-para-adolescentes

[28] https://iapp.org/news/a/argentinas-appi-creates-ai-transparency-and-protection-of-personal-data-program

[29] https://www.argentina.gob.ar/normativa/nacional/ley-27590-345231/texto

[30] https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar

[31] https://www.boletinoficial.gob.ar/detalleAviso/primera/319722/20250116

Brasil

Brasil ha adoptado un enfoque cada vez más integral e integrado de protección infantil en línea, que combina obligaciones legales, orientación regulatoria y estrategia nacional de ciberseguridad. En el centro se encuentra la Ley No. 15.211/2025 ("Digital ECA"), que establece un marco basado en derechos y fundamentado en el interés superior de niñas, niños y adolescentes, e impone obligaciones afirmativas a los proveedores de servicios digitales para garantizar seguridad desde el diseño y privacidad desde el diseño.[32] La ley exige que las plataformas implementen medidas como diseño apropiado para la edad, configuraciones predeterminadas de alta privacidad, controles parentales y evaluación continua de riesgos de funcionalidades que puedan exponer a menores a daños, incluidos sistemas algorítmicos.[33] Estas obligaciones se operacionalizan mediante el Decreto No. 12.880/2026, que crea una arquitectura federal coordinada de aplicación y denuncia, aclara responsabilidades institucionales e incorpora la protección infantil en línea dentro de una estructura de política nacional más amplia liderada por el Ministerio de Justicia.[34] [35] Los materiales gubernamentales, incluida la iniciativa "ECA Digital" del Ministerio, enfatizan un modelo preventivo y sistémico que combina regulación, concientización pública y cooperación intersectorial.[36]

En materia de gobernanza de datos, Brasil aprovecha su régimen existente de protección de datos bajo la Ley General de Protección de Datos Personales (LGPD)[37], con la Autoridad Nacional de Protección de Datos (ANPD)[38], recientemente elevada de autoridad a agencia federal, emitiendo orientación detallada sobre el tratamiento de datos personales de niñas, niños y adolescentes.[39] Esto incluye requisitos de base legal, limitación de finalidad y salvaguardas reforzadas, junto con una expectativa clara de privacidad por defecto y restricciones al perfilamiento y la publicidad comportamental.[40] Como complemento, la orientación preliminar de 2026 de la ANPD sobre verificación de la edad confiable destaca un enfoque técnico que equilibra efectividad con proporcionalidad

---

[32] https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm
[33] https://www.hrw.org/news/2025/09/17/brazil-passes-landmark-law-to-protect-children-online
[34] https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm
[35] https://www.dataguidance.com/news/brazil-president-signs-two-decrees-regulating-digital
[36] https://www.dataguidance.com/news/brazil-president-signs-two-decrees-regulating-digital
[37] https://lgpd-brazil.info/
[38] https://www.gov.br/anpd/pt-br
[39] https://iapp.org/news/a/anpd-becomes-regulatory-agency-a-turning-point-for-brazilian-data-protection-compliance
[40] https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2025/09/lula-sanciona-lei-que-protege-criancas-na-internet-e-anuncia-medidas-para-ampliar-concorrencia-e-infraestrutura-digital

y preservación de la privacidad, alentando métodos basados en riesgos y desincentivando la recolección excesiva de datos. En el plano de ciberseguridad, la Estrategia Nacional de Ciberseguridad de Brasil (E-Ciber 2025) refuerza la protección de poblaciones vulnerables, incluidas niñas, niños y adolescentes, mediante la promoción de infraestructura digital segura, capacidad de respuesta a incidentes y coordinación entre actores públicos y privados.[41] [42] Finalmente, la implementación cuenta en la práctica con el apoyo de alianzas de la sociedad civil como SaferNet Brasil, que proporciona canales ampliamente utilizados de denuncia, líneas de ayuda y recursos educativos, ilustrando cómo Brasil combina mandatos legales con mecanismos operativos para denuncia, apoyo a víctimas y alfabetización digital.[43] En conjunto, estos elementos reflejan una postura en capas que integra política pública, salvaguardas técnicas y coordinación institucional para abordar riesgos para niñas, niños y adolescentes en entornos digitales.

Chile

El enfoque de Chile hacia la protección infantil en línea está determinado por un marco maduro de ciberseguridad junto con una transición significativa en su régimen de protección de datos. La Política Nacional de Ciberseguridad 2023–2028, liderada por la Agencia Nacional de Ciberseguridad (ANCI), establece una estrategia coordinada y basada en riesgos centrada en la protección de infraestructura crítica, respuesta a incidentes y colaboración intersectorial.[44] Operativamente, el CSIRT nacional proporciona respuesta a incidentes a nivel nacional, monitoreo de amenazas y orientación pública, formando la columna vertebral técnica para gestionar riesgos digitales, incluidos aquellos que afectan a menores. Aunque estos instrumentos no son específicos para la niñez, contribuyen a un entorno digital seguro que sustenta una seguridad en línea más amplia.[45]

El marco de protección de datos de Chile está actualmente regido por la Ley No. 19.628, que proporciona una base general para el tratamiento de datos personales pero ofrece disposiciones limitadas específicas para la niñez.[46]

---

[41] https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber
[42] https://depp.oecd.org/policies/BRA2214
[43] https://new.safernet.org.br/denuncie
[44] https://anci.gob.cl/pncs-2023-2028/
[45] https://csirt.gob.cl/
[46] https://www.bcn.cl/leychile/navegar?idNorma=141599

Esto cambiará con la Ley No. 21.719, que entrará en vigor en diciembre de 2026 y establece un régimen modernizado de protección de datos, además de crear una autoridad supervisora dedicada.[47] Se espera que la nueva ley fortalezca salvaguardas, rendición de cuentas y supervisión, con implicaciones más claras para los datos de niñas, niños y adolescentes y los servicios digitales.[48] En el ámbito social y de política pública, iniciativas como Kids Online Chile 2022 y el programa de Ciudadanía Digital del Ministerio de Educación visibilizan los riesgos que enfrentan niñas, niños y adolescentes en línea y promueven alfabetización digital, uso responsable y conciencia entre estudiantes, educadores y familias.[49] [50]

En general, la postura de Chile combina instituciones sólidas de ciberseguridad con un marco de protección de datos en evolución e iniciativas de seguridad infantil centradas en la educación. Su modelo enfatiza la capacidad institucional y el desarrollo de políticas públicas, y es probable que la próxima reforma de protección de datos desempeñe un papel clave en el avance de una gobernanza digital más robusta y sensible a la niñez.

México

El enfoque de México hacia la protección infantil en línea refleja una convergencia creciente entre planificación de ciberseguridad, gobernanza de telecomunicaciones y política de derechos de la niñez. A nivel estratégico, el Plan Nacional de Ciberseguridad 2025–2030[51], apoyado por la Agencia de Transformación Digital y Telecomunicaciones (ATDT)[52], enmarca la ciberseguridad como una cuestión de resiliencia nacional y seguridad pública, con relevancia implícita para la protección de poblaciones vulnerables, incluidos menores.[53] Operativamente, CERT-MX proporciona capacidades de respuesta a incidentes, monitoreo de amenazas y coordinación entre sectores público y privado, formando la columna vertebral de la infraestructura técnica de ciberseguridad de México. Aunque estos instrumentos no son específicos para la niñez, contribuyen a un entorno más amplio de mitigación de riesgos digitales que sustenta la seguridad en línea.[54]

---

47 https://www.bcn.cl/leychile/navegar?i=1209272
48 https://resguard-solutions.com/blog/es/chile-data-protection-law-21719–guide/
49 https://www.unicef.org/chile/informes/kids-online-chile-2022
50 https://ciudadaniadigital.mineduc.cl/
51 https://mexicobusiness.news/cybersecurity/news/mexico-unveils-national-cybersecurity-plan-2025–2030
52 https://www.gob.mx/atdt/
53 https://www.gob.mx/atdt/comunicacion/liderara-mexico-ciberresiliencia-en-la-region-con-plan-nacional-de-ciberseguridad
54 https://www.gob.mx/gncertmx

Las protecciones enfocadas en niñas, niños y adolescentes se desarrollan de manera más explícita mediante canales institucionales y de política pública. SIPINNA (Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes) lidera los esfuerzos federales en seguridad infantil en línea, emitiendo orientación sobre uso seguro de internet, alfabetización digital y prevención de riesgos, a menudo en colaboración con socios internacionales como UNICEF México, que enfatiza un enfoque educativo y basado en derechos.[55] En paralelo, el marco de telecomunicaciones de México desempeña un papel en la configuración de responsabilidades a nivel de plataforma y red, particularmente en torno a acceso, contenido y protecciones para usuarios.[56] La protección de datos se rige por leyes federales aplicables tanto al sector público como privado, que establecen principios como consentimiento, limitación de finalidad y salvaguardas de seguridad, incluidas consideraciones reforzadas para los datos de menores.

En general, la postura de México combina infraestructura de ciberseguridad, regulación de telecomunicaciones y política de derechos de la niñez, pero sigue siendo menos centralizada y prescriptiva que la de otros países. Su fortaleza radica en la coordinación institucional y los esfuerzos de educación pública, mientras que su estructura de gobernanza de datos en evolución y su dependencia de herramientas generales de ciberseguridad resaltan desafíos persistentes para desarrollar un régimen cohesivo de seguridad digital específico para la niñez.

Perú

El enfoque de Perú hacia la protección infantil en línea se apoya en un marco legal dedicado que aborda específicamente el uso seguro y responsable de las TIC por niñas, niños y adolescentes, complementado por la legislación general de protección de datos y estructuras nacionales de ciberseguridad. La Ley No. 30254, modificada por la Ley No. 31664 e implementada mediante el Decreto Supremo No. 093–2019–PCM, establece obligaciones para promover entornos digitales seguros, prevenir riesgos en línea como el grooming y la explotación, y fomentar la coordinación entre gobierno, sector privado y sociedad civil.[57] El marco pone especial énfasis en la concientización, la educación y la responsabilidad compartida, más que en imponer obligaciones

[55] https://www.gob.mx/sipinna/articulos/ciberseguridad-para-ninas-ninos-y-adolescentes-en-el-ecosistema-digital
[56] https://www.gob.mx/crt/es/que-hacemos
[57] https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/292146–30254

directas extensas a las plataformas digitales, y se operacionaliza mediante políticas nacionales e iniciativas interinstitucionales.

El régimen de protección de datos de Perú, bajo la Ley No. 29733, proporciona la base para la privacidad y la gobernanza de datos personales, incluidos principios como consentimiento, limitación de finalidad y salvaguardas de seguridad aplicables a los datos de menores.[58] Aunque no es específico para la niñez, apoya los esfuerzos más amplios de seguridad en línea al regular cómo se recopilan y procesan los datos personales.
En materia de ciberseguridad, el Centro Nacional de Seguridad Digital y funciones relacionadas de CSIRT proporcionan coordinación nacional para respuesta a incidentes, monitoreo de riesgos y política de seguridad digital, contribuyendo a un ecosistema digital más seguro en general.
La protección enfocada en niñas, niños y adolescentes se refuerza mediante esfuerzos gubernamentales de educación pública y coordinación, incluida orientación oficial para familias sobre uso seguro de internet e iniciativas como la Alianza Nacional por una Internet Segura, que reúne a instituciones públicas y actores privados para promover conciencia y prácticas preventivas.[59] En general, la postura de Perú enfatiza educación, coordinación interinstitucional y protecciones legales específicas para menores, respaldadas por marcos generales de privacidad y ciberseguridad, pero con un énfasis comparativamente menor en obligaciones vinculantes a nivel de plataformas.

Uruguay

El enfoque de Uruguay hacia la protección infantil en línea se basa en un marco sólido de protección de datos, apoyado por una gobernanza coordinada de ciberseguridad y un énfasis notable en alfabetización digital y prevención. La Ley No. 18.331 de Protección de Datos Personales establece el régimen legal central, incorporando principios como consentimiento, limitación de finalidad y seguridad de datos, y es supervisada por la autoridad de protección de datos (URCDP), que proporciona supervisión institucional y orientación.[60] [61] Aunque la ley no es exclusivamente específica para la niñez, se aplica a los datos de menores y se complementa con interacción regulatoria y orientación pública que refuerzan las protecciones de privacidad en entornos digitales.

---

[58] https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733
[59] https://www.gob.pe/20720-seguridad-digital-para-ninos-ninas-y-adolescentes
[60] https://www.impo.com.uy/bases/leyes/18331-2008
[61] https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/uruguayan-law-protection-personal-data-and-habeas-data-action-ldpd-2024-09-25_en

En el plano de ciberseguridad, Uruguay ha desarrollado una estructura coherente de gobernanza liderada por Agesic, que coordina la estrategia nacional de ciberseguridad, la gestión de riesgos y la colaboración interinstitucional.[62] Operativamente, CERTuy actúa como el equipo nacional de respuesta a incidentes, ofreciendo monitoreo de amenazas, canales de denuncia y procedimientos de respuesta accesibles tanto para instituciones como para el público.[63] Sus reglas y procesos definidos de reporte de incidentes contribuyen a un enfoque estructurado y transparente para manejar amenazas digitales, incluidas aquellas que pueden afectar a niñas, niños y adolescentes.

La protección enfocada en niñas, niños y adolescentes es particularmente visible en las políticas de prevención de Uruguay. La estrategia de ciudadanía digital de Ceibal integra seguridad en línea, uso responsable de tecnología y habilidades digitales en el sistema educativo, dirigida a estudiantes, docentes y familias.[64] Esto se refuerza con evidencia empírica de Kids Online Uruguay 2022, que documenta comportamientos, riesgos y estrategias de afrontamiento de niñas, niños y adolescentes en línea, informando políticas e intervenciones educativas basadas en evidencia.[65] En general, la postura de Uruguay refleja un modelo equilibrado que combina protección de datos, capacidad institucional de ciberseguridad y fuertes esfuerzos preventivos impulsados por la educación, con una fortaleza particular en integrar la seguridad infantil en línea en su agenda nacional de inclusión digital y educación.

Conclusión regional

En conjunto, estos ejemplos nacionales muestran tanto avances significativos como oportunidades de mejora en toda la región. Si bien existe una clara alineación con principios globales, particularmente en torno a la gobernanza basada en derechos, la prevención y la coordinación institucional, las vías de implementación difieren según tradiciones legales, capacidad institucional y prioridades de política pública. Esta diversidad no es exclusiva de América Latina; países de otras regiones también están experimentando con diferentes combinaciones regulatorias, arreglos institucionales y enfoques técnicos para la protección infantil en línea. No ha surgido un único modelo definitivamente "correcto", y los

[62] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/
[63] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/tramites-y-servicios/servicios/certuy
[64] https://ceibal.edu.uy/institucional/articulos/lanzamiento-nueva-estrategia-nacional-de-ciudadania-digital-2024-2028/
[65] https://www.unicef.org/uruguay/informes/informe-kids-online-uruguay-2022

intentos de imponer una solución uniforme corren el riesgo de ignorar los factores contextuales que determinan tanto los riesgos como las intervenciones viables.

En consecuencia, el camino más efectivo no radica en converger hacia un único modelo, sino en una armonización cuidadosa. Los enfoques nacionales deben continuar tomando como referencia marcos internacionales y estándares compartidos, garantizando interoperabilidad, cooperación transfronteriza y protecciones básicas para niñas, niños y adolescentes en un entorno digital inherentemente global. Al mismo tiempo, estos enfoques deben seguir siendo adaptables a los contextos locales, reflejando sistemas legales nacionales, consideraciones culturales y realidades de recursos. Equilibrar la alineación global con la relevancia contextual será fundamental para construir regímenes de protección infantil en línea resilientes, coherentes y efectivos tanto dentro de América Latina como en el marco de un panorama internacional más amplio y en evolución.

Soluciones prácticas de política pública, técnicas y de gobernanza para la armonización regional

Avanzar la protección infantil en línea en América Latina requiere pasar de la alineación de alto nivel en torno a principios hacia mecanismos prácticos que permitan coordinación, interoperabilidad y rendición de cuentas compartida. Sobre la base de los marcos internacionales existentes y los diversos enfoques nacionales descritos anteriormente, esta sección propone soluciones accionables y adaptables a nivel regional. Estas recomendaciones están diseñadas de forma modular, permitiendo que los países adopten elementos comunes mientras los adaptan a sus sistemas jurídicos, capacidades institucionales y entornos de riesgo nacionales.

Armonización legal y regulatoria

Un paso fundamental hacia la coherencia regional es el desarrollo de un marco modelo de COP o ley de referencia que establezca

estándares mínimos centrales. En lugar de prescribir legislación idéntica, este modelo debería definir elementos básicos clave: definiciones armonizadas (incluidos "niña, niño", "adolescente" y edad de consentimiento digital), salvaguardas mínimas de protección de datos para menores, obligaciones de denuncia obligatoria para daños graves en línea (como explotación sexual infantil y grooming), y disposiciones de puertos seguros para plataformas condicionadas al cumplimiento de requisitos de debido proceso y transparencia. La elaboración debería alinearse con orientaciones internacionales establecidas, incluidos los marcos de la UIT y UNICEF, así como con principios ampliamente aceptados de privacidad y derechos humanos.

Es fundamental alentar a los países a adoptar principios interoperables en lugar de lenguaje estatutario idéntico. Este enfoque permite compatibilidad legal entre fronteras, facilitando la cooperación y la aplicación, al tiempo que preserva la flexibilidad para la adaptación nacional. Organismos o foros regionales pueden apoyar este proceso mediante la emisión de orientación interpretativa, cláusulas modelo y actualizaciones periódicas que reflejen riesgos y tecnologías en evolución.

Interoperabilidad técnica y estándares

La alineación legal debe complementarse con interoperabilidad técnica para garantizar que los sistemas diseñados para detectar, denunciar y responder a daños puedan funcionar sin fricciones entre jurisdicciones. Un área prioritaria es el desarrollo de un estándar regional de denuncia: un esquema de datos compartido para documentar incidentes como explotación sexual infantil, grooming y otros daños de alto riesgo. Esto permitiría reportes consistentes por parte de plataformas, recepción más fluida por autoridades y un manejo más eficiente de casos transfronterizos. Junto con ello, protocolos seguros para el intercambio de evidencia (que incorporen cifrado, salvaguardas de cadena de custodia y protecciones de privacidad) son esenciales para investigaciones transfronterizas oportunas y legales.
En paralelo, América Latina se beneficiaría de estándares técnicos comunes para diseño apropiado para la edad y verificación de la edad que preserve la privacidad. En lugar de depender de métodos de verificación intrusivos o inconsistentes, los países pueden promover enfoques basados en minimización de datos, como pruebas criptográficas o atestaciones de atributos mínimos que confirmen rangos de edad sin exponer la identidad completa. Expectativas estandarizadas de transparencia de plataformas,

respaldadas por API compartidas o herramientas de reporte, pueden fortalecer aún más la rendición de cuentas, permitiendo que reguladores e investigadores accedan a datos comparables sobre moderación de contenidos, reportes de abuso y resultados de mitigación de riesgos.

Aplicación y cooperación transfronteriza

Dada la naturaleza inherentemente transnacional de los daños en línea, fortalecer los mecanismos de aplicación transfronteriza es fundamental. El desarrollo de plantillas estandarizadas de Asistencia Jurídica Mutua (MLA, por sus siglas en inglés) adaptadas a casos de COP puede reducir significativamente demoras y fricciones procedimentales. Estas deberían incluir canales expeditos para asuntos urgentes de seguridad infantil, con plazos claros y vías de escalamiento. Establecer puntos focales designados de COP dentro de agencias de aplicación de la ley, autoridades de protección de datos y redes judiciales puede agilizar aún más la comunicación y coordinación.

Fortalecimiento de capacidades y servicios compartidos

Las disparidades en capacidad institucional siguen siendo una barrera significativa para una implementación efectiva. Abordarlas requiere inversión sostenida en iniciativas regionales de fortalecimiento de capacidades. Podría desarrollarse un currículo de capacitación estandarizado que cubra aspectos legales, técnicos y operativos de la COP para fiscales, jueces, fuerzas de seguridad, equipos CERT y organizaciones de protección infantil. Su entrega mediante centros regionales de capacitación o plataformas en línea garantizaría escalabilidad y accesibilidad.

Los servicios compartidos ofrecen una forma eficiente de ampliar capacidades a países con menos recursos. Laboratorios técnicos regionales podrían proporcionar análisis forense avanzado, procesamiento de evidencia digital y servicios de apoyo a víctimas.

Gobernanza multisectorial y rendición de cuentas

Los marcos efectivos de COP dependen de estructuras de gobernanza inclusivas que reúnan a reguladores, industria, sociedad civil y defensores de los derechos de la niñez. Los países deberían considerar establecer órganos de supervisión multisectoriales tanto a nivel nacional como regional, encargados de monitorear el cumplimiento de plataformas, revisar la efectividad de las políticas y asesorar sobre riesgos

emergentes. Estos órganos pueden mejorar la transparencia, construir confianza pública y garantizar que diversas perspectivas se reflejen en la toma de decisiones.

A nivel regional, estos mecanismos pueden facilitar el aprendizaje entre pares y la comparación de avances, permitiendo que los países comparen progreso, identifiquen brechas y coordinen respuestas. Los procesos de reporte periódico y rendición pública de cuentas deben integrarse en estas estructuras para mantener impulso y credibilidad.

Salvaguardas de privacidad y consideraciones de derechos humanos

Finalmente, todos los esfuerzos de armonización deben basarse en salvaguardas sólidas para proteger los derechos fundamentales. Deben requerirse evaluaciones de impacto en derechos humanos (EIDH) obligatorias para intervenciones relacionadas con COP, particularmente aquellas que involucren tecnologías sensibles como verificación de edad, filtrado de contenido o herramientas de vigilancia. Estas evaluaciones deben analizar proporcionalidad, necesidad y posibles consecuencias no deseadas, garantizando que las medidas diseñadas para proteger a niñas, niños y adolescentes no socaven derechos más amplios a la privacidad, la expresión y el acceso a la información.

Igualmente importante es incluir las voces de niñas, niños y adolescentes en el diseño y la evaluación de políticas. Mecanismos de participación significativa, como paneles asesores juveniles, consultas e investigaciones participativas, pueden aportar información valiosa sobre experiencias vividas y riesgos emergentes. Incorporar estas perspectivas no solo fortalece la relevancia de las políticas, sino que también refuerza la base de derechos de los esfuerzos de COP.

Conclusión

La protección infantil en línea ya no es un tema periférico de política digital; es un componente central de la gobernanza digital, la ciberseguridad, los derechos de la niñez y el desarrollo inclusivo. A medida que niñas, niños y adolescentes en América Latina pasan una mayor parte de sus vidas en línea, la región enfrenta una doble responsabilidad: expandir la conectividad significativa y, al mismo tiempo, garantizar que los entornos digitales sean seguros, protegidos, respetuosos de los derechos y apropiados para la edad. El desafío no consiste simplemente en reducir el daño después de que ocurre, sino en construir sistemas que prevengan el abuso, protejan la privacidad, fortalezcan la resiliencia y permitan que niñas, niños y adolescentes participen plenamente en el mundo digital.

Este documento muestra que los países de América Latina no parten de cero. En toda la región, los gobiernos han desarrollado leyes de protección de datos, estrategias de ciberseguridad, iniciativas de educación pública, mecanismos de denuncia y marcos emergentes de responsabilidad de plataformas. Los modelos internacionales y marcos globales también ofrecen una base sólida. Sin embargo, el progreso sigue siendo desigual, y los enfoques fragmentados limitan la efectividad de los esfuerzos nacionales frente a riesgos inherentemente transfronterizos. La región necesita pasar ahora de iniciativas aisladas hacia una armonización práctica, principios compartidos, estándares interoperables, aplicación coordinada, instituciones más sólidas y fortalecimiento sostenido de capacidades. Esto incluye avanzar marcos legales interoperables basados en principios comunes, desarrollar estándares técnicos regionales para denuncia e intercambio de evidencia, promover enfoques de verificación de la edad que preserven la privacidad, fortalecer mecanismos de cooperación transfronteriza, invertir en servicios regionales compartidos y capacitación, y establecer estructuras de gobernanza multisectorial que apoyen la transparencia y la rendición de cuentas.

No existe un único modelo “correcto” de protección infantil en línea. Cada país debe adaptar soluciones a su sistema jurídico, capacidad institucional, cultura y ecosistema digital. Pero la flexibilidad nacional no debe traducirse en fragmentación regional. Un enfoque más coherente, basado en estándares internacionales de derechos humanos, salvaguardas de privacidad, buenas prácticas de ciberseguridad y participación significativa de niñas, niños y adolescentes, puede ayudar a los países a protegerlos y, al mismo tiempo, preservar la apertura, la innovación y el acceso a la información. Por lo tanto, los esfuerzos de armonización

regional deberían priorizar principios interoperables en lugar de leyes idénticas, permitiendo que los países se alineen en torno a objetivos compartidos mientras mantienen flexibilidad nacional. Al mismo tiempo, salvaguardas como las evaluaciones de impacto en derechos humanos y los mecanismos participativos que incorporen las voces de niñas, niños y adolescentes deben seguir siendo centrales en el desarrollo e implementación de políticas.

Los gobiernos deben modernizar los marcos legales y fortalecer la capacidad de aplicación. La industria debe incorporar seguridad desde el diseño y privacidad desde el diseño en productos y servicios utilizados por niñas, niños y adolescentes. Las plataformas también deben apoyar informes de transparencia estandarizados e implementar medidas de diseño apropiado para la edad que minimicen la recolección innecesaria de datos y protejan la privacidad infantil. La sociedad civil, los educadores, las familias y las organizaciones de protección infantil deben recibir recursos como socios esenciales, en lugar de quedar solos frente a la gestión de riesgos. Las instituciones y socios regionales deben apoyar herramientas compartidas, capacitación, intercambio de evidencia y estándares técnicos que hagan la cooperación más rápida y efectiva.

Proteger a niñas, niños y adolescentes en línea no es un proyecto regulatorio único; es un compromiso continuo de gobernanza. El entorno digital seguirá evolucionando, y también lo harán los riesgos. América Latina tiene la oportunidad de construir un enfoque regional práctico, interoperable y respetuoso de los derechos: uno que proteja a niñas, niños y adolescentes frente a daños mientras los empodera para beneficiarse de las oportunidades de la era digital. Al combinar interoperabilidad legal, coordinación técnica, cooperación transfronteriza, gobernanza inclusiva y sólidas salvaguardas de privacidad y derechos humanos, la región puede avanzar hacia un modelo más efectivo y sostenible de protección infantil en línea que refleje tanto las realidades regionales como las buenas prácticas globales.


DIGI
AMERICAS