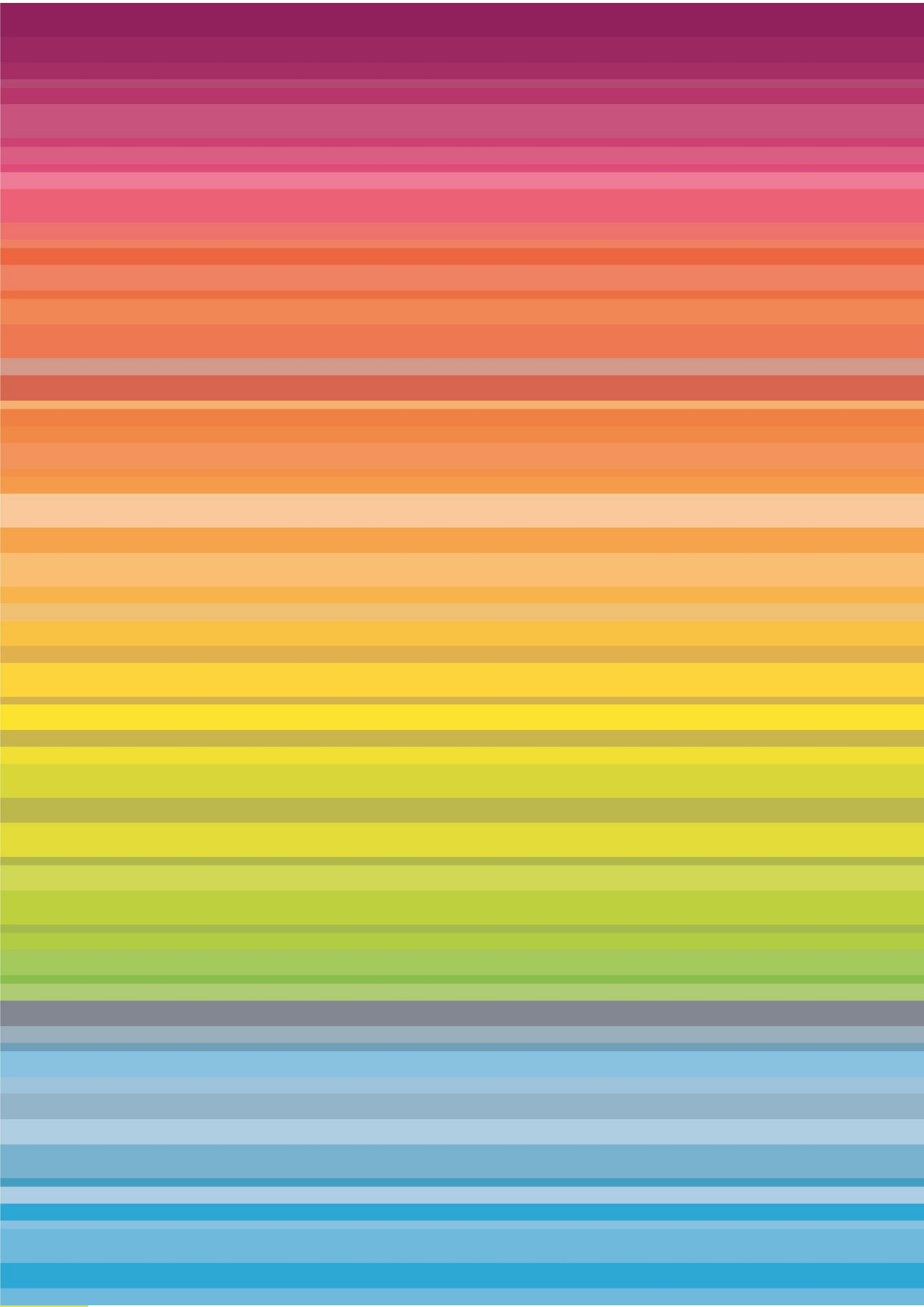




## RESUMEN EJECUTIVO

Responsabilidad del Estado y las empresas como  
garantes de los derechos humanos de niños, niñas y  
adolescentes en el entorno digital

2026





## **COORDINACIÓN, EDICIÓN GENERAL Y DISEÑO**

Defensoría de la Niñez

## **EJECUTADO POR CONSULTORES**

Pablo Carvacho T. (Coordinador general)

Paloma Del Villar T. (Investigadora)

Alejandra Parra N. (Investigadora)

Lorena Rivera A. (Investigadora)

## **FORMA DE CITAR**

Defensoría de la Niñez (2026). Resumen ejecutivo estudio “Responsabilidad del Estado y las empresas como garantes de los derechos humanos de niños, niñas y adolescentes en el entorno digital”.

“Esta publicación es de uso público y sus contenidos pueden ser reproducidos total o parcialmente con la correspondiente cita”

# 1. CONTEXTO Y PROPÓSITO DEL INFORME

El entorno digital se ha convertido en uno de los espacios más relevantes para el desarrollo, la participación y el ejercicio de derechos de niños, niñas y adolescentes (NNA). Las tecnologías digitales atraviesan hoy múltiples dimensiones de su vida cotidiana: educación, recreación, interacción social, acceso a información, consumo y participación cívica, generando nuevas oportunidades para el ejercicio de sus derechos.

Sin embargo, la creciente centralidad de estos entornos también ha intensificado riesgos y vulnerabilidades, tales como la exposición a contenidos dañinos, el ciberacoso, la explotación sexual en línea, la manipulación comercial y el uso extensivo de datos personales. En este escenario, la garantía efectiva de los derechos de NNA exige avanzar hacia marcos regulatorios y de gobernanza capaces de abordar de manera integral los desafíos que plantea el ecosistema digital contemporáneo.

El presente informe fue encargado por la Defensoría de la Niñez con el objetivo de producir un diagnóstico actualizado sobre los riesgos digitales que afectan a NNA en Chile, analizar el marco normativo nacional e internacional aplicable, y proponer lineamientos éticos, normativos y de política pública para avanzar hacia una protección efectiva de sus derechos en el entorno digital. Para ello, el estudio combina una revisión sistemática de la evidencia disponible para Chile, un análisis de derecho comparado de jurisdicciones seleccionadas, y un proceso de participación con NNA realizado a través de encuestas, focus groups y entrevistas.

El informe se estructura en siete capítulos: (1) Introducción; (2) Marco teórico; (3) Evidencia disponible para Chile; (4) Tendencias regulatorias comparadas; (5) Marco normativo chileno; (6) Políticas y programas en Chile; y (7) Propuesta de lineamientos. Este documento sintetiza los hallazgos más relevantes de cada uno de esos apartados.

## 2. DIAGNÓSTICO: RIESGOS EN EL ENTORNO DIGITAL

### 2.1 Marco analítico: el modelo de las 4 C

El informe organiza los riesgos a los que están expuestos NNA en el entorno digital a través del modelo internacionalmente reconocido de las '4 C': riesgos de Contenido, de Contacto, de Conducta y de Consumidor. Este marco permite identificar de manera sistemática las distintas formas en que el entorno digital puede afectar los derechos y el bienestar de NNA, así como orientar las respuestas normativas y de política pública de manera diferenciada.

### 2.2 Riesgos de Contenido

Los riesgos de contenido refieren a la exposición de NNA a información o material potencialmente dañino disponible en línea. En Chile, la evidencia disponible — proveniente de estudios como Kids Online Chile (2022) y la Radiografía Digital de Niñas y Niños (2025) — muestra que una proporción significativa de NNA se expone a contenidos inapropiados, discriminatorios u ofensivos en internet.

Según Kids Online (2022), un porcentaje relevante de estudiantes de 15 años reportó haberse sentido molesto por encontrar contenido inapropiado para su edad en línea, cifras que se elevan considerablemente cuando se trata de contenido discriminatorio o mensajes ofensivos. La exposición es mayor entre adolescentes de mayor edad, con diferencias significativas según género y nivel socioeconómico, lo que subraya el carácter inequitativo del riesgo digital. La Radiografía Digital (2025) confirma estas tendencias y añade datos sobre exposición a contenidos violentos, pornográficos y de autolesión.

De acuerdo con datos de PISA (2022), Chile se ubica entre los países con mayor proporción de estudiantes de 15 años que declaran compartir información inventada en redes sociales sin advertir que es inexacta, lo que revela también importantes déficits de pensamiento crítico frente a la desinformación en el entorno digital.

### 2.3 Riesgos de Contacto

Los riesgos de contacto comprenden las interacciones de NNA con personas externas a través del entorno digital, incluyendo pares y adultos desconocidos. El informe identifica tres modalidades principales:

- **Ciberacoso y violencia digital:** la evidencia muestra altos niveles de victimización en NNA chilenos. Los datos del estudio Kids Online y de la Radiografía Digital revelan que una parte significativa de los y las estudiantes ha experimentado mensajes ofensivos, exclusión deliberada o acoso a través de dispositivos digitales, con mayor prevalencia entre niñas y adolescentes de menor nivel socioeconómico.
- **Acoso sexual o grooming:** la exposición a este tipo de riesgo — que involucra el contacto de adultos con fines de manipulación o explotación sexual — constituye uno de los riesgos más severos identificados. La evidencia disponible para Chile es limitada, pero los datos existentes sugieren que no es un fenómeno marginal, particularmente entre niñas adolescentes.

- Contacto con desconocidos: según la Radiografía Digital (2025), un porcentaje notable de NNA ha establecido contacto en línea con personas que no conocía previamente, lo que representa un factor de riesgo de exposición a distintas formas de daño, incluyendo la manipulación emocional y el abuso sexual.

## 2.4 Riesgos de Conducta

Los riesgos de conducta refieren a comportamientos que los propios NNA pueden desarrollar en el entorno digital y que afectan su bienestar o el de terceros. Entre los principales riesgos identificados destacan:

- Ciberacoso activo: los datos muestran que una proporción de NNA no solo son víctimas de ciberacoso, sino que también ejercen conductas de acoso hacia pares, lo que revela la necesidad de abordar esta problemática desde una perspectiva de prevención integral y no solo de protección de víctimas.
- Difusión de contenidos falsos: como se señaló, los datos PISA evidencian niveles preocupantes de participación de adolescentes chilenos en la difusión de desinformación, asociados a déficits en habilidades de verificación y pensamiento crítico digital.
- Uso problemático del tiempo: el uso excesivo de dispositivos digitales, especialmente en contextos escolares, constituye un riesgo relevante. Los hallazgos cualitativos revelan que los propios NNA perciben el uso no regulado de celulares en clases como una interferencia con el aprendizaje y las relaciones presenciales.
- Presión social y validación digital: los focus groups evidenciaron que NNA experimentan presiones importantes vinculadas a la búsqueda de likes, comparaciones de imagen y dinámicas de validación social en plataformas digitales, con impactos en su bienestar socioemocional.

## 2.5 Riesgos del Consumidor

Los riesgos del consumidor o de 'contrato' refieren a las formas en que NNA pueden ser objeto de prácticas comerciales abusivas, manipulación algorítmica o explotación de sus datos personales. En Chile, la evidencia muestra brechas relevantes en la capacidad de NNA para proteger su privacidad digital: la proporción de estudiantes que declara poder modificar configuraciones de privacidad varía significativamente según nivel socioeconómico, lo que revela que la vulnerabilidad digital no es neutra desde el punto de vista de la equidad.

El uso de técnicas de diseño persuasivo — como el scroll infinito, sistemas de notificaciones, gamificación o mecanismos de recompensa — ha sido identificado tanto en la literatura internacional como en los hallazgos cualitativos del estudio como un factor que favorece el uso intensivo y difícil de regular de plataformas digitales, especialmente por parte de niñas, niños y adolescentes.

## 3. MARCO NORMATIVO COMPARADO

### 3.1 Tendencias regulatorias internacionales

A nivel internacional se observa una convergencia creciente hacia enfoques regulatorios que reconocen que la protección de la infancia en entornos digitales requiere no solo la acción del Estado, sino también la participación activa de los actores privados que diseñan, operan y gobiernan las infraestructuras digitales. Existe un consenso transversal centrado en cuatro pilares: privacidad y protección de datos, seguridad por diseño, diseño apropiado para la edad, y evaluación de riesgos de productos y funcionalidades.

La tendencia más reciente, propiciada especialmente por la Unión Europea, se orienta hacia la denominada 'seguridad por diseño' (safety by design), en virtud de la cual las plataformas deben incorporar mecanismos de protección desde la etapa de diseño de sus productos y servicios, y no solo como respuesta reactiva a daños ya producidos. Este enfoque es más adaptable a la velocidad de cambio tecnológico y evita que la regulación quede permanentemente desfasada respecto de las prácticas del mercado.

### 3.2 Modelos regulatorios por jurisdicción

El informe examina los marcos regulatorios de cinco jurisdicciones, concluyendo que existen modelos diversos que pueden orientar el diseño de una propuesta para Chile:

- Australia: modelo proactivo y administrativo, centrado en un código de prácticas en línea (Online Safety Act) con atribuciones amplias de la Comisionada de Seguridad en Línea, que puede exigir a plataformas la eliminación de contenidos dañinos y la implementación de medidas preventivas.
- Unión Europea: la Ley de Servicios Digitales (Digital Services Act, DSA) establece obligaciones de debida diligencia para plataformas muy grandes, incluyendo evaluaciones de riesgo sistemático, transparencia algorítmica y prohibición de publicidad dirigida a menores basada en perfilamiento.
- Reino Unido: el Children's Code (Age Appropriate Design Code) introduce el principio de 'interés superior del niño' como criterio rector del diseño de servicios digitales, exigiendo configuraciones de privacidad por defecto, limitación de recolección de datos y diseño apropiado para la edad.
- Brasil: el Estatuto da Criança e do Adolescente Digital establece un marco integral de protección, combinando obligaciones estatales, participación de la sociedad civil y mecanismos de responsabilidad empresarial.
- Estados Unidos: modelo más sectorial y reactivo, con protecciones específicas para menores de 13 años a través del COPPA (Children's Online Privacy Protection Act), aunque con debates legislativos en curso para ampliar y actualizar este marco.

## 4. MARCO NORMATIVO CHILENO Y SUS BRECHAS

### 4.1 Normas vigentes

Chile cuenta con un conjunto de normas relevantes para la protección de NNA en el entorno digital, que incluye:

- Ley N°21.430 sobre Garantías y Protección Integral de los Derechos de la Niñez y la Adolescencia (2022): establece un marco general de protección de derechos, con referencias al entorno digital y al derecho a la privacidad e identidad digital.
- Ley N°21.719 de Protección de Datos Personales (2024): introduce protecciones reforzadas para datos de menores de edad, incluyendo restricciones al tratamiento sin consentimiento parental y condiciones para el uso de datos de NNA.
- Ley N°20.536 sobre Violencia Escolar: establece obligaciones para establecimientos educacionales en materia de prevención del acoso, incluyendo el ciberacoso entre pares en contextos escolares.
- Código Penal: contempla sanciones por explotación sexual infantil, pornografía infantil y delitos informáticos vinculados a NNA.
- Proyecto de Ley de Inteligencia Artificial (Boletín N°16821-19): en tramitación legislativa, con disposiciones relevantes sobre sistemas algorítmicos de alto riesgo e impacto en grupos vulnerables.

### 4.2 Vacíos y brechas normativas

No obstante, lo anterior, el informe identifica vacíos significativos en el ordenamiento jurídico chileno:

- Ausencia de regulación integral sobre seguridad digital para NNA: a diferencia de Australia, la UE o el Reino Unido, Chile carece de una ley general que establezca obligaciones específicas de protección de NNA en el entorno digital.
- Sin obligaciones proactivas para plataformas: no existen normas que exijan a las plataformas digitales realizar evaluaciones de riesgo, implementar salvaguardas por diseño o reportar situaciones de vulneración de derechos de NNA.
- Vacío en diseño persuasivo y adictivo: no hay regulación sobre prácticas de diseño que explotan la vulnerabilidad de NNA, como el scroll infinito, notificaciones compulsivas o sistemas de recompensa.
- Sin estándares de verificación de edad: Chile carece de un marco que regule cómo las plataformas deben verificar la edad de sus usuarios y adaptar sus servicios en consecuencia.
- Publicidad digital sin regulación específica para NNA: no existen normas sobre publicidad dirigida a menores a través de plataformas digitales, incluida la publicidad encubierta a través de influencers.
- Fragmentación institucional: no existe una institucionalidad especializada con competencias claras para supervisar el cumplimiento de las obligaciones de las plataformas digitales en relación con NNA.

Los proyectos de ley de debida diligencia en derechos humanos actualmente en tramitación representan una oportunidad relevante para cerrar algunas de estas brechas, al introducir obligaciones para que las empresas — incluidas las tecnológicas — identifiquen, evalúen y mitiguen los impactos negativos de sus actividades sobre los derechos humanos, con especial atención a los grupos en situación de mayor vulnerabilidad.

## 5. POLÍTICAS Y PROGRAMAS EN CHILE

Chile ha desarrollado un conjunto de políticas y programas vinculados a NNA y al entorno digital, aunque estos presentan importantes limitaciones en términos de articulación sistémica y cobertura. El panorama actual puede organizarse en torno a tres grandes categorías:

### 5.1 Programas de acceso digital

Iniciativas como el Programa Enlaces del MINEDUC (desde 1992), Biblioredes y los programas de inclusión digital impulsados por el Ministerio de Desarrollo Social y Familia han sido históricamente orientados a reducir brechas de acceso y promover la alfabetización digital básica. Si bien representan avances importantes, en su mayoría no incorporan una perspectiva específica de protección de derechos en entornos digitales ni abordan los riesgos emergentes a los que están expuestos NNA.

### 5.2 Programas de prevención general

Chile cuenta con un conjunto de programas de prevención de vulneraciones de derechos que, si bien no están orientados específicamente al entorno digital, tienen puntos de contacto relevantes con esta problemática. Entre ellos destacan el Programa de Apoyo a la Salud Mental Infantil (PASMI) del Ministerio de Salud, las Oficinas Locales de la Niñez (OLN) del Servicio Nacional de Protección Especializada, y el Sistema Alerta Niñez (SAN), que utiliza inteligencia artificial para identificar situaciones de riesgo.

### 5.3 Programas de prevención en entornos digitales

En los últimos años se observa un número creciente de iniciativas orientadas específicamente a los riesgos del entorno digital. Entre las más relevantes destacan:

- Ciudadanía Digital (MINEDUC): guías y cuadernos para estudiantes y docentes sobre seguridad, privacidad y responsabilidad digital.
- Orientaciones para la regulación del uso de celulares y dispositivos digitales (2023/2024): lineamientos para establecimientos educacionales sobre regulación del uso pedagógico y prevención de grooming, sexting y ciberacoso.
- Campaña #InfluenciaLoBueno: iniciativa de la Secretaría General de Gobierno enfocada en prevención del ciberacoso y acompañamiento a familias para un uso seguro de la tecnología.
- Guía del MINSAL para detección de ciberacoso en adolescentes: orientaciones para profesionales de salud sobre detección precoz y primera respuesta ante situaciones de violencia digital.
- Orientaciones de la Superintendencia de Educación para prevenir el ciberacoso: protocolos y roles de los equipos directivos escolares ante situaciones de violencia digital.

### 5.4 Diagnóstico general de la oferta programática

A pesar de la existencia de estas iniciativas, el informe concluye que la oferta programática chilena presenta las siguientes debilidades estructurales: dispersión y falta de articulación entre iniciativas de distintos ministerios; ausencia de una estrategia nacional que establezca objetivos comunes y mecanismos de coordinación; escasa evidencia sobre el impacto de los programas existentes; y cobertura insuficiente de grupos prioritarios, como NNA en situación de pobreza, migrantes o con discapacidad.

# 6. PROPUESTA DE LINEAMIENTOS ÉTICOS, NORMATIVOS Y DE POLÍTICA PÚBLICA

## 6.1 Enfoque regulatorio propuesto

Considerando que Chile carece de una ley general de seguridad digital para NNA, el informe propone un enfoque regulatorio gradual, flexible y basado en principios, articulado en torno a dos categorías: (i) deberes de diligencia, prevención y control basados en riesgos, exigibles tanto al sector público como al privado; y (ii) prohibiciones específicas y claras respecto de prácticas particularmente dañinas para NNA.

Este enfoque busca equilibrar la protección efectiva de los derechos con la necesidad de evitar regulaciones obsoletas o desproporcionadas. Al mismo tiempo, reconoce que el acceso equitativo al entorno digital también es un derecho, por lo que cualquier medida regulatoria debe evitar efectos excluyentes o discriminatorios. En particular, debe considerarse que en Chile el entorno digital cumple una función compensatoria de acceso a la información, la cultura y la participación, especialmente para NNA de menores recursos.

## 6.2 Lineamientos éticos

Los lineamientos éticos propuestos establecen los principios rectores que deben orientar tanto la regulación como las prácticas de las empresas digitales:

- **Principio 1:** Interés superior del niño y seguridad por diseño (safety by design): las plataformas digitales deben incorporar salvaguardas desde la etapa de diseño, considerando las características, necesidades y niveles de desarrollo de NNA. Siguiendo la experiencia del Reino Unido, esto implica configurar por defecto altos estándares de privacidad, limitar la recolección de datos y diseñar interfaces que no exploten la vulnerabilidad de los menores.
- **Principio 2:** NNA como sujetos activos de derechos: el diseño de políticas, regulaciones y servicios digitales debe incorporar la perspectiva de NNA, reconociéndolos no solo como usuarios vulnerables a proteger, sino como agentes con capacidad de diagnóstico y propuesta. Los hallazgos de los focus groups evidencian que los propios NNA identifican riesgos con claridad y formulan expectativas concretas respecto del rol de adultos, empresas y Estado.
- **Principio 3:** Corresponsabilidad entre Estado, empresas y sociedad: los riesgos digitales — como el ciberacoso, el grooming o la desinformación — tienen un carácter sistémico que no puede ser abordado únicamente a través de estrategias individuales o de autocuidado. La protección de NNA requiere una responsabilidad compartida entre el Estado (en su rol garante), las empresas (en su responsabilidad de respeto a los derechos humanos) y la sociedad en su conjunto.
- **Principio 4:** Debida diligencia en derechos humanos como estándar empresarial: las empresas deben anticipar los impactos de sus tecnologías sobre los derechos de NNA y adoptar medidas preventivas y correctivas. Este estándar, reconocido en los Principios Rectores de Naciones Unidas sobre Empresas y Derechos Humanos y en la Observación General N°25 del Comité de los Derechos del Niño, implica identificar, evaluar y gestionar

de manera continua los riesgos derivados del diseño, funcionamiento y gobernanza de los servicios digitales.

### 6.3 Lineamientos normativos

El informe identifica una brecha normativa significativa en Chile y propone avanzar en las siguientes líneas:

Ámbito	Recomendación normativa
Debida diligencia empresarial	Establecer obligaciones legales de identificación, evaluación y mitigación de riesgos sistémicos para plataformas digitales que afecten a NNA.
Diseño adictivo o persuasivo	Regular prácticas como scroll infinito, notificaciones compulsivas y mecanismos de recompensa que explotan la vulnerabilidad de NNA.
Protección de datos personales	Fortalecer restricciones al perfilamiento comercial de NNA y asegurar configuraciones de privacidad por defecto.
Publicidad digital	Regular la publicidad dirigida a NNA en plataformas digitales, incluyendo marketing encubierto a través de influencers.
Verificación de edad	Establecer estándares sobre verificación de edad proporcionales y respetuosos de la privacidad de NNA.
Institucionalidad supervisora	Crear o designar una institucionalidad especializada con competencias claras para supervisar el cumplimiento de las obligaciones de las plataformas digitales.

La propuesta destaca que no basta con identificar riesgos a nivel global o general: las empresas tecnológicas deben realizar evaluaciones de impacto ajustadas a las particularidades del contexto chileno, considerando brechas de alfabetización digital, desigualdades socioeconómicas y debilidades en las redes de cuidado. Las evaluaciones de impacto con enfoque de derechos humanos son clave para garantizar que las medidas preventivas sean pertinentes, proporcionales y contextualizadas.

### 6.4 Lineamientos de política pública

En el ámbito de la política pública, el informe formula las siguientes recomendaciones:

- **1: Estrategia nacional de bienestar digital de NNA:** desarrollar una estrategia que articule las iniciativas existentes en educación, salud, protección social y regulación digital, con objetivos comunes y mecanismos de coordinación interministerial. Esta estrategia debe incorporar metas verificables y mecanismos de rendición de cuentas.

- **2:** Alfabetización digital crítica: fortalecer las políticas orientadas no solo al uso seguro de tecnologías, sino también al desarrollo de habilidades para enfrentar la desinformación, la presión social y los riesgos asociados a la interacción digital. Esto implica formación específica para NNA, docentes y familias, con énfasis en el pensamiento crítico y la autonomía digital progresiva.
- **3:** Participación vinculante de NNA: crear mecanismos institucionales que garanticen la participación de NNA en el diseño de políticas y regulaciones digitales, reconociendo su condición de sujetos activos de derechos y su conocimiento situado sobre los entornos digitales.
- **4:** Monitoreo y generación de evidencia: fortalecer los sistemas de producción de datos sobre la situación de NNA en el entorno digital, con especial atención a grupos etarios específicos, perspectiva de género e interseccionalidad (NNA migrantes, con discapacidad, de pueblos originarios, en situación de pobreza).
- **5:** Mecanismos de exigibilidad de la responsabilidad empresarial: promover herramientas que permitan corregir prácticas empresariales que vulneren los derechos de NNA, incluyendo el impulso de mecanismos de reclamación, acciones colectivas y sanciones efectivas ante incumplimientos.

## 7. RECOMENDACIONES ESPECÍFICAS POR TIPO DE RIESGO

El informe sistematiza recomendaciones específicas para cada categoría de riesgo del modelo de las 4 C, distinguiendo entre medidas de tipo normativo, regulatorio y de política pública:

### 7.1 Riesgos de contenido

- Establecer obligaciones de las plataformas para detectar, restringir o eliminar contenidos que promuevan la autolesión, la violencia sexual o la explotación infantil, con plazos y procedimientos definidos.
- Introducir sistemas de reporte y alerta confiables para NNA y adultos que acompañan, con canales accesibles y tiempos de respuesta acotados.
- Prohibir el uso de sistemas de recomendación algorítmica que amplíen la exposición de NNA a contenidos potencialmente dañinos.
- Fortalecer la educación mediática y el pensamiento crítico frente a la desinformación en el currículo escolar.

### 7.2 Riesgos de conducta

- Regular el diseño adictivo de plataformas, incluyendo funcionalidades que incentivan el uso compulsivo y la comparación social, con particular atención a su impacto en NNA.
- Establecer protocolos de detección y respuesta ante situaciones de ciberacoso en el sistema escolar, con roles claramente definidos para docentes y equipos directivos.
- Promover programas de educación entre pares sobre convivencia digital respetuosa y prevención de la violencia en línea.

### 7.3 Riesgos de contacto

- Establecer obligaciones para que las plataformas activen por defecto configuraciones que restrinjan el contacto no solicitado de adultos desconocidos con NNA.

- Regular los sistemas de mensajería privada en plataformas dirigidas o accesibles a NNA, incorporando salvaguardas frente al grooming.
- Fortalecer la capacidad de investigación y persecución penal de delitos de explotación sexual digital contra NNA, con recursos humanos y tecnológicos adecuados.

#### 7.4 Riesgos de consumidor

- Prohibir la publicidad basada en perfilamiento de NNA, incluyendo publicidad encubierta a través de influencers dirigida a audiencias menores.
- Establecer la obligación de transparencia sobre mecanismos algorítmicos de personalización de contenidos accesibles a NNA.
- Fortalecer la educación financiera y del consumidor digital en el currículum escolar, con énfasis en el reconocimiento de estrategias de marketing digital.

#### 7.5 Riesgos transversales

- Incorporar la perspectiva de género e interseccionalidad en el diseño de todas las medidas de protección, reconociendo que los riesgos digitales afectan de forma diferenciada a niñas, NNA migrantes, con discapacidad y de menores recursos.
- Diseñar las regulaciones considerando el impacto sobre el acceso equitativo al entorno digital, evitando que medidas protectoras generen efectos de exclusión o profundización de brechas existentes.
- Establecer mecanismos periódicos de revisión y actualización de las normas, dado el ritmo de evolución tecnológica y la aparición constante de nuevas plataformas y prácticas de riesgo.

## 8. AGENDA PROPUESTA PARA LA DEFENSORÍA DE LA NIÑEZ

El informe propone una agenda de trabajo para la Defensoría de la Niñez articulada en torno a tres etapas:

### 8.1 Etapa previa: sensibilización y articulación

En una primera etapa, la Defensoría puede asumir un rol activo de sensibilización y articulación con actores clave del sistema político, académico, empresarial y de la sociedad civil. Esto implica posicionar el tema en la agenda pública, generar alianzas estratégicas con organismos internacionales y homólogos de otros países, y contribuir al debate legislativo en curso sobre protección de datos, debida diligencia e inteligencia artificial.

### 8.2 Rol normativo y de supervisión

En una segunda etapa, la Defensoría puede asumir un rol activo en la supervisión del cumplimiento de las obligaciones del Estado y las empresas respecto de los derechos digitales de NNA. Esto incluye el monitoreo de la implementación de las normas vigentes, la producción de informes temáticos y la formulación de recomendaciones al Ejecutivo y el Legislativo sobre las brechas normativas identificadas.

### 8.3 Participación y defensa de derechos

En una tercera etapa, la Defensoría puede fortalecer los mecanismos de participación de NNA en el debate sobre derechos digitales, así como la atención de casos individuales y colectivos de vulneración de derechos en el entorno digital. La creación de canales accesibles de denuncia y orientación, junto con el litigio estratégico en casos emblemáticos, pueden contribuir a consolidar estándares de protección y visibilizar la problemática ante la ciudadanía y las instituciones.

## 9. CONCLUSIONES

La protección de los derechos de NNA en entornos digitales constituye uno de los desafíos más urgentes y complejos de la política pública y la regulación contemporánea. Los hallazgos del presente informe evidencian que en Chile existe una brecha significativa entre los riesgos a los que están expuestos NNA en el entorno digital y la capacidad del marco normativo e institucional para prevenir, mitigar y reparar los daños asociados.

El diagnóstico para Chile muestra niveles relevantes de exposición a contenidos inapropiados, violencia digital, acoso sexual en línea y uso problemático de tecnologías, con impactos diferenciados según género, edad y nivel socioeconómico. La experiencia comparada demuestra que los países que han logrado mayores avances en esta materia son aquellos que han adoptado marcos regulatorios integrales, que combinan obligaciones de resultado con deberes de proceso, anclados en la debida diligencia y en sistemas de supervisión independiente.

Chile ha dado pasos importantes en los últimos años con la Ley N°21.430, la nueva Ley de Protección de Datos y diversas iniciativas programáticas. Sin embargo, persisten vacíos normativos relevantes que exigen una respuesta legislativa y de política pública coordinada. El informe propone una hoja de ruta que combina lineamientos éticos, normativos y de política pública, orientada a garantizar entornos digitales seguros, inclusivos y respetuosos de los derechos de NNA, sin perder de vista que el acceso equitativo al entorno digital también es un componente fundamental del ejercicio de sus derechos.