weprotect Global Alliance

CPC LEARNING NETWORK

COLUMBIA | MAILMAN SCHOOL OF PUBLIC HEALTH

Evaluación global de amenazas 2025

Prevención de la explotación y el abuso sexual infantil facilitados por la tecnología: **de la información a la acción**

Índice

Nota sobre el contenido y los recursos de apoyo

Este informe aborda la explotación y el abuso sexual infantil facilitados por la tecnología, incluyendo relatos de supervivientes que pueden resultar angustiosos. Algunos lectores pueden encontrar difíciles de leer algunas secciones del informe. Si este contenido le preocupa, puede consultar los recursos globales confidenciales aquí.

No está solo: hay ayuda disponible.

- Brave Movement, Get Help: centro de líneas de ayuda nacionales.
- Child Helpline International: líneas de ayuda para la niñez específicas de cada país.
- INHOPE: red global de líneas directas para denunciar material de abuso sexual infantil en su país.
- MOORE | Prevención del abuso sexual infantil, Escuela de Salud Pública Bloomberg de la Universidad Johns Hopkins: orientación y recursos para personas que buscan ayuda para sí mismas o para otras personas para prevenir el abuso sexual infantil.
- Programa de autoayuda ReDirection: recurso confidencial en línea que brinda apoyo a personas preocupadas por sus pensamientos o comportamientos sexuales hacia la niñez.

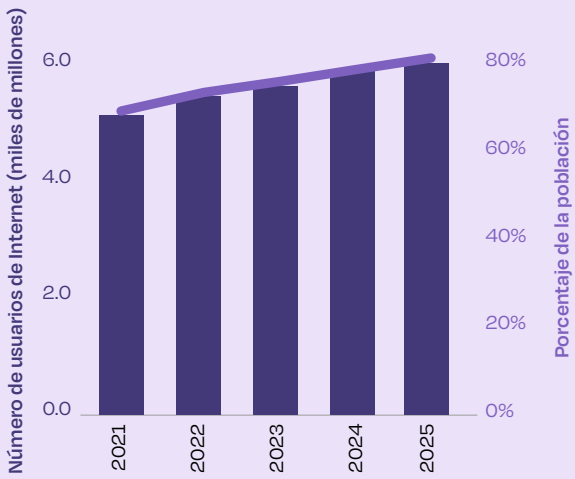
Resumen ejecutivo

> **«El futuro de nuestro mundo digital no tiene por qué ser aterrador, puede ser emocionante y enriquecedor. Pero debemos abordarlo con cuidado, responsabilidad y transparencia. Al entrar en esta nueva era de la inteligencia artificial (IA), debemos asegurarnos de que las generaciones más jóvenes no solo estén preparadas para navegar por estos espacios, sino que también tengan la capacidad de convertirlos en algo mejor.»**
>
> *Defensora de los jóvenes*[1]

La explotación y el abuso sexual infantil facilitados por la tecnología (CSEA, por sus siglas en inglés) son un desafío global complejo que causa un daño profundo a los niños, las familias y las comunidades. Esta amenaza es **prevenible, no inevitable.**[2] Abordar esta cuestión requiere una acción coordinada e intersectorial centrada en los derechos de los niños, y están surgiendo datos y estrategias prometedoras a nivel mundial. La Evaluación de la Amenaza Global 2025 adopta un enfoque orientado a la acción, evaluando el panorama actual y haciendo hincapié en la prevención y las medidas prácticas para mantener la seguridad de la niñez.

El panorama digital está cambiando rápidamente, lo que crea nuevas amenazas para los niños y retos para la detección y la aplicación de la ley. Más de 6.000 millones de personas utilizan Internet y el acceso de los jóvenes supera al de la población general.[3,5] Más de la mitad de la población mundial posee ahora un teléfono inteligente.[4]

Figura 1 . Tendencias en el uso de Internet en los últimos cinco años[5]



Si bien las tecnologías digitales crean oportunidades para la conexión, el aprendizaje y la expresión, también exponen a los niños a nuevos riesgos. La tecnología suele amplificar los daños que afectan a los espacios físicos, sociales y digitales. Las tecnologías existentes y emergentes, como la inteligencia artificial generativa (IA), el cifrado y la realidad extendida, están transformando los entornos digitales de la niñez. En solo unos años, la IA generativa, incluidos los chatbots de IA, ha

pasado de ser en gran medida experimental a estar totalmente integrada en las redes sociales, las plataformas de mensajería y las herramientas cotidianas que utilizan los niños.[6] Si bien estos avances aportan beneficios, también plantean retos importantes para la prevención, la detección y la aplicación de la ley. Las plataformas cifradas mejoran la privacidad de los usuarios, pero también pueden reducir las barreras para cometer delitos contra los niños. Además, dificultan la detección, el bloqueo y la eliminación del material de abuso sexual infantil (CSAM, por sus siglas en inglés).

Los expertos de la sociedad civil destacan una tendencia actual en la que algunos delincuentes inician el contacto con los niños en plataformas abiertas antes de trasladar las interacciones a canales cifrados o entornos fuera de línea con la intención de causar daño. Además, cada vez hay más pruebas que sugieren que la explotación y el abuso sexual perpetrados por compañeros parecen estar aumentando, y que la exposición a contenidos sexuales inapropiados en Internet puede estar influyendo en ello.[7-9] Los daños causados por amigos, compañeros de clase y parejas íntimas suelen surgir cuando se dan una combinación de medidas de protección digital débiles, una supervisión deficiente y una educación limitada sobre la conducta adecuada en Internet y los comportamientos sexuales.[10,11]

El abuso sexual infantil facilitado por la tecnología sigue aumentando en escala y complejidad, impulsado por los rápidos cambios tecnológicos y las deficiencias sistémicas. Desde 2023, los daños existentes han persistido en gran medida, mientras que han surgido nuevas amenazas a un ritmo más rápido del que pueden adaptarse las leyes, las políticas y las medidas de protección. El material de abuso sexual infantil se está detectando, denunciando y eliminando a niveles récord. Sigue siendo difícil obtener datos fiables sobre la prevalencia mundial y es necesario actuar con cautela a la hora de interpretar las tendencias observadas en las denuncias, ya que estas suelen reflejar la capacidad y las prácticas de denuncia, más que la verdadera escala del daño. Por ejemplo, el número de reportes recibidos por CyberTipline del Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) disminuyó de 36,2 millones en 2023 a 29,2 millones de incidentes en 2024, correspondientes a 20,5 millones de denuncias individuales. Esta reducción se atribuye principalmente a dos factores: las prácticas de «agrupación», que consolidan múltiples reportes relacionados en un solo incidente, y el uso creciente del cifrado de extremo a extremo, que dificulta la detección y el reporte de contenido ilegal o perjudicial.[12]

INHOPE recibió
2,5 millones
de denuncias de presuntos casos de CSAM en 2024, más del doble que el año anterior.[13]

El NCMEC recibió
20,5 millones
de denuncias de presuntos casos de explotación sexual infantil en 2024.[12]

La Internet Watch Foundation (IWF) confirmó casi **300 000** casos de CSAM en 2024.[14]

La IA generativa se ha utilizado para facilitar la creación y distribución de CSAM a gran escala, para ocultar las identidades de las víctimas y los agresores, y para eludir las leyes y las medidas de protección, como los métodos de verificación de la edad. También ha impulsado nuevas formas de CSEA, como la extorsión sexual financiera y las imágenes «*deepfake*» que muestran a niños reales en situaciones sexualizadas simuladas. A finales de 2023, se denunciaron las primeras imágenes de abuso sexual infantil generadas por IA a través de líneas directas de Internet y, desde entonces, su prevalencia ha aumentado exponencialmente.[15] **La CyberTipline** del NCMEC registró un aumento del 1.325 % en las denuncias relacionadas con la IA generativa entre 2023 y 2024, lo que representa 67 000 denuncias.[12] Este volumen supone una carga para las fuerzas del orden y los moderadores de contenidos.

En los primeros seis meses de 2025, el NCMEC recibió más de **440 000** denuncias de IA generativa relacionadas con la explotación sexual infantil.[12]

El *grooming* y la seducción en línea siguen siendo frecuentes. En 2024, el NCMEC documentó 546 000 denuncias, lo que supone un aumento del 192 % en comparación con 2023.[12] Los expertos también señalan intersecciones alarmantes entre la CSEA facilitada por la tecnología y otros daños, como las ideas suicidas y las autolesiones, el extremismo, la trata de personas y las estafas con motivaciones económicas. Este fenómeno emergente requiere una mayor investigación y sigue sin entenderse bien. La extorsión sexual con fines económicos es una tendencia persistente que afecta de manera desproporcionada a la niñez.

En 2024, el NCMEC recibió aproximadamente **100** denuncias de extorsión sexual financiera al día.[12]

Se está generando un impulso global para abordar la CSEA facilitada por la tecnología.

Desde 2023, varios países han propuesto o aprobado nuevas leyes para abordar esta cuestión. La **Ley de Denuncias** de **los Estados Unidos** de 2024 impuso obligaciones adicionales a las empresas tecnológicas, entre ellas la obligación de informar al NCMEC casos que antes eran voluntarios y sanciones de hasta un millón de dólares por infracciones.[16] **La Ley de Seguridad en Línea** del Reino Unido de 2023 amplía los nuevos requisitos, incluidas las evaluaciones de riesgos y la verificación de la edad, a cientos de miles de proveedores de servicios en línea de todo el mundo que se dirigen a usuarios del Reino Unido.[17] En Brasil, dos medidas históricas de protección de la infancia en 2025 incluyeron la prohibición a nivel nacional del uso no educativo de los teléfonos inteligentes en las escuelas y una nueva legislación que introduce la seguridad desde el diseño y la obligación de informar para las plataformas en línea.[19,20] Australia ha adoptado una restricción de edad para las redes sociales, limitando su uso a los menores de 16 años, que actualmente se está aplicando.[18] En Singapur, el regulador de las telecomunicaciones pronto exigirá la verificación de la edad para descargar determinadas aplicaciones en dispositivos móviles, la primera legislación de este tipo a nivel mundial.[21] El impacto de esta ola de legislación aún está por verse, ya que las políticas pasan a la fase de regulación y aplicación.

La **Convención de las Naciones Unidas contra la Ciberdelincuencia**, adoptada en diciembre de 2024 y que ahora se encamina hacia su ratificación, marca un hito importante en la protección infantil a nivel mundial. Por primera vez, tipifica como delitos internacionales el material sexual infantil y los delitos de captación de menores en línea.[22,23] El **Pacto Digital Global**, implementado en 2025, proporciona un marco para la cooperación internacional y orienta los esfuerzos para abordar los daños en línea y reforzar la seguridad digital.[24]

También se han logrado avances notables gracias a la adopción de la segunda edición de las **Directrices terminológicas para la protección de los niños contra la explotación y el abuso sexuales** (abreviadas como Directrices terminológicas), la puesta en marcha de asociaciones innovadoras entre distintos sectores para mejorar la detección y la prevención, como **Lantern**, y estudios de investigación a gran escala destinados a colmar las lagunas de pruebas.[25,26] **La revisión sistemática viva** del Safe Futures Hub proporcionará pruebas actualizadas, mientras que iniciativas como **Prevention Global** amplían los conocimientos sobre la prevención de la perpetración y la prevalencia mundial.[27,28]

Las perspectivas de los niños siguen estando infrarrepresentadas. A pesar de algunos enfoques prometedores para integrar las perspectivas de los niños en las políticas y la toma de decisiones, a menudo no se les brinda la oportunidad de participar de manera significativa en las decisiones políticas que les afectan. Nuestra revisión de la bibliografía publicada desde 2023 en relación con la CSEA facilitada por la tecnología reveló que solo una minoría de las publicaciones incluía las opiniones de los niños y que muy pocas les consultaban sobre sus recomendaciones de actuación. La Evaluación Global de Amenazas 2025 incluyó consultas con niños para ayudar a informar y dar forma a las recomendaciones presentadas.

La CSEA facilitada por la tecnología se puede prevenir, pero no existe una solución universal. La prevención requiere la acción de toda la sociedad. El marco de prevención presentado en este informe, que complementa el Modelo de Respuesta Nacional de la Alianza Global WeProtect, ofrece orientación práctica en cuatro áreas de acción interrelacionadas:[29]

- PARTICIPACIÓN Y LIDERAZGO DE LOS NIÑOS
- EDUCACIÓN Y APOYO COMUNITARIO
- SEGURIDAD DIGITAL
- LEGISLACIÓN, POLÍTICAS Y JUSTICIA

Estas áreas de acción se distribuyen en tres niveles de prevención:

- primario (protección proactiva)
- secundario (detección y prevención del daño)
- terciario (respuesta y apoyo tras el daño, lo que puede evitar la revictimización y la reincidencia)

El marco sintetiza las pruebas emergentes, las buenas prácticas y las orientaciones de los expertos. Su objetivo es proporcionar un punto de partida para que las partes interesadas consideren las medidas de prevención pertinentes para su contexto y experiencia. Las áreas de acción se organizan de manera que reflejen el modelo socioecológico, comenzando por los niños y avanzando hacia las comunidades, las instituciones, los gobiernos y los actores globales.[30] Destaca la naturaleza estratificada de la prevención, en la que cada nivel refuerza a los demás. Los facilitadores, como la financiación y la investigación, proporcionan la base para todas las acciones y deben abordarse de forma proactiva y mantenerse para que la prevención sea posible.

Marco de prevención

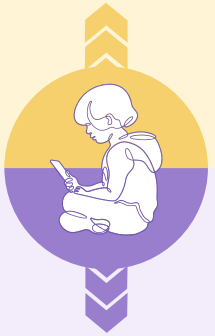
Principios rectores

Todos los niños y niñas tienen derecho a estar a salvo de cualquier daño, incluida la explotación y el abuso sexuales.
Las iniciativas para prevenir la explotación y el abuso sexual de menores facilitados por la tecnología deben:

- Defender los derechos y la dignidad de los niños y los supervivientes y evitar aumentar los riesgos o causar más daños.
- Reconocer que los niños corren el riesgo tanto de sufrir daños como de participar en comportamientos que pueden dañar a otros niños.
- Guiarse por las perspectivas, experiencias y preferencias de los niños y los supervivientes.
- Tener en cuenta las diferencias en la edad, el desarrollo y otras características de la niñez, como la identidad de género, la orientación sexual, el origen étnico, la discapacidad, la condición de migrante, la situación económica y educativa, que pueden afectar a sus necesidades y a los riesgos a los que se enfrentan.

Factores que impulsan la explotación y el abuso sexual de niños facilitados por la tecnología

- Falta de mecanismos de protección
- Motivaciones económicas
- Débil rendición de cuentas
- Vulnerabilidades interseccionales
- Normas sociales y culturales perjudiciales



Factores que facilitan la prevención

- Voluntad política
- Gobernanza digital sólida y rendición de cuentas a nivel mundial, nacional y local
- Terminología y sistemas de datos armonizados
- Coordinación mundial e intersectorial
- Normas sociales y culturales favorables
- Profesionales y proveedores capacitados que trabajan con niños
- Sistemas sólidos de protección infantil

Investigación y datos

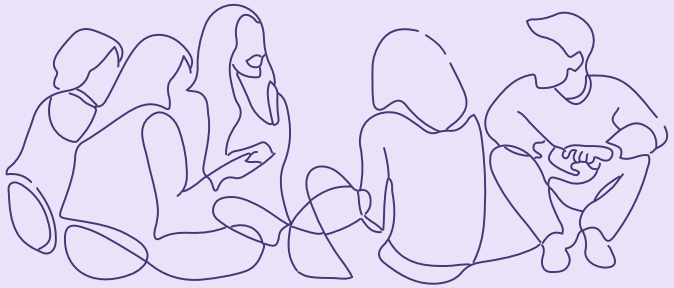
- Utilizar un enfoque de salud pública para la prevención: definir el problema y su prevalencia, identificar los factores de riesgo y de protección, diseñar y poner a prueba intervenciones, y ampliar lo que funciona.
- Dar prioridad al desarrollo de conocimientos y buenas prácticas en países de ingresos bajos y medios y en contextos infrarrepresentados
- Compartir datos, conocimientos y buenas prácticas entre regiones y sectores, adaptando las pruebas de forma sensible a los nuevos contextos
- Realizar análisis costo-beneficio para reforzar los argumentos a favor de la financiación de la prevención
- Dar prioridad a la investigación basada en datos o dirigida por niños, jóvenes, supervivientes y poblaciones marginadas

Financiación sostenible

- Líneas presupuestarias específicas en las estrategias nacionales
- Compromisos de la industria
- Participación de instituciones multilaterales
- Mecanismos de financiación flexibles
- Financiación intersectorial
- Apoyo sostenible a las organizaciones comunitarias
- Financiación para la innovación y la generación de pruebas

PARTICIPACIÓN Y LIDERAZGO INFANTIL

Involucrar de manera significativa a la niñez en la definición de los problemas y en la elaboración de políticas, programas y servicios que les afectan.



Prevención primaria **PROTEGER DE MANERA PROACTIVA**	Prevención secundaria **DETECTAR E INTERRUMPIR**	Prevención terciaria **APOYAR Y RESPONDER**
Diseñe conjuntamente con niños y niñas iniciativas de educación y sensibilización que tengan en cuenta el contexto y reflejen cómo utilizan la tecnología, en quién confían y a quién recurren en busca de ayuda si sufren daños o tienen inquietudes sobre sus propios pensamientos y comportamientos.	Colaborar con organizaciones dirigidas por niños y supervivientes para diseñar, implementar y evaluar conjuntamente canales de denuncia accesibles, fáciles de usar y fiables, incluidos canales no formales, como compañeros capacitados.	Utilizar los conocimientos y los datos de los niños y adultos supervivientes para mejorar la accesibilidad y la calidad de los servicios de apoyo, los sistemas judiciales y los mecanismos de reparación. Explorar los conceptos propios de los supervivientes sobre el daño, la justicia y la rendición de cuentas, incluidos los enfoques de justicia no formal y restaurativa.

Consultar a los niños solo cuando se cuente con personal capacitado, medidas de seguridad y servicios de apoyo. De lo contrario, consultar a jóvenes y adultos que puedan representar las perspectivas de los niños, incluidos los adultos sobrevivientes.

Crear espacios seguros y acogedores, tanto en línea como fuera de línea, para que los niños compartan sus opiniones e influyan en las políticas, los programas y los servicios.

Involucrar a niños de diferentes edades, géneros y orígenes, y abordar las barreras que impiden la inclusión. Recabar la opinión de niños y niñas que han sufrido daños, así como de los que los han causado.

SEGURIDAD DIGITAL

Proteger a los niños dando prioridad a su seguridad, bienestar y derechos en la cultura del sector y en el diseño y desarrollo de productos, servicios e infraestructuras digitales.

Prevención primaria **PROTEGER DE MANERA PROACTIVA**	Prevención secundaria **DETECTAR E INTERRUMPIR**	Prevención terciaria **APOYAR Y RESPONDER**
Dar prioridad a la seguridad, los derechos y el bienestar de la niñez en todos los niveles de la cultura empresarial, la toma de decisiones y la formación de la plantilla. Hacer que la seguridad por diseño sea la norma, integrando evaluaciones del impacto sobre los derechos del niño y la debida diligencia en los procesos de desarrollo. Consultar a los niños y jóvenes para informar las decisiones de diseño y garantizar que las características de seguridad sean funcionales, accesibles y estén disponibles de manera equitativa en todos los lugares e idiomas en los que se ofrece un producto o servicio. Armonizar la terminología y las métricas de transparencia de los informes para mejorar la comparabilidad entre productos y servicios.	Detectar e interrumpir los contenidos y comportamientos nocivos utilizando herramientas en tiempo real que respeten la privacidad y los derechos de los usuarios (por ejemplo, comparación de hash, ventanas emergentes de advertencia, redirección a servicios de apoyo, detección de comportamientos de *grooming* y transacciones financieras de riesgo). Financiar y proporcionar apoyo psicosocial y de salud mental a los responsables de la primera línea digital.	Proporcionar canales de denuncia accesibles y adaptados a la niñez dentro de la plataforma. Estos deben conectar directamente a los usuarios con líneas de ayuda y servicios de apoyo, y proporcionarles información oportuna. Garantizar procesos seguros y libres de estigmatización para que los supervivientes puedan solicitar la retirada de sus imágenes. Reforzar la transparencia y la rendición de cuentas, divulgando el impacto material de los productos y servicios digitales en los derechos del niño en todos los países en los que están disponibles. Recopilar y compartir datos de seguridad anonimizados y desglosados para reforzar el aprendizaje en todo el sector y entre sectores. Colaborar en toda la industria para eliminar el contenido sexual infantil abusivo y otros contenidos nocivos.

LEY, POLÍTICA Y JUSTICIA

Fortalecer los sistemas jurídicos y normativos para prevenir los abusos, garantizar la justicia y exigir responsabilidades a los responsables.

Prevención primaria **PROTEGER DE MANERA PROACTIVA**	Prevención secundaria **DETECTAR E INTERRUMPIR**	Prevención terciaria **APOYAR Y RESPONDER**
Fortalecer, armonizar y hacer cumplir las leyes y reglamentos utilizando una terminología universal y definiendo claramente las obligaciones y sanciones. Consultar con los supervivientes, los grupos de defensa de los derechos del niño, la industria y otras partes interesadas para armonizar la legislación con las leyes sobre los derechos del niño, las pruebas y las buenas prácticas, y permitir una innovación responsable por parte de la industria. Diseñar leyes que reconozcan las diferencias de desarrollo entre niños y adultos, hagan hincapié en la rehabilitación de niños y niñas que causan daño y eviten criminalizar los comportamientos mutuamente deseados entre compañeros de edad similar. Establecer reguladores nacionales/regionales con el poder, los recursos y los conocimientos técnicos necesarios para establecer normas, supervisar su cumplimiento y garantizar una supervisión y una rendición de cuentas sólidas por parte de la industria.	Establecer sistemas proactivos para detectar, investigar y responder a los abusos sexuales de menores facilitados por la tecnología, en lugar de depender únicamente de las denuncias de los supervivientes. Exigir a las instituciones financieras que detecten y denuncien activamente las transacciones relacionadas con la explotación sexual infantil. Establecer canales de denuncia accesibles, adaptados a los niños y sensibles al trauma, vinculados a servicios de apoyo, y proporcionar información clara sobre dónde se deben presentar las denuncias o buscar ayuda en cada país.	Formar a las fuerzas del orden, el poder judicial y los fiscales en procesos adaptados a los niños, sensibles al trauma y centrados en los supervivientes, que defiendan los derechos, la dignidad y el interés superior de los niños. Establecer bases de datos nacionales anónimas de víctimas para informar la prevención y la respuesta. Utilizar el seguimiento y la rehabilitación basados en pruebas para prevenir la reincidencia. Tratar a los niños en conflicto con la ley de conformidad con las normas internacionales de justicia infantil. Utilizar la rehabilitación, la desviación y las penas alternativas. Evitar la detención, el registro y la notificación.

EDUCACIÓN Y APOYO A LA COMUNIDAD

Dote a la niñez, los cuidadores y las comunidades de los conocimientos, las habilidades y las herramientas necesarios para mantener la seguridad de niños y niñas, y responder adecuadamente a los riesgos y daños. Proporcione intervenciones tempranas para los niños y adultos que corren el riesgo de causar daños.

Prevención primaria **PROTEGER DE MANERA PROACTIVA**	Prevención secundaria **DETECTAR E INTERRUMPIR**	Prevención terciaria **APOYAR Y RESPONDER**
Implementar y evaluar iniciativas de educación y sensibilización basadas en pruebas que promuevan la seguridad digital, la denuncia y la búsqueda de ayuda. Asegurarse de que sean accesibles, estén disponibles en varios idiomas y se impartan en las escuelas, las comunidades y las plataformas digitales que utilizan los niños. Enseñar a los niños cómo mantenerse a sí mismos y a los demás seguros tanto en línea como fuera de línea, dónde buscar ayuda, a qué adultos seguros pueden acudir en busca de ayuda y cómo denunciar sus preocupaciones sobre su propia seguridad o la de otras personas, o sobre comportamientos sospechosos.	Establecer múltiples canales de denuncia formales y no formales, accesibles y adaptados a los niños, incluyendo líneas de ayuda, compañeros capacitados y adultos de confianza que puedan proporcionar apoyo y recursos tempranos. Formar a compañeros, cuidadores, educadores y proveedores de servicios para ayudar a los niños a mantenerse seguros tanto en Internet como fuera de ella, y responder adecuadamente a las preocupaciones o denuncias de daños. Llevar a cabo intervenciones tempranas basadas en pruebas para los niños y adultos que corren el riesgo de causar o sufrir daños.	Apoyar a los supervivientes y garantizar que conozcan sus derechos, opciones, servicios disponibles y medidas que pueden tomar para protegerse de daños mayores, solicitar la eliminación de imágenes y buscar justicia. Proporcionar servicios informados sobre el trauma y centrados en los supervivientes, tanto para niños como para adultos, que aborden los daños tanto en línea como fuera de línea, promuevan la seguridad y la dignidad y prevengan daños adicionales. Estos deben incluir servicios de apoyo legal, sanitario, de salud mental y psicosocial. Proporcionar respuestas basadas en pruebas y no carcelarias para que los niños que han causado daños se rehabiliten y se evite la reincidencia.

Recomendaciones

Las recomendaciones que se desprenden de la Evaluación de la Amenaza Global 2025 subrayan la necesidad de una acción global coordinada para prevenir la CSEA facilitada por la tecnología. En conjunto, esbozan un enfoque integral y multisectorial para proteger a los niños tanto en línea como fuera de línea.

Recomendaciones transversales para todas las partes interesadas

1. **Abordar el abuso sexual infantil facilitado por la tecnología como una prioridad urgente de salud pública e invertir en estrategias de prevención, incluidas aquellas destinadas a prevenir la perpetración y reducir el estigma asociado con la búsqueda de ayuda y la divulgación.** Reconocer que la niñez corre el riesgo tanto de sufrir daños como de participar en comportamientos que causan daño a otros niños.
2. **Generar y utilizar pruebas para fundamentar la prevención.** Involucrar de forma segura y ética a los niños y a los supervivientes para definir el problema e identificar las barreras que impiden la inclusión de las poblaciones marginadas.
3. **Colaborar entre sectores para coordinar los esfuerzos de prevención y compartir las lecciones aprendidas.** Adoptar una terminología armonizada y alineada con las Directrices terminológicas, estandarizar las métricas y los sistemas de notificación, compartir datos y pruebas oportunas sobre lo que funciona y lo que no, y establecer sistemas sostenibles.[26]

Organizaciones de la sociedad civil, incluidas las ONG internacionales

1. **Crear espacios seguros e inclusivos para que los niños y los supervivientes compartan sus opiniones e influyan en los esfuerzos de prevención y promoción.** Esforzarse por involucrar a los niños marginados, incluidos los niños con discapacidades, las poblaciones de minorías sexuales y de género, los niños de zonas rurales y que no asisten a la escuela, los niños de minorías étnicas o de origen migrante, y los niños que carecen de acceso a las tecnologías digitales.
2. **Promover la prevención y la respuesta basadas en los derechos y mecanismos sólidos de rendición de cuentas para abordar la CSEA facilitada por la tecnología.**
3. **Fortalecer los servicios comunitarios de denuncia y apoyo, incluidas las líneas de ayuda y los compañeros de apoyo.** Capacitar a los cuidadores, educadores y proveedores de servicios para que presten apoyo tempranos y sin prejuicios; así como garantizar servicios accesibles y centrados en las personas sobrevivientes —tanto niños como adultos— que aborden los daños sufridos en entornos digitales y presenciales, promuevan su bienestar a largo plazo y prevengan la revictimización.
4. **Ofrecer intervenciones tempranas basadas en pruebas para niños y adultos en riesgo de causar o sufrir daños,** y proporcionar respuestas basadas en pruebas y no carcelarias para los niños que han causado daños.

Sector privado, en particular las empresas tecnológicas

1. **Dar prioridad a la seguridad, los derechos y el bienestar de los niños en todos los niveles de la cultura empresarial, la toma de decisiones y la formación de la plantilla.** Proporcionar educación y formación continuas en todo el proceso de contratación, invertir en investigación preventiva y servicios de apoyo a los supervivientes, y garantizar que los equipos de respuesta digital de primera línea y los equipos de confianza y seguridad cuenten con el apoyo y los recursos necesarios.
2. **Hacer que la seguridad por diseño sea la norma, integrando evaluaciones de impacto sobre los derechos del niño y la debida diligencia en los procesos de desarrollo.** Consultar de forma segura a los niños, jóvenes y supervivientes para informar las decisiones de diseño. Garantizar que las funciones de seguridad sean funcionales, accesibles y estén disponibles de forma equitativa en todas las regiones geográficas e idiomas en los que se ofrece un producto o servicio.
3. **Reforzar la transparencia y la rendición de cuentas.** Divulgar todos los impactos materiales sobre los derechos del niño asociados a los productos y servicios digitales a través de los marcos de información corporativa existentes en cada país en el que se opera.31 Recopilar y compartir datos de seguridad anonimizados y desglosados con investigadores, reguladores y todos los sectores para informar sobre la prevención. Incorporar mecanismos de rendición de cuentas independientes en el gobierno corporativo.
4. **Detectar y eliminar de forma proactiva los contenidos y comportamientos perjudiciales.** Utilizar herramientas en tiempo real que respeten los derechos, como la comparación de hash para detectar contenido previamente identificado, la supervisión de actividad en línea, las alertas emergentes que advierten sobre riesgos, la redirección inmediata a servicios de apoyo, y la detección proactiva de conductas de *grooming* y transacciones financieras de alto riesgo. Al mismo tiempo, proporcionar canales de denuncia accesibles y adaptados a la niñez que conecten directamente a los usuarios con líneas de ayuda y servicios de apoyo, eliminar rápidamente los contenidos perjudiciales y dar respuestas oportunas a las denuncias presentadas.

Ámbito académico e investigadores

1. **Dar prioridad a la investigación sobre la prevalencia, los factores de riesgo y de protección, y los factores sistémicos que impulsan el abuso sexual infantil facilitado por la tecnología.** Abordar las lagunas críticas en la investigación, incluidas las vulnerabilidades interseccionales, la escalada entre el mundo en línea y fuera de ella, y las estrategias eficaces de prevención de los abusos, incluyendo el tratamiento de la aparición de comportamientos sexuales perjudiciales entre los niños y los jóvenes.
2. **Desarrollar, adaptar y evaluar intervenciones en diferentes entornos y poblaciones.** Establecer asociaciones entre sectores y llevar a cabo investigaciones sobre la rentabilidad y la implementación para orientar las inversiones sostenibles.
3. **Establecer asociaciones de investigación conjuntas, coordinar agendas de investigación y promover el intercambio oportuno de datos.**

Gobiernos

1. **Revisar, reforzar y armonizar las leyes y reglamentos mundiales para abordar la CSEA facilitada por la tecnología.** Consultar ampliamente con las partes interesadas para armonizar la legislación con las pruebas, las buenas prácticas y las leyes y normas sobre los derechos del niño. Utilizar una terminología armonizada y garantizar que la legislación sea tecnológicamente neutra, abarcando tanto las tecnologías existentes como las futuras. Definir claramente las obligaciones, las sanciones y los mecanismos de rendición de cuentas de los responsables, al tiempo que se permite la innovación responsable de la industria. Diferenciar entre los comportamientos de los adultos y los adolescentes, y evitar criminalizar los comportamientos mutuamente deseados entre compañeros de edades similares.
2. **Dotar de recursos y coordinar los sistemas nacionales de protección y justicia infantil para hacer frente a los daños causados a los niños tanto en línea como fuera de línea.** Establecer múltiples canales de denuncia accesibles, adaptados a los niños y que tengan en cuenta los traumas, vinculados a servicios integrales de salud, psicosociales y jurídicos. Mantener bases de datos seguras y anónimas de las víctimas para orientar la prevención y la respuesta. Formar a las fuerzas del orden, el poder judicial, los educadores y los trabajadores de primera línea en prácticas adaptadas a los niños y que tengan en cuenta los traumas, y proporcionarles apoyo continuo para su bienestar.
3. **Utilizar sistemas de supervisión y rehabilitación basados en datos empíricos para prevenir la reincidencia y dar prioridad al apoyo, la desviación y las penas alternativas para los menores en conflicto con la ley.**
4. **Establecer reguladores nacionales o regionales independientes con la autoridad, los recursos y los conocimientos técnicos necesarios para hacer frente a la CSEA facilitada por la tecnología,** lo que incluye el establecimiento de normas, la supervisión del cumplimiento y la aplicación de sanciones.
5. **Implementar y evaluar programas nacionales de educación y sensibilización basados en pruebas que tengan como objetivo promover la seguridad digital, la denuncia y la búsqueda de ayuda.** Integrar la educación adecuada a la edad en los planes de estudio escolares y formar a los profesores, cuidadores y proveedores de servicios. Llevar a cabo campañas de educación y sensibilización accesibles y multilingües, colaborando con las comunidades y otros sectores para llegar a los niños marginados.

Organizaciones intergubernamentales

1. **Facilitar la cooperación transfronteriza en materia de aplicación de la ley y el intercambio de información.**
2. **Proporcionar asistencia técnica y movilizar recursos para fortalecer la capacidad nacional,** dando prioridad en función de las necesidades y la prevalencia.
3. **Movilizar financiación conjunta y sostenible** para apoyar a los gobiernos nacionales, las organizaciones comunitarias y las iniciativas innovadoras de prevención.

Prólogo

« Mis imágenes se han comercializado en Internet durante más de 20 años. Soy víctima de CSAM todos los días de mi vida. Sufrí abusos cuando era niño, cuando mi primer agresor creó mi CSAM. Desde entonces, cada semana mis abogados reciben nuevas notificaciones de que mi material se encuentra en la colección de otro pedófilo. Hace más de una década acudí al Tribunal Supremo de los Estados Unidos con mis abogados del bufete Marsh Law para tratar este asunto.

Mi serie de CSAM es tan popular que sé que su distribución nunca terminará. Pero no todas las víctimas de CSAM tienen por qué estar condenadas al mismo destino. La tecnología para intervenir, detectar y detener la difusión de CSAM existe. Debemos hacer que las grandes empresas tecnológicas la utilicen.

Era adolescente cuando descubrí que mi CSAM se comercializaba en todo el mundo. En aquel entonces, yo era una de las pocas víctimas de este crimen atroz. Hoy en día, hay [cientos de millones de] niños que son víctimas cada año.

Ahora estoy criando a un adolescente en un mundo que cada día es más peligroso. Es increíblemente difícil criar a niños pequeños en esta era tecnológica tan tóxica. ¿Cómo puedo asegurarme de que mis hijos nunca se encuentren con mi CSAM cuando está literalmente por todo Internet? ¿Cómo puedo mantener a mis hijos a salvo de los depredadores cuando sé que solo están a dos clics del peligro?

Me siento increíblemente orgullosa de ver a víctimas como yo, y a padres como yo, enfrentarse a las grandes empresas tecnológicas. Pero para que quede claro: vamos a necesitar investigación innovadora, herramientas policiales de vanguardia y el apoyo incondicional de defensores dedicados para tener alguna posibilidad. No sé cómo lo vamos a conseguir, pero sé que se lo debemos a todos los niños y niñas, y por eso no vamos a rendirnos.

No tengo ninguna respuesta sobre cómo mantener a los niños seguros en Internet hoy en día, pero sí sé esto: WeProtect [Global Alliance] ha sido un salvavidas para los supervivientes en esta lucha por la vida de nuestros hijos. Gracias a esta red de apoyo, por fin veo la luz al final del túnel. Los problemas relacionados con el material sexual infantil en línea empeoran cada día y la brecha en la rendición de cuentas es cada vez mayor. Sin embargo, las escuelas están prohibiendo los teléfonos, las empresas tecnológicas están tomando conciencia, la verificación de la edad está aumentando, los sistemas de apoyo se están ampliando y los supervivientes de todo el mundo están alzando la voz con valentía.

Por fin estamos avanzando en la dirección correcta. »

Esta declaración ha sido proporcionada, con el apoyo de Protect Children, por un superviviente que, como muchos otros, ha decidido permanecer en el anonimato. WeProtect Global Alliance invitó a este colaborador anónimo a compartir su voz junto con muchas otras personas con experiencias vividas, ya sea de los niños que buscamos proteger en el mundo digital o de los supervivientes de abusos sexuales facilitados por la tecnología, porque estas voces suelen pasar desapercibidas. En esta Evaluación de amenazas globales, entretejemos estas experiencias vividas a lo largo de las pruebas y la investigación, basando nuestro trabajo en la realidad de las personas. Reconocemos que estas voces son complejas, diversas y, en ocasiones, discrepantes, pero deben ser escuchadas.

Introducción

Objetivos

La explotación y el abuso sexual infantil facilitados por la tecnología (CSEA, por sus siglas en inglés) son un desafío global complejo que perjudica profundamente a los niños, las familias y las sociedades. Prevenir y responder a este daño requiere una acción urgente y coordinada entre sectores y fronteras.

La Evaluación de la amenaza global 2025 tiene dos objetivos:

1. Analizar las tendencias mundiales en materia de CSEA facilitada por la tecnología desde 2023.
2. Diseñar conjuntamente un marco de prevención con expertos, defensores de los jóvenes y supervivientes, proporcionando recomendaciones viables en consonancia con el Modelo de Respuesta Nacional de la Alianza Global WeProtect.

La Evaluación de la amenaza global 2025 hace hincapié en la necesidad de adoptar enfoques sensibles al contexto. Los riesgos a los que se enfrentan los niños, su acceso a las tecnologías digitales y a los recursos de protección, y la solidez de los sistemas de protección varían mucho de una región a otra. El informe revela importantes lagunas en materia de protección y destaca la urgente necesidad de equidad en los esfuerzos de prevención a nivel mundial, en particular para proteger a los niños en entornos poco regulados o con recursos limitados.

Marco de derechos de los niños y las niñas

> «Los jóvenes deben tener derecho a comprender sus derechos en Internet. Reconocer estos derechos ya sería un paso adelante para salir de situaciones peligrosas.»

Niña de 14 años, Canadá[32]

La prevención de la explotación sexual infantil y la pornografía infantil facilitadas por la tecnología es un imperativo legal y ético basado en el derecho internacional de los derechos humanos. La Convención de las Naciones Unidas sobre los Derechos del Niño exige a los Estados que protejan a los niños de todas las formas de violencia, explotación y abuso. La Observación general n.º 25 confirma que estos derechos se extienden a los espacios digitales y exige a los gobiernos que integren los derechos de los niños en las políticas digitales, garanticen el acceso a la justicia y consulten a los niños sobre las decisiones que les afectan.[33,34] Si bien la Convención sobre los Derechos del Niño establece obligaciones para los Estados como responsables, los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas y los Principios sobre los Derechos del Niño y las Empresas establecen la responsabilidad del sector privado de respetar los derechos de los niños y prevenir y responder a los abusos de los derechos.[35,36] Estos principios sustentan el análisis de las tendencias mundiales de este informe y sirven de base para el marco de prevención y las recomendaciones que se presentan a continuación.

Nota sobre la terminología

En 2025, un grupo de trabajo interinstitucional mundial actualizó las Directrices de Luxemburgo y publicó la segunda edición de las **Directrices terminológicas para la protección de los niños contra la explotación y el abuso sexuales** (abreviadas como Directrices terminológicas).[26] De conformidad con estas directrices, en el presente informe se utiliza el término «explotación y abuso sexual infantil facilitado por la tecnología (CSEA, por sus siglas en inglés)». La **CSEA facilitada por la tecnología** se refiere al uso de tecnologías digitales en cualquier etapa para preparar, cometer o difundir (en el caso del material de abuso sexual infantil o CSAM, por sus siglas en inglés) la explotación sexual o el abuso sexual de un niño. Abarca los daños cometidos tanto en entornos digitales como no digitales (fuera de línea), incluyendo, por ejemplo, el intercambio de información, la coordinación de acciones y el contacto con niños para prepararlos o coaccionarlos. Este término reconoce que la tecnología desempeña un papel en la facilitación del abuso y en la perpetuación de los daños causados por el abuso, tanto en los espacios físicos como en los digitales.

Se entiende por **niño** cualquier persona menor de 18 años. Los niños, incluidos los adolescentes, difieren en función de características como la edad, la etapa de desarrollo, la orientación sexual, la identidad de género, la discapacidad, el origen étnico, el nivel educativo, la situación económica y la condición migratoria. Estos factores interrelacionados pueden afectar a los riesgos y daños a los que se enfrentan los niños, así como a su acceso a los recursos de protección. Un **superviviente** es una persona que ha sufrido explotación o abuso sexual. Muchos supervivientes de CSEA facilitado por la tecnología son ahora adultos que también deben ser incluidos en los esfuerzos de prevención y respuesta. Reconociendo que las personas con experiencia vivida utilizan diferentes términos para describirse a sí mismas, este informe utiliza indistintamente los términos «**víctima**» y «**superviviente**.»

Metodología

Este informe se basa en una amplia gama de fuentes de datos y conocimientos especializados. Ha sido elaborado bajo la dirección de un comité directivo de expertos formado por 14 representantes del gobierno, las fuerzas del orden, el sector privado, la sociedad civil, la academia, organizaciones internacionales y defensores de las experiencias vividas.

Las pruebas se sintetizaron mediante:

- Una revisión exploratoria de la literatura académica y gris relacionada con los dos objetivos del informe, publicada en inglés entre enero de 2023 y octubre de 2025.
- Entrevistas semiestructuradas con 32 partes interesadas de todos los sectores y regiones entre junio y julio de 2025, con el fin de triangular perspectivas y abordar las lagunas en la literatura.
- Una encuesta en línea con 77 expertos en septiembre de 2025 para recabar perspectivas multisectoriales sobre la priorización de las medidas de prevención.
- Las conclusiones de cuatro talleres para jóvenes y supervivientes dirigidos por organizaciones centradas en los supervivientes y los jóvenes. Los supervivientes también revisaron las guías de las entrevistas y los grupos de discusión para garantizar su pertinencia y sensibilidad.
- Estudios de casos compartidos por organizaciones y miembros de la Alianza Global WeProtect, en los que se muestran prácticas prometedoras y respuestas innovadoras.

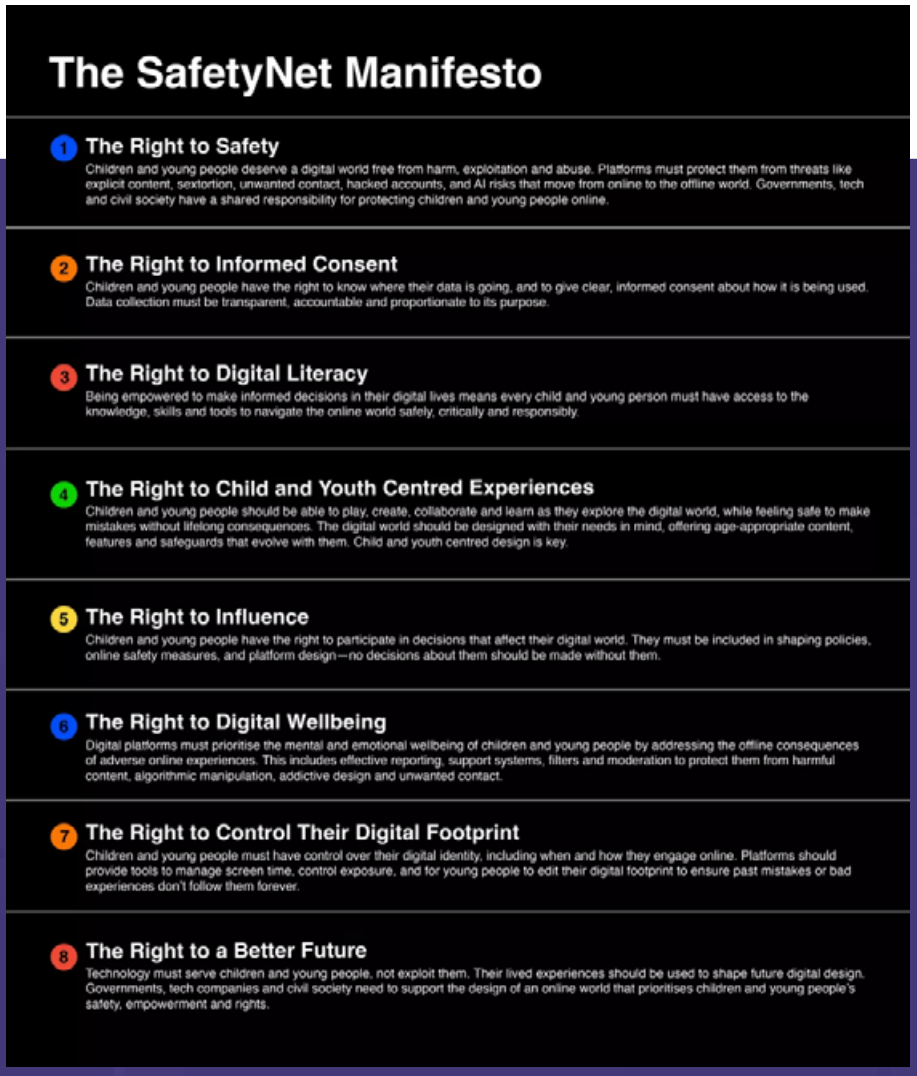
Se garantizó la diversidad geográfica mediante la selección de las partes interesadas, los ejemplos de buenas prácticas y los estudios de casos, prestando especial atención a las regiones y contextos infrarrepresentados. El marco de prevención se creó y revisó de forma conjunta mediante procesos participativos que se basaron en esta diversidad y representación.

Entre las limitaciones se incluyen la restricción a las publicaciones en inglés, lo que limita la representación regional, el breve plazo para la recopilación de datos y el posible sesgo de selección en la inclusión de partes interesadas y estudios de casos, a pesar de los esfuerzos por garantizar la diversidad geográfica y sectorial.

El Manifiesto SafetyNet: las voces de los jóvenes por un futuro digital más seguro

Para comprender mejor cómo los niños y los jóvenes experimentan el mundo digital e imaginar un futuro en línea más seguro, WeProtect Global Alliance lideró la segunda fase del proyecto #MyVoiceMyFuture. A través de consultas con 109 jóvenes entre 13 y 24 años de 10 países, y en colaboración con siete organizaciones juveniles, la iniciativa recopiló información sobre la seguridad digital, los derechos y la CSEA facilitada por la tecnología. El resultado es el **Manifiesto SafetyNet**, una declaración de derechos digitales impulsada por los jóvenes y una hoja de ruta para construir un futuro digital más seguro y equitativo. El Manifiesto pide protecciones más sólidas, un diseño inclusivo y una acción colectiva para garantizar que todos los niños y jóvenes puedan existir en línea sin miedo.[37]

Figura 2. Manifiesto SafetyNet publicado en el Safe Futures Hub en junio de 2025[38]



El panorama digital

Los niños de hoy en día crecen en una era de rápida transformación digital. Si bien el entorno digital ofrece valiosas oportunidades para el aprendizaje, la conexión, la expresión y la pertenencia, también puede exponer a los niños a riesgos y daños importantes, tanto en línea como fuera de línea. Estas oportunidades y riesgos han evolucionado rápidamente en los últimos años, acelerados por el auge de tecnologías como la inteligencia artificial generativa (IA), los entornos de realidad extendida (XR), la descentralización, la computación cuántica y el cifrado de extremo a extremo, que han puesto a prueba la capacidad de prevenir, detectar y responder a la CSEA facilitada por la tecnología.[39]

Los niños están más conectados que nunca, pero persisten las desigualdades digitales.[40] En la actualidad hay 6.000 millones de usuarios de Internet, lo que supone aproximadamente tres cuartas partes de la población mundial, frente al 64 % en 2021.[5] Más de la mitad de la población mundial posee ahora un teléfono inteligente.[4] En algunos países de la Mayoría Global, la mayor parte del tráfico web se produce en dispositivos móviles, que a menudo se comparten dentro de los hogares o entre amigos.[41] Por ejemplo, el 88 % del tráfico web en Filipinas y el 85 % en Nigeria procedían de un dispositivo móvil en febrero de 2025.[41]

El uso de Internet de los jóvenes supera al del resto de la población en un 13 %.[42] Una encuesta mundial realizada a más de 380 000 niños de 55 países reveló que la mayoría comenzó a utilizar un dispositivo digital antes de los 10 años.[43] En solo unos años, las tecnologías de IA han pasado de ser en gran medida experimentales a estar totalmente integradas en las redes sociales, las plataformas de mensajería y las herramientas cotidianas que utilizan los niños, como los chatbots con IA.[6,44] Si bien la IA ofrece beneficios educativos y sociales, está amplificando rápidamente los riesgos y daños para la niñez, incluido el abuso sexual infantil facilitado por la tecnología. Los esfuerzos para aprovechar su potencial para proteger a los niños se están quedando atrás.

Las conclusiones del **Índice de Bienestar Digital** 2025 revelan que el 80 % de los adolescentes y jóvenes adultos de la generación Z afirmaron haber experimentado algún tipo de riesgo en línea.[45] Las interacciones potenciales de grooming eran comunes y el intercambio de imágenes íntimas estaba muy extendido. Además, aproximadamente uno de cada cuatro encuestados indicó que había encontrado imágenes sexuales generadas por IA, mientras que el 25 % de los participantes desconocía que la generación de imágenes sexuales de menores es ilegal.

Aunque cada vez más niños de todo el mundo tienen acceso a las tecnologías digitales, dicho acceso —y, con él, la exposición a los riesgos— sigue siendo desigual. Casi la mitad de los seis millones de escuelas de todo el mundo carecen de acceso a Internet, la mayoría de ellas en países del sur global y zonas rurales remotas.[46] Se ha relacionado sistemáticamente un estatus socioeconómico más alto con una mayor alfabetización digital, y la brecha digital actúa como «un amplificador de exclusiones sociales más amplias».[47] Los niños que carecen de acceso a dispositivos digitales siguen estando en riesgo, ya que los abusos sexuales presenciales a menudo se graban, almacenan y difunden a través de tecnologías digitales, incluidos los dispositivos compartidos.

Panorama jurídico y político

En los últimos años, los gobiernos y los organismos internacionales han impulsado respuestas legislativas y políticas con el fin de armonizar las leyes, reforzar la regulación y adaptarse a la rápida evolución de las tecnologías. **La Convención de las Naciones Unidas contra la Ciberdelincuencia** (2024) establece la primera norma universal contra la ciberdelincuencia, que abarca explícitamente los delitos contra la niñez, como el CSAM y el *grooming*, al tiempo que refuerza el intercambio internacional de pruebas.[23]

La **Primera Conferencia Ministerial Mundial sobre la Erradicación de la Violencia contra los Niños** (2024) impulsó la coordinación multisectorial y los compromisos nacionales para reforzar los marcos de protección de la infancia, incluido el tema de los daños en línea.[48] El **Esquema de Clasificación Universal Versión 3** (2025) proporciona un marco armonizado para identificar, categorizar y responder al material de explotación y abuso sexual infantil, con etiquetas legibles por máquina y definiciones alineadas a nivel mundial más allá de las fronteras.[49] La segunda edición de las **Directrices Terminológicas** (2025) proporciona una base de terminología universal para facilitar la reforma legal.[26]

Ha surgido una «tercera ola» de reformas legislativas en todos los países, caracterizada por una mayor armonización, que incluye restricciones de edad en las redes sociales, medidas para garantizar la viabilidad futura y esfuerzos para cerrar las lagunas jurídicas en torno a nuevos daños, como las imágenes de abuso sexual infantil generadas por IA y la extorsión sexual.[50] Sin embargo, muchos marcos para proteger a la niñez siguen estando fragmentados u obsoletos, con una autoridad reguladora inconsistente y protecciones limitadas contra los contenidos sexuales generados en primera persona que involucran a niños o el abuso facilitado por la IA.[50,51] En algunos entornos, los niños víctimas de extorsión sexual siguen corriendo el riesgo de ser criminalizados, lo que refleja las lagunas entre la ley, las políticas y la realidad que viven los niños.[52]

Los persistentes retos en materia de aplicación de la ley y regulación siguen socavando los avances. Las investigaciones transfronterizas se ven ralentizadas por la fragmentación jurisdiccional, la desigualdad en la asignación de recursos y la debilidad de los sistemas de intercambio de datos. Solo el 45 % de los 20 países del Grupo de Trabajo Global de la Alianza Global WeProtect tienen obligaciones formales de notificación para las empresas tecnológicas.[53] La dependencia de medidas voluntarias del sector deja importantes lagunas en materia de rendición de cuentas, especialmente en los países de la mayoría global. Los representantes de la industria argumentan que los sistemas de notificación voluntaria pueden ser más ágiles y receptivos, pero existe un amplio consenso entre las partes interesadas en que se necesitan obligaciones vinculantes.

> «Pero, como empresas, a menudo no lo hacen a menos que se vean obligadas a ello.»
>
> *Industria*[7]

Los rápidos cambios tecnológicos están superando a las herramientas legales existentes, y las tensiones entre la protección de la privacidad y la detección proactiva siguen sin resolverse.[39] Se requiere una mayor coordinación internacional y armonización legislativa, reguladores con más poderes, un aumento de los recursos destinados a los sistemas de protección infantil y a la aplicación de la ley, y obligaciones industriales exigibles para proteger a los niños en el entorno digital en rápida evolución.

> «No podemos resolver este problema con detenciones.»
>
> *Gobierno*[54]

Magnitud y naturaleza de la explotación y el abuso sexual infantil facilitados por la tecnología

Desde la última Evaluación Global de Amenazas, los daños existentes han continuado, mientras que han surgido nuevos riesgos a un ritmo más rápido del que pueden responder las salvaguardias legales, políticas y tecnológicas. Este capítulo reúne las pruebas disponibles sobre la magnitud de los abusos, las características de las víctimas y/o supervivientes, los perfiles de los autores y las amenazas emergentes, reconociendo que los datos globales siguen siendo fragmentados, incompletos y difíciles de comparar. Varios estudios sobre la prevalencia de los autores que se publicarán próximamente tienen por objeto subsanar las lagunas existentes en los datos (véase el apéndice). A pesar de estas limitaciones, las conclusiones ofrecen una imagen importante del entorno de amenazas entre 2023 y 2025 y sientan las bases para las recomendaciones que se formulan más adelante en este informe.

Panorama de los datos

> « La verdad es que... es realmente imposible dar una escala precisa del problema. »
>
> *Industria*[7]

Los datos disponibles sobre la CSEA facilitada por la tecnología reflejan los avances colectivos en materia de coordinación, notificación y supervisión, y son esenciales para comprender la amenaza y movilizar la acción. Sin embargo, comenzamos señalando las limitaciones persistentes del entorno de datos, ya que estos retos condicionan tanto la interpretación de las cifras disponibles como el análisis que sigue a continuación. Los datos disponibles son fragmentados y parciales. Por ejemplo, los esfuerzos por medir la prevalencia mundial se ven limitados por las lagunas en la cobertura geográfica, las definiciones incoherentes, la diferente eficacia de los sistemas de detección y notificación, y la calidad variable de los estudios. La limitada transparencia del sector también dificulta la evaluación de las medidas que están tomando las empresas: por ejemplo, el 60 % de las 50 principales plataformas mundiales de intercambio de contenidos no publican información sobre cómo abordan la explotación sexual infantil y, entre las que lo hacen, los datos son fragmentados y carecen de comparabilidad.[55]

Los datos disponibles pueden sobreestimar, debido a la duplicación o a la clasificación incorrecta del material, como subestimar, debido al cifrado y a las plataformas ocultas.[7] Los datos sólidos y representativos sobre las víctimas y los autores siguen siendo limitados, como se analiza más adelante en este capítulo. A la luz de estos retos, hemos realizado entrevistas con expertos y defensores de las víctimas para abordar las lagunas en las pruebas y recabar información actualizada y específica sobre las tendencias emergentes y los retos operativos. Aunque no sustituyen a los datos representativos, la triangulación de estas perspectivas con los conjuntos de datos y las investigaciones existentes proporciona una visión más completa y matizada.

Magnitud y patrones del daño

En esta sección se describen los principales daños que configuran el panorama de amenazas a nivel mundial, entre los que se incluyen el material de abuso sexual infantil (CSAM), el grooming, los abusos retransmitidos en directo, la inteligencia artificial, el extremismo violento en línea y los avances tecnológicos, como el cifrado de extremo a extremo, la descentralización, la computación cuántica y la realidad extendida (XR).

Material de abuso sexual infantil

El CSAM se está detectando, denunciando y eliminando a niveles sin precedentes. Como se ha comentado anteriormente, las tendencias en las denuncias reflejan más la capacidad de denuncia que la prevalencia real y la mayoría de los datos sobre CSAM proceden de plataformas de altos ingresos, lo que ofrece una visión parcial de los daños a nivel mundial. También es importante reconocer que las tendencias al alza pueden reflejar en parte avances positivos, como el aumento del número de niños que denuncian los daños, la mejora de los sistemas de detección por parte de las empresas y una mayor transparencia del sector en el intercambio de datos.

Los datos de diversas fuentes, incluidos los informes obligatorios de la industria del Centro Nacional para Niños Desaparecidos y Explotados (NCMEC), las líneas directas de INHOPE y la detección proactiva y las remisiones de la Fundación para la Vigilancia de Internet (IWF), tienen fines distintos y utilizan metodologías diferentes, por lo que sus cifras no pueden combinarse de manera significativa.

Las cifras comunicadas siguen siendo extraordinariamente elevadas

INHOPE: recibió más de 2,5 millones de denuncias de presuntos contenidos de abuso sexual infantil en 2024, lo que supone un aumento del 218 % con respecto a 2023. De ellas, el 65 % fueron confirmadas como contenidos ilegales. Este aumento se debió en gran medida a SafeNet Bulgaria, que aportó 1,6 millones de denuncias.[13]

NCMEC **CyberTipline**: recibió 20,5 millones de denuncias correspondientes a 29,2 millones de incidentes en 2024, lo que supone un descenso con respecto a los 36,2 millones de 2023. Este descenso se atribuyó en parte a las prácticas de «agrupación» que agrupan las denuncias relacionadas y al impacto del cifrado de extremo a extremo, que limita la capacidad de las empresas para detectar y denunciar material perjudicial.[12]

IWF: evaluó 424 047 denuncias y confirmó 291 273 casos de CSAM o enlaces a este tipo de contenido en 2024, lo que supone un aumento del 6 % con respecto a 2023.[14]

Los tipos de contenido perjudicial son diversos y cada vez más vídeos

NCMEC: en 2024 se denunciaron casi 63 millones de archivos, incluidos 33 millones de vídeos, 28 millones de imágenes y 1,8 millones en otros formatos. De ellos, más de 51 000 afectaban a niños en peligro inminente que requerían una intervención urgente.[12]

IWF: clasificó 734 048 archivos únicos como CSAM, incluidos más de 47 000 vídeos y más de 4000 imágenes no fotográficas prohibidas.[14]

El alojamiento y la distribución siguen concentrándose geográficamente en el contenido que se puede rastrear. INHOPE informó que el 59 % de los servidores detectados se encontraban en los Países Bajos y el 13 % en los Estados Unidos, posiciones que han mantenido durante los últimos cinco años.[13] Del mismo modo, la IWF descubrió que más de la mitad de las URL relacionadas con el abuso sexual infantil que se tomaron medidas en 2024 estaban alojadas en Estados miembros de la Unión Europea, con los Países Bajos, Bulgaria y Rumanía alojando el 29 %, el 9 % y el 7 %, respectivamente.[14]

El índice Into the Light de Childlight destaca los altos niveles de alojamiento de CSAM a nivel mundial que se pueden rastrear hasta los Países Bajos, así como los 4,5 millones de denuncias procedentes solo de India, Pakistán y Bangladesh.[57] La combinación de una infraestructura de alojamiento a gran escala, una conectividad de alta velocidad y una normativa que da prioridad a la libertad de expresión crea unas condiciones que los delincuentes aprovechan para almacenar y distribuir contenidos abusivos. La ubicación de algunos contenidos no se puede rastrear fácilmente porque están alojados en redes anónimas como Tor, diseñadas para ocultar el origen físico del servidor.[11] El NCMEC señaló que el 11 % de las denuncias de **CyberTipline** tenían un origen desconocido en 2024.[58]

Los patrones de distribución cambiaron junto con los esfuerzos de detección. La contribución de SafeNet Bulgaria supuso que los foros representaran el 61 % de las denuncias recibidas por INHOPE en 2024, frente a menos del 9 % en 2023, mientras que las denuncias procedentes de plataformas de alojamiento de imágenes y sitios web convencionales disminuyeron drásticamente.[13] Paralelamente, la IWF recibió principalmente URL y confirmó 291 270 páginas web que contenían CSAM en 2024, lo que supone un aumento del 5 % con respecto a 2023.[14]

Grooming y seducción en línea

La seducción en línea, a menudo denominada grooming, se produce cuando los autores se dirigen a los niños que utilizan Internet para identificarlos y coaccionarlos para que realicen actos sexuales ilegales. En 2024, el NCMEC documentó 546 000 denuncias de seducción en línea, lo que supone un aumento del 192 % con respecto a 2023, y se espera que las cifras aumenten a medida que más empresas cumplan con la **Ley de Denuncias de Estados Unidos**.[16]

Inteligencia artificial generativa

El material de abuso sexual infantil generado por IA, señalado en anteriores evaluaciones de amenazas globales y en entrevistas con informantes clave, sigue creciendo a un ritmo alarmante.[54] Las tecnologías *deepfake* (imágenes o vídeos generados por IA que representan de forma realista a personas que nunca han existido o que alteran fotos y grabaciones reales), los chatbots de IA (herramientas de conversación automatizadas que pueden suplantar la identidad de niños o adultos) y los modelos generativos (sistemas de IA capaces de producir nuevos textos, imágenes o vídeos a partir de patrones aprendidos) se están utilizando como armas para explotar a los niños y difundir CSAM a gran escala.[59]

«Si la tecnología ahora puede crear imágenes y vídeos que nunca han ocurrido realmente, ¿cómo sabremos qué es real en el futuro y cómo cambiará eso la forma en que confiamos unos en otros en Internet?».

Hombre de 15 años, Etiopía[60]

NCMEC: documentó un aumento del 1325 % en las denuncias relacionadas con el contenido sexual infantil abusivo generado por IA entre 2023 y 2024, lo que representa 67 000 denuncias.[12] Para junio de 2025, las cifras preliminares muestran 440 419 nuevas denuncias relacionadas con contenido de explotación sexual infantil generado por IA, frente a las 6.835 del mismo periodo de 2024.[61]

IWF: un solo foro compartió más de 3500 imágenes/vídeos de niños alterados digitalmente o sintéticos en un solo mes.[63]

Thorn: 1 de cada 17 adolescentes denuncia haber sido víctima de imágenes sexuales *deepfake*.[62]

Entre las tácticas emergentes de los delincuentes se incluye el uso de IA predictiva y sistemas de recomendación para identificar y difundir CSAM.[63-65] Algunos delincuentes comparten modelos de IA personalizados entrenados con material real de abuso para generar contenido sintético, mientras que otros prueban estrategias de captación en chatbots con aspecto infantil.[8,63,66] Al mismo tiempo, la IA puede utilizarse para proteger a los niños, y apoyar la detección y la investigación.

Figura 3. IA: promesas y dificultades [6,67,68]

OPORTUNIDADES

Automatizar la detección de comportamientos nocivos: interrumpir las interacciones de alto riesgo, el grooming y la trata antes de que se produzca el daño.

Automatizar la detección de CSAM: identificar, bloquear y eliminar rápidamente los contenidos nocivos.

Apoyo a las fuerzas del orden: agilizar las investigaciones, revisar y clasificar el CSAM, identificar a las víctimas y los delincuentes, y reducir la exposición humana a contenidos traumáticos.

Seguridad desde el diseño: desarrollar e implementar sistemas y modelos de IA generativa seguros.

AMENAZAS

Amplificar el daño: revictimizar a los niños creando nuevas imágenes a partir del material CSAM existente, difundir CSAM y guías para cometer delitos, eludir los sistemas de verificación de la edad y potenciar los contenidos nocivos mediante algoritmos.

Generar CSAM: producir representaciones sexualizadas o explícitas de niños, en su totalidad o en parte, incluyendo *deepfakes* de niños reales en situaciones sexualizadas simuladas.

Complicar la detección y la aplicación de la ley: impedir la identificación de víctimas y delincuentes, saturar los sistemas de detección y eliminación, y la capacidad de las fuerzas del orden.

Reducir las barreras técnicas y sociales al daño: permitir la fácil creación de CSAM, facilitar el *grooming* en línea y normalizar la explotación y la sexualización de los niños (por ejemplo, aplicaciones de «nudificación»).

> «En mi opinión, la IA podría ser muy útil, pero, como cualquier herramienta poderosa, necesita normas de seguridad y, en lugar de eliminarla, deberíamos crear protecciones sólidas y trucos de seguridad, como filtros, supervisión y orientación, para garantizar que sea segura para los niños y para todos los demás.»
>
> *Mujer de 15 años, Etiopía*[60]

Extremismo violento en línea

Desde la Evaluación Global de Amenazas 2023, los grupos en línea que promueven la violencia han proliferado, con un aumento del 200 % en los informes del NCMEC (más de 1.300 en total) entre 2023 y 2024.[12] Estos grupos animan a los niños a hacerse daño a sí mismos o a otros, lo que pone de relieve nuevas intersecciones entre la explotación sexual, la radicalización en línea y los daños fuera de línea. Se han observado nuevas intersecciones con ideas suicidas, trastornos alimentarios, estafas por motivos económicos y trata de personas, aunque las investigaciones siguen siendo limitadas. Los autores suelen dirigirse a los niños en foros en los que estos buscan ayuda.[7]

> **«Seguiremos viendo esta fusión de riesgos... Creo que [la extorsión sexual] es un gran ejemplo en el que se han unido tantas amenazas diferentes para crear este nuevo daño... cuando alguien se acerca a ti y te dice: "Oye, eres guapa, ¿quieres charlar?"...entonces se convierte en un intercambio de imágenes... y luego puede convertirse en la producción real de imágenes de abuso sexual infantil. A continuación, puede convertirse en acoso y hostigamiento antes de convertirse en chantaje real, lo que podría llevar a la autolesión....»**
>
> *Industria*[7]

Desde la primera línea de la detección de daños: perspectivas de PGI sobre los grupos «Com»

PGI (Protection Group International) ayuda a gobiernos, ONG y empresas a detectar y combatir los daños en línea, desde la explotación infantil y la desinformación hasta el extremismo violento, utilizando inteligencia dirigida por personas y respaldada por tecnología.

Los grupos «Com» (también conocidos como «Com») son un archipiélago de comunidades en línea en las que se manipula a niños y jóvenes para que produzcan material de abuso sexual infantil, se autolesionen o incluso graben actos violentos. Estos grupos son en su mayoría transnacionales y se conocen con nombres diferentes y cambiantes: 764, 676, Harm Nation, Leak Society y CVLT se engloban bajo este paraguas. Aunque los autores suelen ser jóvenes —predominantemente adolescentes varones—, hay solapamientos con subculturas extremistas y marginales, incluidos grupos con ideologías violentas.

Tácticas de la «Com»
Los autores suelen utilizar plataformas convencionales para identificar a niños y adolescentes vulnerables, a menudo buscando a aquellos que ya tienen problemas de salud mental. Por ejemplo:

- Se infiltran en comunidades en línea de autolesiones o trastornos alimentarios e invitan a los niños a chats grupales cerrados.
- Aprovechan los videojuegos populares dirigidos a los niños como espacios para conocer a posibles víctimas, redirigiéndolas a plataformas de mensajería privada.

Una vez aislados, los jóvenes pueden enfrentarse a amenazas, manipulación o extorsión. Las víctimas pueden ser presionadas para que graben o retransmitan en directo actos perjudiciales, como autolesiones, CSAM o consumo de drogas. Este material se recopila en los llamados «*lorebooks*», que también contienen información personal de las víctimas. Estos *lorebooks* circulan entre los miembros de la comunidad, y los autores ganan estatus en función del nivel de daño que infligen. Los perpetradores crean regularmente nuevas identidades en línea para evitar ser detectados.

Repercusión en las víctimas
- Las víctimas suelen sufrir graves daños psicológicos y viven bajo un miedo constante debido a las amenazas y el chantaje. La exposición a la coacción y a las exigencias violentas puede intensificar vulnerabilidades ya existentes, como la depresión, la ansiedad o las ideas suicidas, que en ocasiones se intensifican hasta convertirse en actos forzados de autolesiones o intentos de suicidio.
- La exposición constante a material extremo puede normalizar los comportamientos dañinos para las víctimas, lo que a veces conduce a una participación continua. Algunas víctimas pasan de la participación coaccionada a la implicación continua con los grupos de delincuentes, y en casos excepcionales incluso crean sus propios canales y repiten los patrones de abuso.

Abuso transmitido en directo

Como se destaca en la Evaluación Global de Amenazas 2023, la escala y la naturaleza del abuso sexual de menores transmitido en directo, que se produce tanto en las principales redes sociales como en plataformas dedicadas a la transmisión en directo, sigue siendo importante y está poco documentada.[69] Las encuestas a delincuentes que buscan CSAM en la deepweb sugieren que más de un tercio consume material transmitido en directo, con una prevalencia que varía según las regiones.[70] Las investigaciones muestran que las retransmisiones en directo suelen estar preacordadas, con pequeñas transacciones financieras que vinculan a los consumidores de las regiones con mayores ingresos con los facilitadores de las jurisdicciones de alto riesgo.[71]

Proyectos como el estudio **Scale of Harm** *(Escala de daño)* de International Justice Mission cubren lagunas de datos fundamentales, pero se necesita un seguimiento más sistemático. El seguimiento financiero es una vía prometedora para la detección (véase Prevención).

Tecnologías en evolución: cifrado, descentralización, computación cuántica y realidad extendida

Cifrado de extremo a extremo

Cada vez más utilizado como función de privacidad y seguridad, el cifrado de extremo a extremo garantiza que solo los remitentes y los destinatarios puedan ver el contenido de los mensajes. Sin embargo, cuando se introduce sin medidas de protección infantil adicionales, hace prácticamente imposible detectar el material sexual infantil o el *grooming*, y limita gravemente la capacidad de las fuerzas del orden para identificar a las víctimas.[72] En diciembre de 2023, una de las principales aplicaciones de mensajería mundial, Meta, habilitó el cifrado de extremo a extremo de forma predeterminada, y se espera que otras plataformas sigan su ejemplo. Es probable que la creciente adopción y el uso del cifrado de extremo a extremo hayan contribuido a una **disminución de 7 millones en los incidentes de explotación sexual infantil en línea** denunciados al NCMEC.[12] Varias plataformas importantes también redujeron el volumen de denuncias en aproximadamente un 20 % en 2024, lo que suscitó preocupaciones sobre la transparencia y la rendición de cuentas.[73]

Descentralización

La informática descentralizada distribuye las tareas entre múltiples dispositivos o sistemas en lugar de depender de una autoridad central, lo que permite conexiones entre pares y aplicaciones como redes sociales, almacenamiento de datos, transacciones financieras y aprendizaje automático.[39] Si bien esta arquitectura puede mejorar la privacidad, también plantea retos únicos para prevenir y abordar la CSEA facilitada por la tecnología. La descentralización complica la identificación de sospechosos, la moderación de contenidos y la eliminación de material ilegal.[39] De cara al futuro, el principal reto radica en la creciente adopción de tecnología descentralizada sin las garantías adecuadas para los riesgos ya observados.[39]

Computación cuántica

La computación cuántica es un campo emergente que permite procesar la información de forma exponencialmente más rápida que los computadores clásicos. Aunque aún no se han documentado casos de su uso en la CSEA, los riesgos futuros podrían incluir la aceleración de la generación de CSAM generado por IA o la ruptura de los sistemas de cifrado que actualmente protegen los datos de los niños. Es fundamental adoptar políticas tempranas y consideraciones de seguridad desde el diseño antes de que las aplicaciones maduren.[39]

Realidad extendida

Las tecnologías XR (realidad virtual, aumentada y mixta) son cada vez más accesibles y asequibles, lo que aumenta los riesgos de uso indebido y abuso.[75] Las investigaciones destacan posibles usos indebidos, como experiencias inmersivas de CSAM y la normalización de comportamientos perjudiciales.[76] Es esencial tomar medidas preventivas antes de que la XR se generalice. Al mismo tiempo, la XR es prometedora para la prevención y la formación, ya que ofrece simulaciones realistas para la aplicación de la ley y las intervenciones terapéuticas. Sin embargo, las pruebas de su eficacia siguen siendo limitadas.

> **« ... con la realidad virtual, pronto se podrá tocar y sentir, y habrá numerales en los cuerpos, lo que supondrá una nueva forma de infligir daño físico en el espacio virtual por parte de los agresores. »**
>
> *Superviviente*[77]

Características y vulnerabilidades de las víctimas y/o supervivientes

En la siguiente sección se resume lo que se sabe actualmente sobre las víctimas y/o supervivientes, al tiempo que se señalan las persistentes lagunas de datos. La información sobre las víctimas que aparecen en el material de abuso sexual infantil sigue siendo escasa: solo una pequeña parte de los millones de niños que aparecen en los informes de Interpol han sido identificados, localizados geográficamente o confirmados por su edad.[9] La magnitud del problema supera la capacidad de las fuerzas del orden, debido a la escasez de personal, capacidad técnica y recursos financieros para identificar a las víctimas. Los delincuentes ocultan deliberadamente los detalles que permiten identificarlos o utilizan tecnologías de cifrado o anonimización, lo que dificulta enormemente el análisis de las imágenes y el rastreo de su origen.[78]

El material denunciado muestra de manera desproporcionada a niños prepúberes, mientras que los adolescentes probablemente estén infrarrepresentados debido a la falta de investigación sobre este grupo demográfico concreto y a la dificultad de distinguir sus imágenes de las de los adultos jóvenes.[8,9] El estigma, las prácticas de denuncia inconsistentes y la falta de desagregación de datos en los sistemas de datos administrativos limitan la capacidad de comprender la demografía y las características de las víctimas. Los grupos marginados, incluidas las poblaciones de minorías sexuales y de género, los niños con discapacidades y aquellos que viven en condiciones institucionales o inestables, siguen estando en gran medida ausentes de los datos cuantitativos a pesar de enfrentarse a un mayor riesgo.[8]

> «No sabemos qué les sucede a las víctimas.»

Fuerzas del orden[79]

Edad y género

En consonancia con la Evaluación Global de Amenazas de 2023, las niñas prepúberes siguen siendo las víctimas más frecuentemente representadas en los casos de CSAM denunciados. En 2024, los datos de I See Child Abuse Material (ICCAM) mostraron que el 98,7 % de los casos denunciados involucraban a niñas y el 93,2 % eran niñas prepúberes.[13] Los niños representan una proporción desproporcionada de las víctimas de extorsión sexual, ya que constituyen el 91 % de las denuncias recibidas por la IWF en 2023.[14] Las pruebas anecdóticas sugieren que es posible que más niños sean objeto de extorsión sexual con fines económicos debido a los hábitos de los niños de compartir imágenes o a la impresión que tienen los delincuentes de su disposición y capacidad para pagar.[9]

> «Hemos oído que sí se aprovechan de las chicas [con extorsión sexual económica], pero de otra manera. No lo hacen por dinero. Lo hacen para obtener imágenes con las que... chantajearlas. Los chicos son su objetivo.»

Industria[7]

La edad sigue siendo un factor crítico para comprender el riesgo. Los datos de un estudio representativo de jóvenes entre 16 y 24 años en Australia indican que los niños suelen experimentar por primera vez el intercambio no deseado de sus propias imágenes sexuales alrededor de los 15 años, aunque aproximadamente el 9 % afirma haber tenido su primera experiencia antes de los 11 años.[80] Los datos del ICCAM muestran un ligero aumento en la proporción de denuncias de CSAM que involucran

a niños prepúberes (del 90 % en 2023 al 93,2 % en 2024), mientras que las denuncias que involucran a adolescentes (14-17 años) y bebés/niños pequeños (menores de 3 años) disminuyeron ligeramente.[13] INHOPE también ha documentado un volumen creciente de CSAM que muestra a niños menores de 10 años.[81]

Vulnerabilidades

En consonancia con las conclusiones de evaluaciones globales de amenazas anteriores, los niños marginados, ya sea por pobreza, pertenencia a minorías, abandono, condiciones de vida inestables o residencia en zonas rurales, corren un riesgo desproporcionado.[80,82-84] Otros factores de riesgo son las dinámicas familiares que normalizan los comportamientos controladores, la falta de conocimientos digitales o de supervisión por parte de los padres, la falta de apoyo social y la exposición previa a la violencia, el material sexual infantil y la pornografía violenta.[54,84-86] Los niños con discapacidades también se enfrentan a riesgos agravados de explotación sexual, por ejemplo, un mayor impacto negativo en la salud mental y comportamientos sexuales de riesgo, y barreras significativas para la divulgación, incluyendo el miedo a la culpa de los padres, el juicio y la pérdida de autonomía.[87-89] Las investigaciones muestran que los adolescentes que se enfrentan a múltiples formas de abuso son más propensos a sufrir victimización sexual tanto fuera de línea como en línea, con repercusiones duraderas en su educación y salud mental.[90-93]

Características y comportamientos de las personas con riesgo de delinquir y que han causado daño

Las nuevas pruebas procedentes de las fuerzas del orden, la investigación y las comunidades de delincuentes están profundizando nuestra comprensión de quiénes son los delincuentes, cómo actúan y qué motiva su comportamiento. Aunque la mayoría de los autores son hombres adultos, los patrones son cada vez más complejos, con variaciones en cuanto a edad, género, geografía, motivaciones y métodos. Cada vez se reconoce más a los niños y jóvenes en riesgo de delinquir y que han causado daño, así como la necesidad de una investigación, prevención y apoyo específicos centrados en este grupo de edad. Hasta hace poco, la investigación se centraba en los delincuentes adultos identificados por los sistemas judiciales o que buscaban ayuda, lo que limitaba el conocimiento de las vías de perpetración y las oportunidades de intervención temprana. Enfoques innovadores, como los estudios que encuestan directamente a los delincuentes en la *deep web* y las estimaciones de prevalencia entre muestras representativas de hombres, están ampliando la base empírica, aunque siguen siendo escasos los datos sólidos y representativos.[57,94] Los sesgos en la notificación y las inconsistencias en las definiciones también limitan los datos.[95] A pesar de estas lagunas, la investigación sigue arrojando luz sobre las vulnerabilidades, las tecnologías, los entornos sociales y los fallos sistémicos que permiten la perpetración.

> **«Hacemos todo lo posible por mitigar el riesgo y reducir el daño. Pero mientras haya personas que sigan sintiendo interés sexual por los niños, mientras haya personas que quieran explotar a otras para su propio beneficio económico o de otro tipo, seguiremos teniendo estos problemas. Son lo que llamamos problemas que afectan a toda la sociedad.»**
>
> *Industria*[7]

Perfiles de los delincuentes adultos y patrones de perpetración

Las pruebas disponibles indican que los delincuentes que compran e intercambian contenidos son predominantemente hombres.[96,97] Las encuestas realizadas a los usuarios de CSAM en la *deep web* muestran que el 68 % se identifica como hombre y el 17 % se niega a revelar su género.[94] En el caso de los abusos retransmitidos en directo, los resultados sugieren que los consumidores son en su mayoría hombres, predominantemente de Asia, Europa y América del Norte, mientras que los productores pueden ser tanto hombres como mujeres.[55] Los patrones de edad varían según el tipo de delito y la población estudiada. De los 4.549 encuestados que declararon consumir CSAM en la *deep web*, el 43 % tenía entre 18 y 24 años.[91] Otro estudio muestra que los consumidores de abusos retransmitidos en directo tienden a ser mayores.[94,98]

La perpetración también va más allá de los individuos que actúan por su cuenta. A menudo involucra a actores interconectados a través de las fronteras: un abusador inicial produce imágenes o vídeos; otros suben o distribuyen el material; y los consumidores y compradores alimentan la demanda que impulsa su circulación. Las redes en línea intercambian, normalizan y amplifican este abuso a nivel internacional, lo que hace extremadamente difícil identificar a los perpetradores, a pesar de las investigaciones especializadas.[79,99]

Una cadena global de abuso

En la Operación Víbora (marzo-mayo de 2025), dirigida por la Policía Nacional española con Interpol y Europol, se detuvo a 20 personas y se identificó a otros 68 sospechosos en 12 países relacionados con el CSAM.[100] En la Operación Cumberland (febrero de 2025), Europol desmanteló una plataforma gestionada desde Dinamarca que distribuía CSAM generado por IA, lo que condujo a 25 detenciones, la identificación de 273 sospechosos y la incautación de 173 dispositivos en 19 países.[101]

Aunque muchas víctimas y agresores siguen sin ser identificados, los datos disponibles sobre los casos conocidos sugieren que una proporción significativa de los materiales de abuso sexual infantil y otras formas de abuso facilitadas por la tecnología son producidos por personas conocidas.[102] Los informes de Thorn, basados en datos del NCMEC, muestran que dos de cada tres niños son abusados por alguien de su entorno fuera de Internet.[10,103] Una revisión de 2023 de 66 estudios sobre la producción parental de CSAM destaca que los miembros de la familia son un grupo significativo, pero poco reconocido, en riesgo de cometer delitos, que suelen producir material en el que participan niños prepúberes.[104]

> « Hay un aspecto digital [en el abuso]... se trata de abuso sexual infantil intrafamiliar... los delincuentes... incluso los abuelos utilizan servicios digitales como WhatsApp... chats privados y toman fotos. »
>
> *Sociedad civil*[11]

Niños que muestran comportamientos sexuales perjudiciales

Los comportamientos sexuales perjudiciales entre los niños se reconocen como un problema creciente, aunque su verdadera prevalencia sigue sin estar clara. Antes de los 18 años, uno de cada cinco niños sufre daños sexuales, tanto en línea como fuera de línea, y más de la mitad de estos casos se producen entre compañeros.[105,106] Estos comportamientos pueden comenzar como una exploración relacionada con los compañeros, pero a veces pueden escalar hasta convertirse en delitos más graves. Por ejemplo, un niño puede empezar viendo imágenes sexuales de compañeros de su misma edad y seguir buscando material similar a medida que crece.[9]

Los niños que muestran comportamientos sexuales dañinos suelen compartir vulnerabilidades que se solapan, como haber sido víctimas anteriormente o haber estado expuestos a contenidos sexuales, traumas, negligencia, desigualdad social y neurodiversidad.[107] Estas vulnerabilidades suelen verse agravadas por la falta de concienciación, una educación inadecuada y unos sistemas de prevención y apoyo deficientes.[108] Sin un apoyo oportuno, estos comportamientos pueden perturbar el desarrollo saludable, dañar las relaciones y causar un importante malestar psicológico. El estigma y la exclusión pueden causar un daño adicional, especialmente cuando se etiqueta a los niños como delincuentes en lugar de reconocerlos como niños con necesidades específicas de protección y desarrollo.[107]

Las iniciativas de prevención e intervención existentes se han centrado en gran medida en los adultos autores de estos actos. Las intervenciones centradas en los niños suelen estar integradas en programas más amplios de prevención de la violencia, lo que deja lagunas en la comprensión y la respuesta.[107] La mayoría de las intervenciones comienzan demasiado tarde, después de que el daño ya se ha producido, perdiendo una oportunidad crítica para la prevención.[108] Al pasar por alto que la exploración, la puesta a prueba de los límites y la asunción de riesgos son típicas del desarrollo, las iniciativas de prevención y respuesta a menudo no satisfacen las necesidades de estos niños.[108]

Datos recientes también destacan a los niños que han causado daño en línea, en particular compartiendo imágenes sexuales de otros niños.[80,99,109] Muchos no actúan con la intención de causar daño, sino más bien por aburrimiento, por intentar ser graciosos o por expectativas sobre la masculinidad.[7,99,108] Las niñas son más propensas a sufrir presión para producir contenido sexual, mientras que los niños son más propensos a compartirlo.[99] Los jóvenes pertenecientes a minorías sexuales y de género se enfrentan a un mayor riesgo de chantaje y acoso.[110] Sigue siendo habitual culpar a las víctimas, y las encuestas muestran que casi la mitad de los niños y dos tercios de los cuidadores de Camboya y Filipinas culpan a las víctimas cuando se comparten sus imágenes contra su voluntad.[111] Como compartió un adolescente: «Era bastante popular. En realidad, no afectó su popularidad...Creo que se trata más bien de lo que envió la chica y que el chico realmente no sufre ninguna repercusión.»

Motivaciones y vías hacia la perpetración

Las investigaciones destacan múltiples vías hacia la perpetración de la CSEA facilitada por la tecnología. El alto deseo sexual, el interés sexual por los niños, la neurodiversidad y la desregulación emocional se documentan como factores de riesgo.[94,108] En los datos de las líneas de ayuda, algunos delincuentes informaron de que su propia victimización durante la infancia contribuyó a su posterior comportamiento abusivo, con el trauma actuando como motivador y racionalizador.[52,112]

Los nuevos datos de la encuesta profundizan en la comprensión de estas motivaciones. Un estudio de 2024 realizado con 4.549 delincuentes de la *deep web* oscura reveló que:

- 30 % estaba motivado por el interés sexual en los niños
- 15 % intentaba regular emociones como la soledad o la depresión
- 10,6 % tenía el deseo de comprender su propia experiencia de abuso
- 6,3 % buscaba material que representara su propio abuso.

Cabe destacar que casi el 40 % de los delincuentes declararon haber consumido pornografía para adultos en grandes cantidades antes de pasar al CSAM.[94] Esto concuerda con otros estudios que muestran que los delincuentes suelen empezar consumiendo pornografía para adultos, pero luego comienzan a buscar novedad y «variedad».[95,113] El consumo de pornografía cada vez más violenta o extrema puede derivarse de otros factores problemáticos que impulsan comportamientos sexuales dañinos e interactuar con ellos, lo que refleja un patrón de desensibilización. Se necesitan más investigaciones para comprender estas complejas interacciones y vías de escalada y perpetración.

Las motivaciones económicas son importantes: hay pruebas de que el CSAM se utiliza para impulsar el tráfico de Internet, mientras que delitos como la extorsión sexual, la retransmisión en directo y la trata de personas, a menudo facilitados por la IA generativa, son muy rentables.[2115] Los autores de extorsión sexual financiera a menores suelen residir en países de ingresos bajos y medios, como Nigeria, Filipinas y Costa de Marfil, mientras que las víctimas suelen encontrarse en países de ingresos altos.[116] En 2024, el NCMEC recibió alrededor de 100 denuncias diarias de extorsión sexual financiera a menores, siendo los niños los más afectados.[117] La IWF también informó de que el 91 % de las víctimas de extorsión sexual eran hombres.[117]

> «A menudo se piensa que los delincuentes solo actúan por satisfacción sexual, pero cada vez más la motivación es económica.»
>
> *Industria*[7]

Métodos y tecnologías utilizados para cometer los delitos

Los métodos de perpetración son dinámicos y están determinados por la evolución de las tecnologías. Los delincuentes aprovechan el anonimato, el cifrado y las lagunas de las plataformas para compartir CSAM en la web abierta y oscura.[118] Ocultando el contenido mediante la manipulación de enlaces, redes de distribución de contenido, sitios web *doppelgänger* (enmascarados) e intercambios cifrados en redes sociales para evitar ser detectados y eliminados.[11,119] Los algoritmos también pueden revelar material dañino o conectar a los niños con los delincuentes.

Al mismo tiempo, las herramientas de inteligencia artificial, la tecnología *deepfake* y las aplicaciones «*nudify*» (software que crea imágenes falsas de desnudos o sexualmente explícitas a partir de fotos de personas reales) permiten la producción de imágenes sexuales sintéticas de niños, que pueden utilizarse para coaccionar a las víctimas a producir CSAM reales.[13,118,121] Este patrón suele implicar un primer contacto y captación en las principales redes sociales, plataformas de juegos y mensajería, seguido de un traslado a entornos cifrados o anónimos para intensificar el abuso.[120]

> «Antes solo se encontraba en foros oscuros o en la web oscura... pero en los últimos años se ha producido un enorme aumento de la disponibilidad de [CSAM].»
>
> *Industria*[7]

> «No hay ninguna plataforma segura, los delincuentes utilizan todas las plataformas... cuando les preguntamos dónde contactan con los niños, responden que, por supuesto, en la web abierta, las redes sociales y las plataformas de juegos, donde están los niños. Los niños [pequeños] no están en la deep web.»

Sociedad civil[11]

Prevención

Utilizamos una definición amplia de prevención, que abarca todas las acciones que tienen como objetivo:

1. Evitar que los niños sean objeto de explotación y abuso o que causen daño a otros niños.
2. Prevenir la revictimización y la reincidencia.
3. Reducir las consecuencias perjudiciales para los niños que ya han sufrido abusos y garantizar la rehabilitación de quienes han causado daño.

Esta definición incluye acciones que pueden tener lugar después de que se haya producido el daño, a menudo descritas como prevención terciaria. Si bien estos esfuerzos suelen recibir más atención y recursos, es necesario prestar mayor atención a abordar las causas fundamentales, fortalecer los factores de protección y prevenir el daño antes de que se produzca. Las iniciativas de prevención deben abarcar todos los niveles del entorno del niño, incluidos sus compañeros, familias, comunidades, instituciones y la sociedad en general, y adaptarse a un panorama tecnológico en constante evolución.[30] Las respuestas creativas intersectoriales están demostrando que la prevención es posible, y varias de ellas están dirigidas o inspiradas por los propios niños y supervivientes. Las tecnologías emergentes han introducido nuevos riesgos, pero también ofrecen oportunidades de protección.

Una prevención eficaz comienza por abordar los factores sociales, estructurales y económicos que provocan el daño. Debe tener en cuenta cómo factores como la edad, la orientación sexual y la identidad de género, la discapacidad, la neurodiversidad, el origen étnico, la condición de indígena o migrante, las condiciones socioeconómicas y el nivel educativo se entrecruzan para determinar los riesgos de daño o comportamiento perjudicial de los niños. Los desequilibrios de poder, la pobreza, la baja alfabetización digital y la supervisión parental limitada pueden aumentar los riesgos para los niños.[123,124] Las normas sociales perjudiciales, el estigma, la vergüenza y la culpabilización de las víctimas pueden disuadir de la revelación y la búsqueda de ayuda, mientras que las leyes y la gobernanza débiles permiten que el abuso prospere.[85,91,121] También deben abordarse los factores económicos, como la extorsión sexual financiera y los ingresos procedentes del tráfico y la publicidad en línea. La prevención de la CSEA facilitada por la tecnología también requiere un compromiso político y una inversión sostenida en los sistemas, recursos y procesos que protegen a los niños. Entre los factores clave se incluyen:

- Un compromiso político sostenido y una financiación específica para dar prioridad a la seguridad y el bienestar de la niñez.
- Una gobernanza digital sólida y la rendición de cuentas en todos los niveles del gobierno.
- Investigación y datos para informar la prevención y priorizar los recursos.
- Sistemas sólidos de protección infantil con profesionales capacitados que puedan detectar los riesgos de forma temprana y responder con un apoyo adaptado a los niños, basado en el conocimiento y sensible al trauma.[121]

- Normas sociales favorables que reconozcan que el abuso sexual infantil facilitado por la tecnología se puede prevenir, fomenten la denuncia y promuevan la búsqueda de ayuda para las personas con pensamientos o comportamientos sexuales dañinos.[125]
- Colaboración global e intersectorial para coordinar la prevención, reforzar la rendición de cuentas y armonizar la terminología, las normas sobre datos y los sistemas de seguimiento.

> «Si le das a tu hijo un dispositivo y un teléfono móvil o acceso a Internet... le estarás abriendo la puerta a un entorno social lleno de adultos. ¿Harías eso en tu casa? ¡Acabas de abrir la puerta y decir "bienvenidos, todos"!.»

Sociedad civil[11]

Cerrar la brecha de financiación

> «Veo oportunidades perdidas porque la financiación es muy escasa en este momento, especialmente [con] lo que está sucediendo en el mundo... Todo el mundo está luchando [por] la financiación, por lo que la colaboración no es muy fácil... Deberíamos trabajar más conjuntamente para prevenir estos delitos.»

Sociedad civil[11]

A pesar de la creciente escala y complejidad de la CSEA facilitada por la tecnología, existe una «brecha de financiación global significativa y cada vez mayor» para la prevención, la respuesta y la investigación. Safe Online identifica la falta crónica de financiación como «el mayor obstáculo para lograr un futuro digital seguro, inclusivo y ético para los niños».[126] El desajuste entre las inversiones en prevención y los costes de los daños es evidente. La violencia contra los niños puede costar a los países hasta un 11 % del PIB, superando en algunos casos seis veces el gasto nacional en salud.[126]

En Estados Unidos, se gastan más de 5000 millones de dólares al año en encarcelar a adultos condenados por delitos sexuales contra niños, más de 3.000 veces el presupuesto destinado a la investigación para la prevención del abuso infantil.[127] Los países de ingresos bajos y medios están especialmente infrafinanciados y, a menudo, dependen de una financiación a corto plazo basada en proyectos, en lugar de respuestas nacionales sostenidas.[128] Para cerrar la brecha de financiación se necesitan enfoques innovadores, como la financiación catalítica procedente de fuentes filantrópicas, la cofinanciación de los gobiernos, la inversión sostenida de las instituciones financieras internacionales y otros organismos multilaterales, y mecanismos más sólidos para la financiación a largo plazo. También se necesita financiación para fortalecer los sistemas nacionales que son esenciales para la prevención, incluidos los sistemas de salud, educación, protección infantil, servicios sociales y jurídicos.

Reconociendo la realidad de un entorno de financiación limitado, es esencial utilizar los recursos disponibles de manera más eficiente, coordinando mejor los esfuerzos de prevención entre los distintos sectores, utilizando pruebas y datos para priorizar las inversiones, y adaptando y probando intervenciones basadas en pruebas, incluidas las de la agenda sobre la violencia contra los niños.[9,129] También se necesitan análisis sólidos de la relación costo-beneficio para demostrar que la prevención es más rentable que las respuestas reactivas a la CSEA facilitada por la tecnología.

> «Hay muchos elementos interesantes para... armonizar más el diálogo Norte-Sur, para acercar el mundo académico al ámbito profesional... [pero] lamentablemente creo que el panorama de la financiación no es propicio para mejorar eso.»
>
> *Sociedad civil*[11]

Fortalecimiento de la base empírica para la prevención

Es esencial contar con pruebas sólidas para comprender los riesgos emergentes, evaluar las estrategias de prevención y orientar las inversiones. Un enfoque de salud pública puede guiar este proceso: (1) definir y supervisar el problema y su prevalencia; (2) identificar los factores de riesgo y de protección; (3) diseñar, probar y evaluar estrategias de prevención; y (4) compartir lecciones y ampliar lo que funciona.[123] Para traducir la investigación en una prevención más eficaz se requiere una investigación coordinada y el intercambio de datos entre sectores y países.

La **iniciativa Data for Change**, puesta en marcha en 2022 y en la que ahora participan 120 organizaciones, tiene por objeto cartografiar las buenas prácticas, reducir las barreras al intercambio de datos y dar prioridad a los datos de los países de la mayoría global.[130] La iniciativa hace hincapié en la adaptación de los enfoques a contextos específicos y en la participación de jóvenes investigadores de países de ingresos bajos y medios, con el fin de que los datos mundiales sean más inclusivos y aplicables. El informe de datos de Unicef sobre **la medición de la violencia contra los niños facilitada por la tecnología, en consonancia con la Clasificación Internacional de la Violencia contra los Niños**, impulsa los esfuerzos para mejorar la calidad y la comparabilidad de los datos mundiales.[131]

Para mantenerse informado sobre las tendencias emergentes y las últimas pruebas globales sobre estrategias de prevención eficaces, consulte el apéndice.

> «Es una frase casi automática decir... que necesitamos más datos, pero en algún momento tenemos que reconocer el hecho de que... Si hay más de 500 [estudios sobre la explotación sexual de niños migrantes], es injusto decir que no hay datos. Lo que pasa es que la calidad de los datos es a menudo deficiente.»
>
> *Académico*[8]

Convertir la evidencia en acción para poner fin a la violencia sexual infantil: el marco global de revisión sistemática viva y conocimiento basado en la práctica del Safe Futures Hub

Lanzado en septiembre de 2023, el Safe Futures Hub está codirigido por la Iniciativa de Investigación sobre la Violencia Sexual (SVRI), Together for Girls y WeProtect Global Alliance.[132-135] Su misión es poner fin a la violencia sexual infantil promoviendo soluciones basadas en datos, pruebas, conocimientos de los profesionales y enfoques dirigidos por la comunidad.

A principios de 2026, el Safe Futures Hub, junto con la Universidad de Oxford, lanzará la **revisión sistemática** global **Living Systematic Review**, un recurso actualizado que sintetiza las pruebas sobre lo que funciona para prevenir la violencia sexual infantil. La **Living Systematic Review** aplica métodos rigurosos y transparentes para identificar, evaluar y resumir los estudios de intervención emergentes, garantizando que los responsables políticos, los profesionales y los investigadores tengan acceso a las pruebas más actuales. A diferencia de las revisiones estáticas, esta evaluación en tiempo real tiende un puente entre la investigación y la práctica. Basándose en el informe de pruebas **Building Safe Futures** 2024 y su llamamiento a una acción más firme y basada en pruebas, este recurso orientará las inversiones hacia estrategias eficaces y contextualmente relevantes. Al destacar las intervenciones que funcionan, **la revisión sistemática viva** del Safe Futures Hub permitirá a las partes interesadas ampliar y adaptar las soluciones que protegen a los niños de la violencia sexual.

En diciembre de 2025, el Safe Futures Hub lanzará dos nuevos recursos para reforzar el reconocimiento y el uso del conocimiento basado en la práctica (PbK) en la prevención y la respuesta a la violencia sexual infantil.

- El documento de referencia explica qué es el PbK y por qué es importante para prevenir y responder a la violencia sexual infantil, mostrando cómo dar voz a los grupos infrarrepresentados, refuerza la práctica y valora tanto la experiencia de los profesionales como la experiencia vivida.
- El marco de orientación ofrece herramientas y procesos prácticos para ayudar a los profesionales a recopilar, utilizar y compartir el PbK de forma segura, ética y práctica.

En el contexto de la prevención y la respuesta a la violencia sexual infantil, el PbK se refiere a los conocimientos generados a través de la experiencia vivida y la participación directa en programas, servicios o iniciativas de promoción. Mientras que la investigación muestra *lo que* funciona, el PbK explica *cómo* funciona, por qué funciona y cómo mantenerlo en funcionamiento en contextos complejos y cambiantes. Juntos, el PbK y la investigación pueden hacer que las estrategias sean más eficaces, pertinentes y basadas en contextos del mundo real.

Diseño del marco de prevención

A lo largo de las consultas, ha surgido un mensaje unificador: tenemos que actuar ahora. Es necesario comprender la magnitud y la naturaleza de la CSEA facilitada por la tecnología, pero no es suficiente. La persistente pregunta —«¿por dónde empezamos?»— se convirtió en el motor que impulsó la creación de este marco de prevención: una guía concreta para transformar la preocupación compartida en acción coordinada.

El marco de prevención se desarrolló para complementar la Respuesta Nacional Modelo de la Alianza Global WeProtect, que proporciona una estructura para la acción a nivel nacional y sistémico. Juntos, guían la acción global para abordar la CSEA facilitada por la tecnología.[29] El marco también se basa en otros modelos bien establecidos:

- El modelo socioecológico, que destaca que los riesgos y las protecciones existen en múltiples niveles del entorno del niño.[30]

- El enfoque de prevención de la salud pública, que define la prevención en diferentes niveles, desde enfoques para toda la población hasta medidas específicas para personas en riesgo de sufrir o causar daños.[123]

El marco también se basa en las normas internacionales y regionales sobre los derechos del niño, incluida la Convención de las Naciones Unidas sobre los Derechos del Niño y las Observaciones generales 16, 24 y 25, así como el Pacto Digital Global.[24,33,136] Se creó de forma conjunta mediante un proceso participativo en el que intervinieron jóvenes, supervivientes y un comité directivo de expertos que representaba a gobiernos, la sociedad civil, la industria y organismos intergubernamentales. Las partes interesadas contribuyeron a través de talleres y comentarios por escrito.

> **«Cuando realizamos esfuerzos de prevención, creo que debemos involucrar a todas las partes interesadas: supervivientes, personas con amplia experiencia, industrias tecnológicas, instituciones religiosas, líderes comunitarios, profesores, padres, mentores juveniles, ONG, sociedad civil e incluso organismos regionales como la Unión Africana, la ONU o la Interpol.»**
>
> *Sociedad civil[11]*

El marco de prevención se organiza en torno a cuatro áreas de acción interrelacionadas:

- Participación y liderazgo infantil
- Educación y apoyo comunitarios
- Seguridad digital
- Ley, política y justicia

El orden en que se presentan refleja un enfoque socioecológico, que comienza con los niños y avanza hacia la comunidad, las instituciones, los gobiernos y los actores globales. Las áreas de acción se distribuyen en tres niveles de prevención: primaria (protección proactiva), secundaria (detección y prevención del daño) y terciaria (respuesta y apoyo tras el abuso). Los facilitadores, como la investigación y la financiación, son fundamentales y deben abordarse de forma continua para garantizar que todas las acciones sean eficaces y sostenibles.

En lugar de clasificar las intervenciones según la solidez de las pruebas, lo que aún no es posible, este marco presenta recomendaciones temáticas para ayudar a las partes interesadas a identificar las medidas de prevención pertinentes para su contexto y experiencia. El marco destaca los enfoques basados en pruebas, cuando están disponibles, y señala las recomendaciones de los expertos, las buenas prácticas y las prácticas innovadoras que necesitan una evaluación más profunda.

> **«Ahora se requiere un enfoque de salud pública, con el establecimiento de un sistema para prevenir la perpetración, detectar y abordar los delitos, pero también para apoyar a las víctimas y sus familias.»**
>
> *Académico[8]*

Opiniones de expertos sobre las prioridades en materia de prevención extraídas de la Evaluación Global de Amenazas 2025

Nuestra encuesta en línea a 77 profesionales que trabajan para combatir el abuso sexual infantil facilitado por la tecnología (61 % sin ánimo de lucro, 19 % gubernamental, 16 % industrial y 3 % organismos estatutarios independientes) confirmó un fuerte apoyo a las cuatro áreas de acción. Los encuestados pidieron una comprensión más profunda del comportamiento, las motivaciones y los perfiles de los autores (47 %); las causas fundamentales y los factores sistémicos que impulsan el daño (45 %); y las perspectivas de los niños sobre el uso de la tecnología (39 %). Las principales prioridades identificadas para ampliar los esfuerzos de prevención fueron la financiación flexible a largo plazo (87 %), la formación y el apoyo técnico para el personal (58 %) y el acceso a herramientas y orientación de código abierto centradas en los niños (50 %).

Aunque se basan en una pequeña muestra de expertos, estas ideas reflejan un amplio consenso sobre las prioridades en materia de prevención y la urgente necesidad de inversión, desarrollo de capacidades y colaboración.

Poner en práctica la prevención: el modelo del queso suizo

El modelo del queso suizo ofrece una perspectiva muy útil para comprender cómo se puede aplicar este marco de prevención en la práctica.[137] Ampliamente utilizado en campos críticos para la seguridad, como la aviación, la medicina y la ingeniería, el modelo hace hincapié en que los daños graves rara vez se deben a un único punto de fallo. En cambio, los daños se producen cuando se alinean múltiples debilidades en los sistemas de protección. Cada «loncha» de queso suizo representa una capa de protección, por ejemplo, medidas de seguridad digital o leyes, políticas y mecanismos judiciales. Cada loncha tiene «agujeros» que representan puntos débiles. Un solo agujero puede no causar daños porque otras capas actúan como barrera, pero cuando los agujeros de varias capas se alinean, pueden producirse daños graves.

Aplicado al abuso sexual infantil facilitado por la tecnología, el modelo del queso suizo subraya tres ideas importantes:

- Cada vez que un niño sufre daños por CSEA facilitada por la tecnología, esto refleja un fallo del sistema y múltiples oportunidades perdidas para intervenir.
- Ningún actor o sector tiene por sí solo todas las soluciones. Las múltiples capas de prevención deben funcionar conjuntamente.
- La prevención requiere un aprendizaje y una adaptación continuos para identificar dónde existen debilidades en la protección, cuán graves y urgentes son las posibles consecuencias y qué recursos están disponibles para abordar las deficiencias o reforzar otras capas de protección.

Utilizados conjuntamente, el marco de prevención y el modelo del queso suizo proporcionan estructura y método. Mientras que el marco de prevención abarca todas las formas de CSEA facilitadas por la tecnología, el modelo del queso suizo puede ayudar a las partes interesadas a priorizar las acciones, evaluar los riesgos e identificar las debilidades que contribuyen a un incidente o tipo de daño concreto. Juntos, cambian el enfoque de soluciones aisladas a la creación de sistemas resilientes con múltiples capas de protección para mantener la seguridad de los niños.

Escenario: Amal está en el instituto. Recientemente ha roto con su pareja, que tiene la misma edad que ella. Para vengarse, su pareja publicó fotos íntimas de Amal en Internet y otras personas las difundieron en su colegio. Lo que le sucedió a Amal fue el resultado de fallos a varios niveles. Así es como sucedió desde su perspectiva.

Figura 4 . Visualización del modelo del queso suizo: comprensión de los riesgos en los contenidos sexuales generados en los que participan niños

Participación y liderazgo infantil

- Compañeros de apoyo capacitados para recibir denuncias y poner a los niños en contacto con los servicios de apoyo.
- Diseño de materiales educativos y de sensibilización, canales de denuncia y funciones de seguridad digital dirigidos por niños y supervivientes.

Educación y apoyo comunitarios

- Programas escolares sobre relaciones saludables, sexualidad y seguridad digital.
- Apoyo temprano para la niñez en riesgo de sufrir daños o de causar daños.
- Formación de educadores y políticas escolares claras para la prevención y la respuesta.
- Campañas de sensibilización de la comunidad para cambiar las normas, reducir la culpabilización de las víctimas y fomentar la denuncia.

Seguridad digital

- Evaluaciones del impacto en los derechos del niño y funciones de «seguridad por diseño» durante el desarrollo de la plataforma (por ejemplo, detección de desnudos, ventanas emergentes con advertencias sobre el contenido que interrumpen el intercambio de contenido peligroso y animan a buscar ayuda).
- Opciones de denuncia accesibles que proporcionen información oportuna, enlacen con servicios de apoyo y eliminen rápidamente los contenidos o cuentas perjudiciales.

Leyes, políticas y justicia

- Leyes que respeten los derechos, protejan a las víctimas y eviten criminalizar los comportamientos consentidos entre personas de edades similares.
- Organismos reguladores facultados para supervisar el cumplimiento de la industria, investigar los abusos e imponer sanciones.
- Justicia adaptada a los niños y acceso a la reparación a través de policías, jueces y fiscales capacitados.

Áreas de acción preventiva

Participación y liderazgo infantil

> «Las voces de los niños deben ser escuchadas en todas las etapas de la prevención, la detección y la respuesta.»

Superviviente, Filipinas[138]

Los niños y los supervivientes tienen derecho a compartir sus opiniones e influir en las políticas, los programas y los servicios que les afectan mediante una participación segura y significativa.

Las alianzas con organizaciones dirigidas por la niñez y centradas en ella pueden promover una participación segura, detectar riesgos y daños tempranos e informar sobre intervenciones eficaces y centradas en ellos y ellas.

Se deben realizar esfuerzos para involucrar a toda la niñez, en particular a quienes provienen de entornos marginados, reconociendo que los niños corren el riesgo tanto de sufrir daños como de causarlos a otros niños.

Principios para una participación segura y significativa

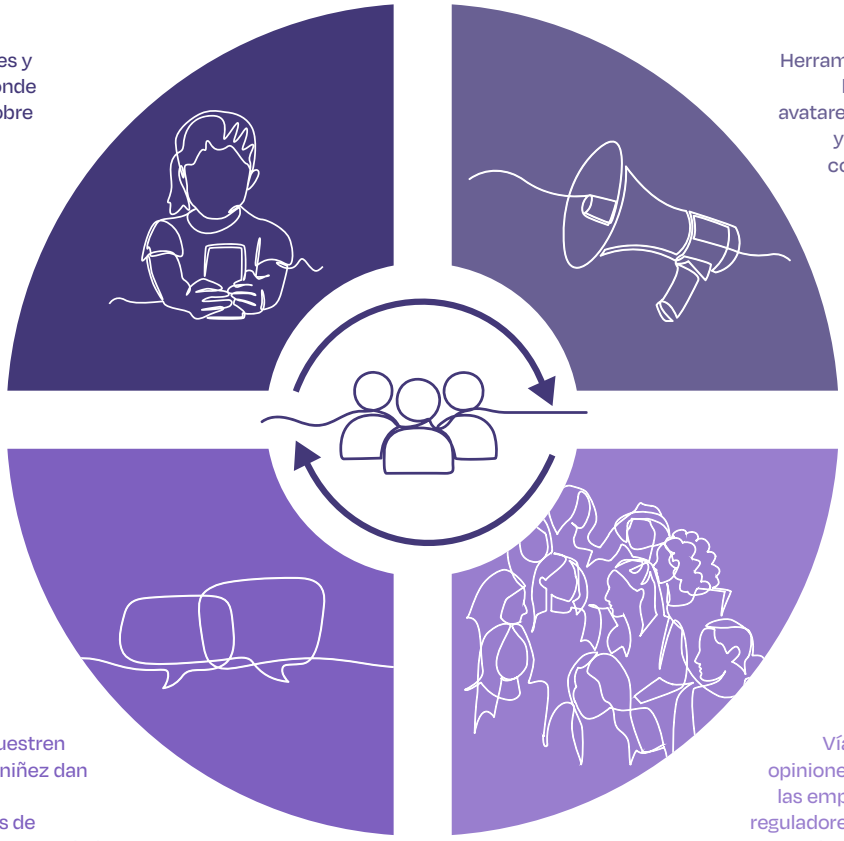
> «Ellos [los niños] son las personas más vulnerables y las más necesarias para resolver el problema.»

Superviviente, Filipinas[138]

El artículo 12 de la Convención de las Naciones Unidas sobre los Derechos del Niño afirma el derecho de todos los niños a estar informados, expresar sus opiniones y participar en las decisiones que afectan a todos los aspectos de sus vidas.[33] El **modelo Lundy** (véase la figura 5) proporciona un marco práctico para aplicar el artículo 12 con el fin de apoyar la participación significativa de los niños.[139] Los niños y los jóvenes pueden ayudar a identificar los riesgos emergentes y a informar sobre estrategias de prevención proactivas. Como parte de una campaña llevada a cabo en Indonesia, Nepal y Filipinas, la organización de defensa de los derechos del niño Kindernothilfe elaboró una

guía y **un conjunto de herramientas** para apoyar la participación significativa de la niñez y la juventud en la promoción de la prevención y la protección contra la violencia en línea.[140,141] Unicef ha elaborado **una guía destacada** en la que se comparten las mejores prácticas para involucrar a la niñez en las evaluaciones del impacto de los derechos digitales de los niños.[142]

Figura 5. Características de la participación significativa aplicadas en línea[143]



ESPACIO
Foros seguros, accesibles y adaptados a la niñez, donde estos puedan debatir sobre los riesgos digitales.

VOZ
Herramientas adecuadas para la edad, como sondeos, avatares, encuestas anónimas y medios creativos, para conocer las experiencias de los niños en línea

INFLUENCIA
Enlaces visibles que muestren cómo los aportes de la niñez dan lugar a mejoras, como herramientas eficientes de denuncia, funciones de privacidad más sólidas o programas de prevención en las escuelas.

AUDIENCIA
Vías directas para que las opiniones de los niños lleguen a las empresas tecnológicas, los reguladores, las fuerzas del orden y los responsables políticos

La seguridad, la calidad y el interés superior de la niñez deben ser siempre prioritarios cuando se trabaja con ellos y ellas. La participación de los niños solo debe llevarse a cabo cuando se disponga de personal adecuado, medidas de protección y servicios de apoyo que tengan en cuenta los traumas para protegerlos de cualquier daño. Si esto no es posible, se debe recurrir a las opiniones de los jóvenes, los adultos y las organizaciones que pueden representar los puntos de vista de la niñez, así como a las pruebas, investigaciones y buenas prácticas existentes.

Involucrar a la niñez y a los supervivientes en la prevención

> «Creo que las ONG creadas por jóvenes y para jóvenes serán de gran ayuda. Estas organizaciones podrían concienciar de una forma más cómoda, ya que los consejos provendrían de otros jóvenes.»

Hombre de 17 años, Pakistán[60]

Entre las iniciativas que involucran a los niños y jóvenes para informar sobre la prevención se incluyen:

- **Mtoto News**, una plataforma digital y mediática con sede en Kenia que facilita la defensa de los derechos de la niñez y permite a más de 100 000 niños y niñas interactuar directamente con sus líderes sobre cuestiones como el abuso sexual infantil en línea y fuera de línea.[144]
- **El Índice de Bienestar Digital** de la Fundación Snap, que involucra a jóvenes de seis países para que compartan sus opiniones sobre su bienestar psicológico y sus experiencias en plataformas en línea, revelando información importante para la prevención.[45]
- **BeSmartOnline**, el centro oficial para una Internet más segura del Gobierno de Malta, que cuenta con la orientación de un panel de jóvenes que ayuda a identificar nuevos riesgos en línea y a diseñar conjuntamente estrategias eficaces de sensibilización.[145,146]

Liderazgo juvenil en seguridad en línea: ideas de VoiceBox

VoiceBox es una empresa social y plataforma de contenidos con sede en el Reino Unido y dirigida por jóvenes que ayuda a los creadores de entre 13 y 25 años a prosperar y a configurar entornos digitales más seguros que se centran en sus experiencias vividas.[147] Con una red global que abarca más de 50 países, VoiceBox amplifica perspectivas diversas y, a menudo, puede identificar los riesgos emergentes en línea más rápidamente que la investigación tradicional, lo que le permite actuar como un «sistema de alerta temprana» para los responsables políticos y los líderes del sector. Esto garantiza que los responsables de la toma de decisiones dispongan de información en tiempo real, basada en las opiniones de los jóvenes, sobre las amenazas en constante evolución.

VoiceBox recopila información honesta y sin filtros de los jóvenes sobre los complejos retos de la seguridad en línea, incluyendo la alfabetización mediática, los daños en línea y los riesgos digitales emergentes. Su enfoque combina oportunidades de liderazgo para los jóvenes con un fuerte apoyo basado en la protección y el conocimiento de los traumas. VoiceBox utiliza grupos de discusión dirigidos por compañeros, entrevistas y métodos creativos de recopilación de información (como el arte, los videos y la poesía) para que los jóvenes puedan compartir sus experiencias de forma segura y auténtica. Este enfoque ha arrojado luz sobre cuestiones como los agentes de IA y las plataformas por suscripción.[44]

La niñez que sufren discriminación interseccional, como las poblaciones de minorías sexuales y de género, y niños y niñas con discapacidades, se enfrentan a riesgos y daños únicos en Internet, pero a menudo se les excluye de las políticas y los programas.[11]

> «Si no se tienen debidamente en cuenta en el diseño de las interacciones y las políticas, corremos el riesgo de dejar de lado a esta población infrarrepresentada.»
>
> *Sociedad civil*[11]

Es importante consultar a los niños marginados y a aquellos con necesidades específicas que pueden navegar por las tecnologías digitales de forma diferente a sus compañeros.[8] Por ejemplo, los niños sordos, que a menudo dependen de la comunicación por video, se enfrentan a riesgos únicos en Internet y pueden tener menos oportunidades de reconocer o denunciar posibles explotaciones.[11] Garantizar estrategias de comunicación accesibles, personalizadas e inclusivas es fundamental para apoyar su seguridad en Internet. A continuación, se destacan algunos ejemplos de iniciativas dirigidas por supervivientes y basadas en su experiencia:

- **Disrupting Harm** genera pruebas de alta calidad sobre los daños digitales que sufren los niños y los jóvenes en 25 países de 6 regiones. El proyecto utiliza procesos participativos basados en el trauma, siguiendo estrictas directrices éticas y procedimientos de protección infantil. La primera fase reveló que casi uno de cada tres niños no revelaba los daños y casi la mitad afirmaba que no sabía a quién contárselo ni dónde buscar ayuda.[10] En 2025 se completó una segunda ronda de entrevistas en profundidad con más de 100 jóvenes supervivientes de América Latina, Europa del Este y Oriente Medio, cuyos resultados se darán a conocer próximamente.
- **Global Boys Initiative** documenta las experiencias de niños sometidos a explotación y abuso sexual en diez países, destacando las barreras para la revelación, la denuncia y el acceso a los servicios.[148]
- **Our Voice Male Survivors** (Supervivientes masculinos) proporciona uno de los mayores conjuntos de datos sobre niñez que han sido víctimas de abusos sexuales. Muestra patrones distintivos, como un inicio más temprano, diferentes perfiles de agresores y retrasos más prolongados antes de la denuncia, lo que subraya la necesidad de investigaciones y servicios sensibles al género.[114]
- **Secrets Worth Sharing** es una plataforma que ofrece recursos basados en el trauma que reconocen la diversidad de experiencias de los supervivientes. Ofrece talleres, podcasts y videos centrados en los supervivientes que tratan temas como el abuso sexual infantil, la interseccionalidad en el trauma y niños y niñas que muestran comportamientos sexuales dañinos.[149] Como compartió el fundador:

> «Una cosa que hacemos de manera diferente como organización es producir recursos en línea específicos para diferentes factores de identidad, como ser un hombre negro, o queer, o hablar otro idioma. Mi mayor compromiso con los adolescentes y los jóvenes es sobre las sugerencias para estos episodios [de podcast y video]. Creo que esto se debe a que los niños y los jóvenes no quieren verse solo como supervivientes o víctimas, sino que están interesados en cómo sus experiencias son únicas en función de sus propias identidades.»
>
> *Sociedad civil*[150]

Educación y apoyo comunitarios

> Para promover la educación y la colaboración digitales, no solo hay que centrarse en las herramientas de seguridad, sino también en dotar a los niños y adolescentes de los conocimientos y habilidades necesarios para navegar de forma segura y responsable. Involucrar a los padres, los educadores y los propios jóvenes en la creación de entornos digitales más seguros y positivos.

Hombre de 18 años, Nicaragua[60]

Las iniciativas de educación y sensibilización deben tratar de cambiar los comportamientos y promover la denuncia y la búsqueda de ayuda. Deben basarse en pruebas, adaptarse al contexto, ser accesibles para todos la niñez y coordinarse entre los distintos sectores para garantizar unas funciones claras y unos mensajes coherentes y eficaces.

La niñez necesita múltiples vías fiables para denunciar sus preocupaciones, buscar ayuda y acceder a servicios de apoyo centrados en los supervivientes, como líneas de ayuda, canales de denuncia formales, compañeros de apoyo capacitados y adultos de confianza.

Se deben poner a disposición de la niñez en riesgo de sufrir daños, así como de los niños y adultos en riesgo de causar daños, intervenciones tempranas basadas en pruebas.

Los mensajes disuasorios y las advertencias deben adaptarse a las diferentes personas en riesgo de causar daños y combinarse con vías inmediatas de apoyo para los pensamientos y comportamientos sexuales dañinos.

Campañas de educación y sensibilización

> Tenemos que educar tanto a los niños como a los padres sobre la seguridad en Internet... Creo que la mayoría de la gente piensa que no tiene a quién acudir [en busca de ayuda] porque es en Internet... Los padres también deben recibir más formación sobre cómo manejar estas situaciones. Y las leyes podrían ser más estrictas, especialmente en mi país, donde nunca he oído hablar mucho de estas cosas.

Mujer de 14 años, Etiopía[60]

Las iniciativas de educación y sensibilización son fundamentales para la prevención. Estos esfuerzos deben ir más allá de la simple sensibilización para impulsar un cambio real en el comportamiento y garantizar el acceso a la ayuda.[9]

Expertos de todos los sectores, así como defensores de los jóvenes y supervivientes, destacaron que las iniciativas eficaces de educación y sensibilización deben:

- Estar basadas en la información proporcionada por los niños y los supervivientes, o desarrollarse juntamente con ellos, tener en cuenta los traumas y ser sensibles al contexto.
- Evitar mensajes basados en el miedo o el estigma que disuadan de denunciar y buscar ayuda.
- Ser inclusivas y accesibles. Deben impartirse en varios idiomas, formatos y lugares, incluidas las escuelas y otros espacios físicos y digitales donde los niños aprenden y se relacionan. Se deben realizar esfuerzos para llegar a los grupos marginados, incluidos los niños con discapacidades, los niños que no asisten a la escuela y los que viven en zonas rurales o en contextos educativos frágiles.
- Dotar tanto a los niños como a los adultos —incluidos los cuidadores, los educadores y los proveedores de servicios— de los conocimientos y habilidades necesarios para prevenir, reconocer y responder a la explotación y el abuso sexuales, tanto en línea como fuera de línea. Esto debe incluir información sobre las leyes pertinentes, cómo denunciar las preocupaciones, dónde buscar ayuda y cómo apoyar a los niños y a los compañeros, y evitar causar daño.
- Ser coordinada y sostenida, con funciones claras en las escuelas, las familias, las comunidades, la industria y el gobierno para garantizar un mensaje coherente y eficaz.
- Ser adecuada para la edad y la etapa de desarrollo de los niños, y tener una programación estratégica (por ejemplo, antes de que un niño reciba su primer teléfono o empiece a conectarse a Internet sin supervisión).

Algunos supervivientes y defensores de los jóvenes expresaron su preocupación por el hecho de que la educación pueda tener dificultades para seguir el ritmo de los riesgos asociados a las tecnologías en rápida evolución (por ejemplo, la realidad extendida) y que los entornos educativos formales puedan resultar intimidantes o inseguros para que los niños hablen de temas delicados. Esto pone de relieve la necesidad de involucrar a los niños en la identificación de los riesgos y en la configuración de las iniciativas de educación y sensibilización.

> **«Habrá muchos niños que no querrán participar en algo así [la educación escolar] porque sigue siendo un tema tabú y habrá niños que tengan miedo de decir algo y de expresarse.»**
>
> *Superviviente*[77]

> Los padres, especialmente los recién llegados, pueden no tener las habilidades lingüísticas o los conocimientos tecnológicos necesarios para mantenerse al día [con los riesgos asociados a las nuevas tecnologías]. Los recursos... deberían enseñar seguridad en las redes sociales, o las escuelas deberían enviar materiales en varios idiomas para educar a los padres.

Defensor de los niños, Canadá[38]

Los programas de prevención del abuso sexual infantil están respaldados por pruebas, aunque las pruebas de los programas que abordan los riesgos relacionados con la tecnología aún son limitadas y están en desarrollo.

- **El programa Tackling Online Child Sexual Exploitation (TOCSE)** aborda la violencia en línea a nivel individual, comunitario, industrial y sistémico en Vietnam. Involucra a los niños en consultas participativas, en el diseño de materiales basados en la información proporcionada por la niñez y en iniciativas dirigidas por niños en las escuelas.[153,154] TOCSE ha proporcionado educación y formación profesional a más de 18 000 niños de 12 años o más y a 11 000 padres y profesores, además de reforzar las líneas de ayuda y los servicios de apoyo a los niños.[153,154]
- El informe de Unicef sobre programas de crianza se basa en una rápida síntesis de pruebas y en consultas con más de 50 expertos de múltiples sectores para identificar las consideraciones clave para diseñar intervenciones que apoyen a los padres y cuidadores en la prevención y la respuesta a la CSEA facilitada por la tecnología.[155]

> Creo que debería haber más lecciones y talleres en las escuelas sobre la explotación infantil o el abuso sexual en línea... Creo que fácilmente podría haber sido víctima de ello. Pero ahora que he asistido a algunos talleres, sé más sobre cómo los traficantes victimizan a las personas y cómo eligen a las víctimas... Por eso, creo que educar a los estudiantes sobre... cómo los traficantes eligen a las víctimas realmente evitaría que se convirtieran en víctimas de la trata.

Defensor de los niños, Canadá[38]

> Se necesita más educación sobre qué evitar y por qué evitarlo. Los niños no escuchan cuando solo se les dice que no hagan algo. Es mejor darles una educación paso a paso y explicarles las partes incómodas de por qué algo está mal, para que sepan que no deben hacerlo.

Defensor de los niños, Kenia[38]

Las campañas de sensibilización pública eficaces pueden cambiar comportamientos y reforzar la idea de que el abuso sexual infantil en línea se puede prevenir. También pueden reducir el estigma que rodea a la denuncia, la búsqueda de justicia y la búsqueda de ayuda para los pensamientos y comportamientos sexuales dañinos. Por ejemplo, tras la campaña de sensibilización sobre la extorsión sexual « » (No es un juego) de la Agencia Nacional contra el Crimen del Reino Unido, la proporción de encuestados que afirmaron que compartirían imágenes explícitas en una situación de extorsión disminuyó significativamente.[156] Del mismo modo, los datos de la IWF muestran que, tras una campaña sobre la distribución no consentida de imágenes íntimas, aumentó el uso de la herramienta **«Report Remove»**, aunque la campaña no promocionaba específicamente dicha herramienta.[157] Sin embargo, el contenido, la calidad y la eficacia de las campañas varían, y pocas iniciativas se evalúan formalmente. Entre los ejemplos recientes de campañas de sensibilización se incluyen:

- **Help Children be Children** en Uganda y Zambia, que combinó campañas de sensibilización con el fortalecimiento de la capacidad de las líneas directas y las fuerzas del orden. Las campañas dieron lugar a un aumento de las denuncias y a una mejora de los conocimientos del personal de las líneas directas.[157]
- **Beware the Share**, de la UNODC, campañas interactivas en idiomas locales que informaron al público sobre el grooming, el sexting y el abuso basado en imágenes en cinco países del sudeste asiático.[158]
- En respuesta a un estudio que reveló que el 70 % de los padres de Nepal desconocían los riesgos y los daños del abuso sexual infantil en línea, ChildSafeNet se asoció con TikTok para impartir formación sobre seguridad digital a niños, padres y educadores en siete distritos de Nepal.[159]

« Creo que todo el mundo debería recibir formación desde una edad muy temprana sobre el uso y el mal uso de las tecnologías digitales y, si surgen problemas, sobre cómo abordarlos. Y, en ambos casos, la familia, los amigos y todas las personas deberían ser conscientes de ello. »

Mujer de 19 años, Nepal[38]

Comportamiento responsable con los jóvenes y los niños (RBYC): promover el desarrollo de normas sexuales saludables y abordar el abuso por parte de compañeros de edad similar

Desarrollado por expertos en prevención del abuso sexual infantil y la violencia escolar de MOORE | Prevención del abuso sexual infantil, Escuela de Salud Pública Bloomberg de la Universidad Johns Hopkins.

RBYC es un plan de estudios escolar basado en pruebas para niños de 11 a 14 años que tiene como objetivo prevenir comportamientos sexuales problemáticos y ayudar a los adolescentes a desarrollar interacciones seguras y apropiadas, tanto con niños más pequeños como con sus compañeros y adultos, tanto en línea como fuera de línea.[74] El programa consta de cinco sesiones interactivas apoyadas por vídeos animados y debates en el aula.[74]

Una alta proporción de los abusos sexuales a menores son perpetrados por otros niños y adolescentes. La adolescencia temprana es una etapa crítica del desarrollo, en la que los jóvenes están formando su identidad y sus normas sexuales, y pueden carecer de las habilidades o los conocimientos necesarios para manejar de forma segura las relaciones que están surgiendo.[160,161] **RBYC** aborda estas carencias mediante un enfoque basado en las fortalezas y que tiene en cuenta el trauma. El plan de estudios puede impartirse como un programa independiente o integrarse en los planes de estudios existentes sobre salud, educación sexual o prevención de la violencia. Las sesiones abarcan:

- Relaciones saludables y toma de decisiones
- Límites personales y consentimiento
- Diferencias de desarrollo entre adolescentes y niños más pequeños
- Comportamientos responsables e irresponsables tanto en contextos en línea como fuera de línea
- Identificación y prevención de comportamientos sexuales problemáticos
- Adultos y amigos seguros

El programa RBYC incluye materiales para llevar a casa destinados a las familias y componentes centrados en los adultos para educadores y padres/cuidadores, con el fin de fomentar la comunicación abierta y reforzar los mensajes de prevención en el hogar y en la escuela.

Un ensayo controlado aleatorio con 160 estudiantes en los Estados Unidos reveló que los niños que participaron en **el RBYC** demostraron un aumento significativo en la autoeficacia para prevenir el daño sexual y mejoraron sus conocimientos sobre las diferencias de desarrollo, el consentimiento y los comportamientos sexuales problemáticos en comparación con los que no recibieron el plan de estudios.

Más allá de su ensayo en Estados Unidos, **el RBYC** se está ampliando y adaptando a nivel mundial. El programa se ha adaptado para su uso en Alemania (con un ensayo controlado aleatorio en curso en 24 escuelas) y en Filipinas (llegando a 250 estudiantes como parte de programas de prevención combinados).[162] En colaboración con el Instituto Kennedy Krieger, **el RBYC** también se ha adaptado para adolescentes neurodiversos y se ha mejorado con videos educativos para aumentar la accesibilidad y la participación. [8]

Contenido sexual en el que participan niños

> «Los niños van a hacer esto [sexting] en el contexto de las relaciones de pareja, y ¿cómo conseguimos que lo hagan de una manera que no les persiga en el futuro?».

Sociedad civil[11]

Compartir imágenes íntimas puede ser una parte normal de las relaciones adolescentes. Sin embargo, la distribución y la criminalización de este tipo de contenido puede causar daño, especialmente cuando las leyes y políticas no distinguen entre el material sexual infantil producido por adultos y las imágenes compartidas por los niños y las niñas. Las pruebas demuestran que los enfoques basados en el miedo o la abstinencia total suelen ser ineficaces y pueden desalentar la denuncia y la búsqueda de ayuda.[163]

> «Había un trabajador social y un agente de policía que nos hablaban de ello y decían que... si envías tus propias fotos desnuda, eso sigue siendo distribución de pornografía infantil, así que... Estoy bastante segura de que la mitad de la gente que estaba allí había enviado fotos desnudas... Probablemente pensaban: "Oh, hay un agente de policía ahí mismo y me va a arrestar en medio del gimnasio"».

Mujer de 17 años[164]

Leaked: contenido sexual autogenerado por menores en Tailandia

- Los jóvenes suelen compartir y encontrar contenido sexual en Internet y describen principalmente el daño como algo que ocurre cuando pierden el control sobre el contenido.
- Los enfoques basados en la educación sexual pueden ser más eficaces que las advertencias severas y las amenazas contra cualquier tipo de intercambio de contenido sexual.

Leaked es una colaboración de tres años entre el Proyecto HUG, una ONG con sede en Chiang Mai, y la empresa de investigación Evident, con sede en Bangkok, que cuenta con el apoyo de la Fundación World Childhood.[165,166,167] Esta iniciativa se propuso comprender mejor cómo los jóvenes de Tailandia interactúan con los contenidos sexuales autogenerados y cómo los interpretan. Incluye una encuesta representativa de la población realizada a 1916 jóvenes de entre 9 y 17 años en escuelas del norte de Tailandia, así como entrevistas en profundidad con expertos interesados. Los conocimientos derivados del análisis de los datos constituirán la base para diseñar nuevos planes de estudio adaptados, que se implementarán en la fase final del proyecto.[110]

Más de uno de cada tres jóvenes (36 %) afirmó haber recibido o visto imágenes sexuales de alguien que creía que era menor de 18 años. Las motivaciones para compartir contenido sexual eran variadas. Muchos creían que el contenido se compartía para ganar «me gusta» y seguidores (46 %), para ganar dinero, regalos o crédito (45 %), para sentirse bien consigo mismos (40 %) o para demostrar confianza en una relación (27 %).[110] Un joven explicó:

> **«Algunos de mis amigos y conocidos más jóvenes también han compartido imágenes de desnudos. Cuando les pregunté por sus motivos, me dijeron que buscaban aceptación. Se sentían seguros de sus cuerpos, pero no habían considerado plenamente las posibles consecuencias. Estas personas tienen talento, pero carecen de espacio y oportunidades suficientes para expresarse. Como resultado, se involucraron en este comportamiento como una forma de llamar la atención.»**

Informante clave de 18 años[110]

Una proporción notable de los encuestados (34 %) creía que los jóvenes comparten contenido sexual porque se ven presionados, engañados o coaccionados. Los jóvenes también describieron cómo la tecnología facilita demasiado el intercambio impulsivo de imágenes sexuales explícitas, al tiempo que ofrece poco apoyo cuando surgen problemas.[110]

Es fundamental destacar que el proyecto **Leaked** hace hincapié en que los daños identificados por los jóvenes no se derivan del hecho de compartir contenido íntimo en sí, sino de perder el control sobre él. El intercambio no deseado de imágenes sexuales generadas en primera persona se reveló como la principal preocupación de los jóvenes (81 %), seguida del arrepentimiento (76 %), el acoso (70 %) y el malestar emocional (68 %).[110] Esta evidencia desafía los enfoques tradicionales basados en el miedo, que se basan en advertencias severas y amenazas legales para desalentar el intercambio de cualquier contenido sexual. Estos mensajes no reflejan la realidad de la vida de los jóvenes y, de hecho, pueden empeorar el estigma o disuadirles de buscar ayuda. En cambio, los datos de **Leaked** respaldan un enfoque que aboga por:

- Una educación sexual integral basada en los derechos que reconozca la realidad de la tecnología en las interacciones sexuales modernas.
- Características de seguridad más sólidas en las plataformas para proteger a la niñez de contenidos sexualizados, sensacionalistas o perjudiciales.
- Cambios culturales —del castigo al apoyo— en la respuesta a los problemas derivados de los contenidos sexuales autogenerados.
- Espacios libres de juicios para dialogar abiertamente con los jóvenes sobre cómo tomar decisiones en línea.

> **«Creo que deberíamos intentar comprender su situación y no culpar a las víctimas. Como esto es habitual en mi país... La gente se suma al carro de insultar a la persona que en realidad era la víctima.»**

Hombre de 17 años, Pakistán[60]

Apoyo a adultos y niños en riesgo de causar daño

> «Llamar a la línea de ayuda por primera vez fue lo más difícil que he hecho nunca, pero me alegro mucho de haberlo hecho. [Fue] la primera vez en años que reconocí mi adicción al porno para adultos, que me llevó a ver otras imágenes [de CSAM]. He recibido un gran apoyo y nunca me he sentido juzgado.»

Llamada anónima a ***Stop It Now!***[112]

Los programas de prevención de la perpetración son una importante estrategia de prevención respaldada por pruebas cada vez más sólidas.[28] Pueden proporcionar ayuda temprana a las personas preocupadas por sus propios pensamientos o comportamientos sexuales hacia la niñez, interrumpir las vías que conducen a la comisión de delitos y prevenir el daño antes de que se produzca. Los pensamientos y comportamientos sexuales dañinos suelen comenzar en la infancia, lo que subraya la necesidad de intervenciones tempranas y personalizadas tanto para los adultos como para los niños que corren el riesgo de causar daño.[168] Las barreras para buscar ayuda pueden reducirse ofreciendo múltiples opciones accesibles que prioricen el anonimato y establezcan límites claros de confidencialidad.[168] A continuación se enumeran algunos ejemplos de iniciativas de prevención de la perpetración:

- El proyecto **ReDirection** encuesta a personas anónimas que buscan CSAM en la web oscura y las redirige a servicios de apoyo, al tiempo que genera datos para informar estrategias de prevención eficaces.[169] Con más de 26 000 respuestas recopiladas en varios idiomas, el proyecto ha proporcionado información importante sobre las vías de delincuencia y los comportamientos de búsqueda de ayuda de los delincuentes. El programa de autoayuda **ReDirection** ha sido evaluado en cuanto a su escalabilidad y está siendo objeto de una evaluación más detallada.
- **Help Wanted**, un curso en línea que ofrece ayuda a adolescentes y adultos jóvenes atraídos por niños más pequeños, se desarrolló en los Estados Unidos y ahora se está adaptando para México.[170]
- La línea de ayuda **Stop It Now!** ofrece asesoramiento y apoyo confidenciales a personas preocupadas por sus propios pensamientos o comportamientos sexuales hacia los niños o los de otras personas. El apoyo está disponible en más de 200 idiomas. En 2023-24, casi la mitad de los 4000 clientes que llamaron a la línea de ayuda eran adultos que buscaban ayuda para sus propios pensamientos y comportamientos, incluidos aquellos que ya habían causado daño a niños.[112] Alrededor del 12 % de las personas que buscaban ayuda eran desconocidas para las autoridades en el momento del primer contacto, lo que sugiere que las líneas de ayuda pueden llegar a las personas en riesgo antes de que intervengan las fuerzas del orden.[112]
- **Prevention Global** es una plataforma de conocimiento y una ambiciosa iniciativa de investigación que evalúa siete programas desarrollados para prevenir los abusos sexuales a menores, entre los que se incluyen terapia individual y grupal, asesoramiento a distancia, materiales autoguiados y planes de estudios escolares. **Prevention Global** publica una serie de productos de conocimiento y la publicación Scalability explora las barreras y las oportunidades para ampliar los programas de prevención, incluyendo una evaluación de los programas con un enfoque particular en la prestación de servicios de ayuda a quienes la solicitan.[125]

> **«Podemos ver que algunos delincuentes pueden ser desviados de su comportamiento delictivo. Y si nos centráramos más en eso, estaríamos haciendo un mejor trabajo. Pero es muy difícil que la gente lo entienda... Es una narrativa muy complicada de aceptar desde el punto de vista político y social... lo que hace que no sea muy popular hablar de ello, ni financiar estas iniciativas. Pero cada vez hay más pruebas de que, en el caso de algunas personas, se puede intervenir y desviarlas del camino que están siguiendo.»**

Sociedad civil[11]

Disuadir la búsqueda de material de abuso sexual infantil: perspectivas de la Fundación Lucy Faithfull

La Fundación Lucy Faithfull trabaja para prevenir el abuso sexual infantil a través de servicios profesionales para personas en riesgo de causar daño, familias afectadas por el abuso y herramientas y recursos para que los profesionales creen entornos más seguros para los niños.

- Las tipologías y trayectorias de los delincuentes varían significativamente, lo que requiere tácticas personalizadas y mensajes diversos y multicanal para llegar a los diferentes perfiles de delincuentes.
- Las advertencias deben transmitirse en todos los puntos en los que alguien pueda intentar acceder a contenidos ilegales.
- Los mensajes deben estar cuidadosamente diseñados y no ser críticos. Los mensajes disuasorios por sí solos no pueden disuadir de cometer delitos, pero si se combinan con un apoyo accesible y anónimo, pueden animar a las personas a buscar ayuda para abordar sus pensamientos y comportamientos sexuales.

> **«La mayoría del público prefiere considerar los delitos sexuales como algo ajeno. Es algo que les pasa a otras personas. Otras personas son los delincuentes. Otras personas son las víctimas... Eso no contribuye en nada a la protección de los niños. No contribuye en nada a mantenerlos a salvo... No te darás cuenta si tu hijo está abusando de tu otro hijo... No te darás cuenta si solo buscas monstruos y depredadores.»**

Sociedad civil [11]

La Fundación Lucy Faithfull ha sido pionera en la difusión de mensajes disuasorios a través de campañas en canales en línea y fuera de línea, incluidos los medios de comunicación convencionales, las redes sociales, la publicidad digital de pago, cortometrajes y colaboraciones con las fuerzas del orden y otras organizaciones estatutarias y voluntarias.[171]

Tras más de once años de mensajes disuasorios y campañas, la Fundación Lucy Faithfull identificó cuatro mensajes fundamentales que advierten eficazmente a quienes buscan CSAM:

- Acceder a imágenes sexuales de niños es un delito.
- Causa daño a los niños.
- Tiene consecuencias para ti y tu familia.
- Si quieres dejarlo, hay ayuda anónima disponible.

La Fundación Lucy Faithfull, en colaboración con IWF y Aylo (una plataforma de contenido para adultos), probó si los mensajes disuasorios anónimos basados en chatbots podían interrumpir y reducir las búsquedas de CSAM en Pornhub UK. Aylo mantiene una lista dinámica de miles de términos prohibidos debido a su asociación con imágenes sexuales de niños. Cuando un usuario busca uno de estos términos en Pornhub UK, aparece un mensaje de advertencia estático. Además, aparece un chatbot, similar a un cuadro de atención al cliente estándar que se ve habitualmente en otros sitios web. En función de las respuestas de los usuarios, el chatbot puede dirigir a las personas a servicios de apoyo anónimos, como la línea de ayuda **Stop It Now!**, el correo electrónico o el chat en vivo, recursos de autoayuda en línea, la línea nacional de prevención del suicidio o los servicios urgentes de salud mental del Servicio Nacional de Salud.[171]

Una evaluación de la intervención reveló que:[171]

- El 82 % de las sesiones en las que se buscaba contenido ilegal fueron interrumpidas. Algunos usuarios terminaron su sesión por completo, mientras que otros cambiaron a contenido legal o abandonaron el sitio.
- La combinación del mensaje de advertencia y el chatbot animó a las personas a buscar ayuda en los servicios de **Stop It Now!**
- Cuando se desactivó el chatbot durante un mes, aumentaron las búsquedas de CSAM.

Impacto del proyecto en cifras

- Se produjo una reducción estadísticamente significativa en las búsquedas de imágenes sexuales de menores de 18 años durante los 18 meses que duró el proyecto.
- El chatbot y el mensaje de advertencia se mostraron 2,8 millones de veces.
- El 99,8 % de las búsquedas realizadas durante los 18 meses que duró el proyecto no activaron el chatbot ni el mensaje de advertencia.
- 1.656 personas solicitaron información sobre los servicios de la línea de ayuda después de ver el chatbot o el mensaje de advertencia.
- 490 personas visitaron el sitio web **Stop It Now!** después de ver un mensaje de advertencia o el chatbot.
- Se identificó que 68 personas que llamaron a la línea de ayuda **Stop It Now!** habían interactuado con el chatbot.

Opciones de denuncia accesibles y fiables y apoyo centrado en las víctimas

> Los gobiernos, las empresas tecnológicas y las instituciones educativas deben [...] garantizar que los niños puedan denunciar en cualquier lugar y en cualquier momento. [...] Y entonces se podrán tomar las medidas necesarias para ayudar a reducirlo.

Mujer de 24 años, Uganda[38]

Se necesita una serie de mecanismos de denuncia accesibles y fiables para poner en contacto a los niños que han sufrido daños con servicios de apoyo integrales, adaptados a los niños y centrados en los supervivientes. Las pruebas demuestran sistemáticamente que los niños rara vez utilizan los canales de denuncia formales. Por ejemplo, **Disrupting Harm** descubrió que solo alrededor del 3 % de los niños sometidos a explotación o abuso sexual en línea lo denunciaron a un canal de apoyo o a la policía, en comparación con el 40 % que se lo contó a sus amigos y el 24 % que se lo contó a sus hermanos.[60]

> Normalmente no hablo con adultos. Suelo hablar con gente de mi edad, porque están pasando por cosas similares y pueden identificarse más fácilmente, y sé que los adultos tienen buenas intenciones, pero a veces siento que quizá no lo entienden del todo, o que lo ven de otra manera, y.... es mejor hablar con gente de mi edad.

Mujer de 15 años, Etiopía[60]

> Creo que mucha gente podría no [hablar con sus padres] porque sienten que les restringirán el uso del teléfono si lo cuentan... Quizás muchos niños se sientan culpables, especialmente en casos de abuso sexual. Podrían sentirse culpables y pensar que también es culpa suya.

Mujer de 15 años, Reino Unido[60]

> Prefiero hablar con adultos porque creo que tienen más ideas... Los adultos con los que hablo me escuchan bien, especialmente mi hermana.

Chica de 17 años, Nigeria[60]

Los defensores de los jóvenes hacen hincapié en que la denuncia debe ser fácil de acceder y utilizar, libre de estigmas y fiable.[60] Algunos jóvenes sugieren modelos dirigidos por compañeros, como adolescentes formados que puedan responder de manera eficaz y dirigir a sus compañeros a los servicios de apoyo adecuados.[60] Otros ejemplos en la práctica incluyen:

- **Meri Trustline**, una línea de ayuda en la India que apoya a niños, mujeres y personas de identidades marginadas que corren el riesgo de sufrir daños en línea.[172] Las denuncias enviadas a través de WhatsApp, correo electrónico o teléfono son recibidas por consejeros capacitados. La plataforma también integra la herramienta **Report Remove** de la IWF, que permite a los niños denunciar contenidos en línea y solicitar su eliminación.[173]
- Modelos de servicios multidisciplinarios centrados en la niñez para los niños víctimas de abuso y explotación sexual, como **Barnahus** (Casa de los Niños), que ofrece servicios adaptados a los niños y sensibles al trauma, incluyendo entrevistas forenses, exámenes médicos, servicios terapéuticos y apoyo a las víctimas y sus familias. Los centros de atención integral son otro ejemplo: proporcionan respuesta inmediata a situaciones de crisis y servicios de apoyo a las mujeres y los niños que sufren violencia de género, especialmente en los países de ingresos bajos y medios. Sus servicios integrales y ubicados en un mismo lugar incluyen servicios jurídicos, servicios sociales y asesoramiento.[174] Unicef está examinando cómo estos modelos de atención pueden ayudar a los niños y niñas víctimas de abuso y explotación sexual infantil facilitados por la tecnología.[174] Próximamente se publicarán experiencias de Filipinas, Sudáfrica, Nigeria y Bulgaria.[174]
- Los productos de conocimiento de Prevention Global's **Serving Youth** incluyen una **guía práctica para líderes** de organizaciones juveniles que destaca ocho prácticas sistemáticas para prevenir y abordar el abuso sexual infantil.[175,176] Las investigaciones muestran una disminución de más del 20 % en la prevalencia de la victimización en las organizaciones que prestan servicios a los jóvenes y que han implementado estrategias de prevención del abuso sexual infantil.[180]

> **«En mi opinión, la mejor manera sería escucharlos sin juzgarlos, creer lo que dicen, darles acceso a asesoramiento o ayuda, y asegurarse de que sepan que no están solos, porque eso significaría mucho... sentirse seguros, ser escuchados, tener apoyo para recuperarse y también asegurarse de que las personas que lo hicieron rindan cuentas.»**
>
> *Mujer de 15 años, Etiopía*[38]

Seguridad digital

> «A medida que seguimos construyendo estos mundos digitales, debemos asegurarnos de hacerlo teniendo en cuenta la seguridad. No se trata solo de dar a los jóvenes acceso a nuevas tecnologías interesantes, sino de proporcionarnos las herramientas necesarias para protegernos, enseñarnos a reconocer cuándo algo no va bien y crear espacios en los que podamos disfrutar de todas las ventajas de estas innovaciones sin los peligros que acechan.»

Defensora de los jóvenes

La seguridad, los derechos y el bienestar de los niños deben ser una prioridad en todos los niveles de la cultura empresarial, la gobernanza y la formación de los equipos de trabajo.

Las empresas deben integrar evaluaciones del impacto sobre los derechos de los niños y niñas, medidas rigurosas de seguridad infantil y características de diseño centradas en el niño en todos los procesos de desarrollo.

Las empresas deben detectar y eliminar de forma proactiva los contenidos y comportamientos perjudiciales, además de moderarlos de forma reactiva.

La transparencia, la rendición de cuentas y la colaboración intersectorial son esenciales para reforzar las defensas globales contra la CSEA facilitada por la tecnología.

Promover una cultura industrial de seguridad infantil

La creación de un ecosistema digital más seguro para la niñez requiere una cultura industrial que dé prioridad a los derechos, la seguridad y el bienestar de los niños en todos los niveles de la cultura empresarial, la gobernanza, la toma de decisiones y la formación de sus colaboradores. La seguridad infantil debe enfatizarse como una responsabilidad profesional desde la fase inicial, incluyendo los planes de estudios de informática y las vías de contratación de la industria.[32] El personal que participa en el diseño, el desarrollo y la entrega de productos y servicios digitales debe recibir formación continua para reconocer y mitigar los riesgos para los niños. La seguridad infantil también debe integrarse en las políticas y códigos de conducta de las empresas. En 2024, el Gobierno de Camboya formó a 48 empresas de tecnología digital sobre las directrices del sector para la protección de los niños en Internet; cuatro de estas empresas formadas integraron posteriormente la protección infantil en sus políticas internas y elaboraron un código de conducta de protección infantil para su personal.[159]

Los moderadores de contenidos y los trabajadores de seguridad digital, descritos como los «trabajadores esenciales para la seguridad de Internet», realizan una labor vital y difícil, pero a menudo se enfrentan a condiciones precarias y

a riesgos para su propia salud y bienestar. Deben recibir apoyo con condiciones laborales justas, desarrollo profesional, acceso a servicios de salud mental y apoyo psicosocial, y apoyo tras la finalización del empleo.[181] Estas medidas pueden mejorar la retención de la mano de obra, aumentar la experiencia y mejorar la calidad y la eficacia de las respuestas de seguridad digital.

Hacer de la seguridad por diseño la norma

Un enfoque de seguridad desde el diseño requiere que todas las partes interesadas que participan en el diseño y desarrollo de productos y servicios digitales se pregunten: «¿qué haríamos de manera diferente si supiéramos que el usuario final es un niño?».[182] Esto traslada la responsabilidad a las empresas de garantizar que sus productos no causen daño a los niños. Es importante destacar que estas medidas de seguridad deben aplicarse a todas las tecnologías digitales, ya que los niños suelen acceder a productos y servicios que no han sido creados específicamente para ellos.[183] Varios expertos de la sociedad civil señalaron la percepción de que los intereses comerciales prevalecen sobre los derechos y la seguridad de los niños.[184] Los representantes de la industria sostienen que un enfoque de seguridad desde el diseño no tiene por qué entrar en conflicto con los intereses comerciales.

Las características clave de la seguridad desde el diseño incluyen:[31]

- Integrar las evaluaciones del impacto sobre los derechos del niño y la diligencia debida en los procesos de diseño y desarrollo. Las evaluaciones del impacto sobre los derechos del niño son procesos que permiten a las empresas evaluar cómo sus operaciones, productos y servicios afectan a los derechos del niño, tal y como se definen en la Convención de las Naciones Unidas sobre los Derechos del Niño y otros instrumentos de derechos humanos.[185]
- Privacidad y protección de datos, incluyendo estrictos ajustes predeterminados de privacidad, experiencias de usuario adecuadas a la edad y salvaguardias contra el uso indebido de los datos personales de los niños.
- Diseño y educación centrados en los niños, como involucrar a los niños y jóvenes en el diseño y las pruebas de productos, proporcionar información clara y accesible, e incorporar funciones educativas que aumenten la capacidad de acción y la conciencia de los niños.
- Protecciones integradas, como controles parentales, límites de contacto, salvaguardias financieras para evitar que los niños transfieran dinero en línea y modos o dispositivos de funcionalidad limitada.
- Responsabilidad mediante obligaciones claras de transparencia en la presentación de informes, una moderación sólida y mecanismos accesibles de denuncia y reparación.

Las funciones de seguridad infantil deben ser funcionales, accesibles y estar disponibles de forma equitativa en todas las regiones geográficas y en todos los idiomas en los que se ofrece un producto o servicio.

> **«Si abres una cuenta [en redes sociales] aquí en América Latina y el Sur Global, la pregunta era si tendrían el mismo tipo de protecciones y salvaguardias que las personas que tienen una cuenta en Estados Unidos y Reino Unido, y la respuesta era: ¡por supuesto que no!... Las personas aquí en América Latina están menos seguras que los niños de otros países. ¿Y por qué tiene que ser así?».**
>
> *Sociedad civil*[11]

Un marco complementario, los derechos del niño por diseño, reconoce que las tecnologías digitales deben apoyar la realización de los derechos

del niño, incluido su derecho a la seguridad.[186] La aplicación de estos enfoques requiere el compromiso de los líderes, recursos específicos y personal capacitado. Las empresas más pequeñas y las *start-ups* suelen carecer de esta capacidad, aunque existen directrices para ayudar a las empresas a evaluar el impacto de las tecnologías digitales, incluida la IA generativa, en los derechos del niño.[36,184,187–189] La aplicación eficaz de los principios de seguridad desde el diseño debe basarse en pruebas y requiere transparencia por parte de la industria y mecanismos de rendición de cuentas independientes.

Tabla 1. Ejemplos de seguridad desde el diseño y derechos del niño

Elemento de diseño	Acción	Ejemplos en la práctica
Medidas de seguridad del producto	Integrar las evaluaciones de riesgos para la seguridad en el desarrollo de productos.	**La caja de herramientas D-CRIA** de Unicef orienta a las empresas sobre cómo realizar evaluaciones sólidas del impacto en los derechos del niño y la debida diligencia en relación con el entorno digital. Incluye una plantilla D-CRIA, una guía de inicio rápido y orientaciones destacadas para la participación y el compromiso de los niños.[185] **El Marco de IA responsable** y **la Lista de verificación de seguridad por diseño** de Thorn para plataformas tecnológicas tienen como objetivo reducir los riesgos asociados a la IA generativa.[188]
Medidas de seguridad del producto	Diseñar dispositivos o modos seguros para los niños con funcionalidad o acceso limitados. Las funciones mejoradas pueden ser desbloqueadas por un padre o cuidador.	**HMD Fuse** es un smartphone seguro para niños con un filtro de contenido de IA integrado que bloquea la visualización, grabación o almacenamiento de contenido con desnudos. Se inicia en un modo restringido sin acceso a aplicaciones ni redes sociales, a menos que los cuidadores habiliten funciones adicionales.[190] **La seguridad en las comunicaciones** de Apple está habilitada de forma predeterminada para las cuentas infantiles. Escanea las imágenes y los videos del dispositivo para detectar y difuminar automáticamente el contenido de desnudos, advierte al niño y proporciona orientación y recursos de seguridad adecuados a su edad, además de permitir el control parental a través de la configuración de Screen Time.[191]
Privacidad y protección de datos	Aplique medidas de privacidad y protección estrictas por defecto, y recopile la mínima información posible de las cuentas infantiles o cuando la edad del usuario sea incierta.	Las cuentas de redes sociales para adolescentes, como **el modo Snapchat Teen**, pueden hacer que las cuentas sean privadas, restringir los mensajes directos, filtrar contenidos nocivos y desactivar el uso compartido de la ubicación de forma predeterminada.192 **YouTube Kids,** para niños menores de 13 años, filtra el contenido, desactiva los comentarios, el uso compartido de la ubicación y los anuncios personalizados de forma predeterminada.

Elemento de diseño	Acción	Ejemplos en la práctica
Comunicación, educación y mecanismos de denuncia adaptados a los niños	Proporcione información, educación y mecanismos de denuncia/queja adecuados a la edad y aptos para los niños.	El programa de seguridad digital **Be Internet Awesome** de Google incluye juegos interactivos sobre seguridad en línea, privacidad y uso respetuoso de las redes sociales.[193] LEGO ha desarrollado un código de conducta adaptado a los niños. La herramienta **Captain Safety** de la ya desaparecida aplicación LEGO Life incorporaba un compromiso de seguridad, recordatorios de seguridad dentro de la aplicación y explicaciones adaptadas a los niños sobre las políticas de privacidad y moderación.[194] El programa **School Partnership** de Instagram ofrece recursos de seguridad digital y da prioridad a las denuncias de contenidos y cuentas perjudiciales presentadas por estudiantes y educadores, garantizando su revisión en un plazo de 48 horas.[195]

> **«Cuando era adolescente, buscaba una razón para decir que no. Y él seguía presionándola [para que enviara más imágenes sexuales], y ella no podía luchar... No podía decir que no... Pero "mi teléfono no me deja hacer fotos desnuda" parece una forma muy poderosa de devolver ese poder a las víctimas para que digan que no pueden. "Sí. Yo no, el dispositivo no me deja".»**
>
> *Sociedad civil*[11]

Detectar y neutralizar de forma proactiva los daños

Las empresas tecnológicas deben detectar y bloquear de forma proactiva y en tiempo real los contenidos, cuentas y comportamientos perjudiciales utilizando herramientas como los sistemas de comparación de hash y los filtros de supervisión de contenidos, respetando, al mismo tiempo, los derechos de los usuarios.[73] Están surgiendo iniciativas para aprovechar la IA y el aprendizaje automático para la detección proactiva de contenidos, entre ellas un servicio de detección de *grooming* que utiliza el aprendizaje automático y un sistema de inteligencia para la detección de CSAM que ha demostrado ser capaz de distinguir con precisión entre publicaciones CSAM y no CSAM en la *deep web*, al tiempo que genera información útil sobre los creadores y las víctimas.[196,197]
El producto **Safer** de Thorn es un conjunto de herramientas basadas en IA que las empresas pueden utilizar para detectar, identificar y denunciar CSAM. **Safer** se integró en la aplicación web de IA generativa DALL-E2 de OpenAI.[198]

La Tech Coalition está probando un concepto para detectar y responder al abuso sexual infantil facilitado por la tecnología en entornos de transmisión en directo.[199] Este programa piloto utilizará señales de metadatos, como las características de la sesión y el uso de servicios de anonimización, para generar una puntuación de riesgo que indique la probabilidad de que se produzca abuso sexual infantil en línea dentro de una sesión de transmisión en directo determinada, para que los equipos de seguridad infantil lo investiguen más a fondo. Las pruebas y la evaluación se llevarán a cabo esta primavera para evaluar la viabilidad de una adopción más amplia por parte de la industria.

Los niños deben poder denunciar inmediatamente sus inquietudes y los contenidos y comportamientos nocivos que encuentren en Internet —incluidos el material sexual infantil, la extorsión sexual, la captación de menores o la distribución de imágenes sin consentimiento— a través de canales sencillos y fiables dentro de la propia plataforma.[60] Las denuncias deben dar lugar a respuestas oportunas para eliminar los contenidos y bloquear las cuentas nocivas, así como para poner a los usuarios en contacto con los servicios de apoyo y realizar un seguimiento.

Muchos productos digitales no ofrecen mecanismos de denuncia accesibles y, aunque los haya, los niños a menudo no los utilizan. Un estudio mundial sobre la extorsión sexual reveló que **solo el 4 % de los niños denunciaban los incidentes a la plataforma en la que se producían**.[52] Los defensores de los jóvenes hicieron hincapié en que la experiencia de denunciar y solicitar la retirada de imágenes sexuales es tan importante como la función en sí misma: debe ser fácil, segura y libre de estigmas. Como ejemplo positivo, el servicio **Take It Down** del NCMEC tranquiliza a los niños con mensajes no estigmatizantes («tener desnudos en Internet da miedo, pero hay esperanza de que se eliminen»), asistencia multilingüe, videos explicativos y preguntas frecuentes.[200] Las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económicos) subrayan que los sistemas de reparación deben diseñarse con la participación de los niños y adaptarse a los riesgos específicos de cada plataforma.[182]

> «Creo que [algunas plataformas digitales]... se centran más en sus beneficios que en la seguridad [de los niños]. Algo que sin duda podría ayudar es mejorar los mecanismos de denuncia en la plataforma, porque creo que muchas veces es muy difícil saber dónde denunciar y no hay mucha información sobre cómo funciona realmente. Y, en muchos casos, no recibes respuesta. Así que te da la sensación de que es inútil y de que no tiene sentido denunciar.»

Chica de 15 años, Reino Unido[60]

Transparencia y rendición de cuentas

Es esencial reforzar el compromiso con la transparencia y la rendición de cuentas. Las empresas deben realizar evaluaciones obligatorias del impacto sobre los derechos del niño y publicar informes de transparencia oportunos que recojan los riesgos, los daños y los comportamientos de los usuarios que puedan servir de base para las estrategias de prevención. Estos pueden incluir, por ejemplo, datos demográficos de las víctimas y los autores, tasas de abandono de sesiones o clics en servicios de apoyo activados por ventanas emergentes de advertencia. La estandarización de las métricas de seguridad infantil y los procesos de denuncia en todo el sector pueden abordar los retos actuales en materia de comparabilidad de datos. El programa **Lantern** de la Tech Coalition destaca la necesidad de un ecosistema en el que se compartan datos, conocimientos y responsabilidades entre todos los sectores para reforzar la protección de los niños en Internet.

Lantern: acción coordinada de la industria contra la explotación y el abuso sexual infantil en línea: conocimientos de la Tech Coalition

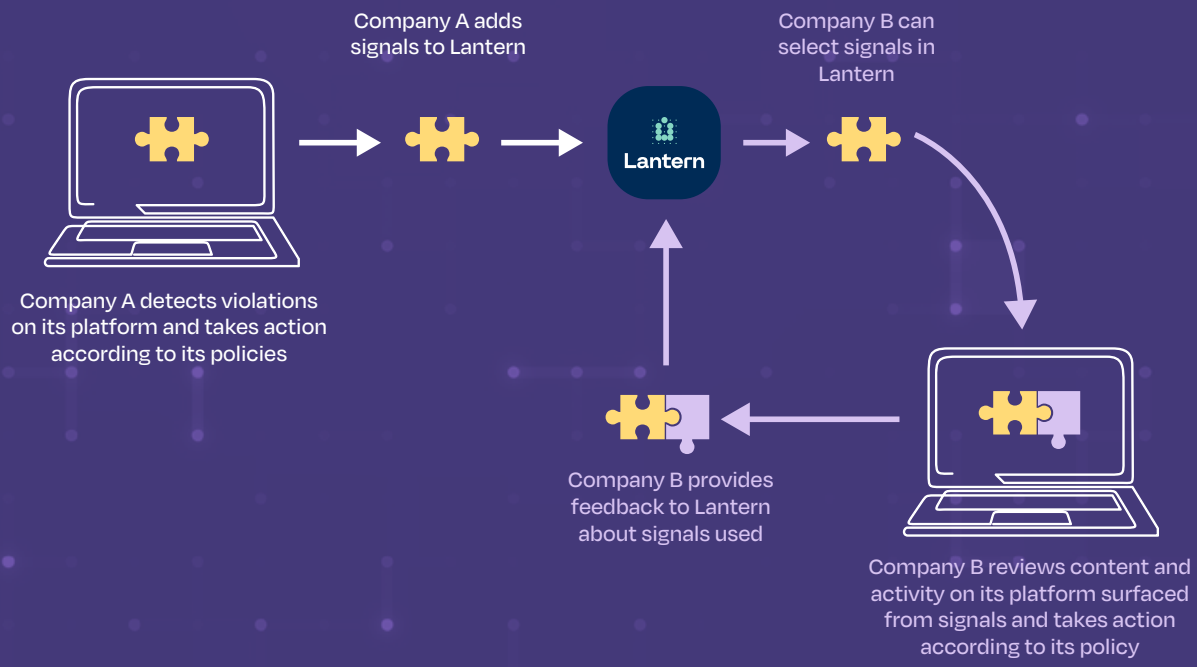
La Tech Coalition es una alianza global de más de 55 empresas tecnológicas comprometidas con la protección de los niños contra la explotación y el abuso sexual en línea mediante el intercambio de conocimientos, la identificación de amenazas y el desarrollo de soluciones colaborativas.

Los autores suelen utilizar múltiples plataformas para compartir contenidos abusivos y explotar a los niños en línea. Históricamente, no existía un marco universal para coordinar los esfuerzos de toda la industria para detectar la explotación y el abuso, lo que dejaba lagunas en la detección y la respuesta. **Lantern** se creó para colmar esta laguna, permitiendo a las empresas participantes compartir señales de abuso que se pueden actuar, lo que permite detectar y responder a daños que, de otro modo, podrían pasar desapercibidos.[201]

Basándose en el principio de que compartir información sobre amenazas mejora la respuesta de la industria al CSEA en línea, **Lantern** facilita la colaboración para fortalecer las defensas colectivas contra las amenazas emergentes. Las señales, como los hash, las URL o los nombres de usuario, representan contenidos o comportamientos potencialmente dañinos relacionados con el CSEA en línea. Cuando una plataforma envía una señal, otras pueden revisar de forma independiente la actividad relacionada en sus propios servicios.[25]

Cuando una empresa identifica CSEA en su plataforma, toma las medidas adecuadas para hacer cumplir sus políticas de seguridad infantil y comparte las señales asociadas a través de **Lantern**. Esto permite a otras plataformas detectar y eliminar de forma proactiva el contenido o las cuentas relacionadas, lo que refuerza el ecosistema general de seguridad en línea.

Figura 6. Marco y proceso de intercambio de señales **de Lantern**[25]



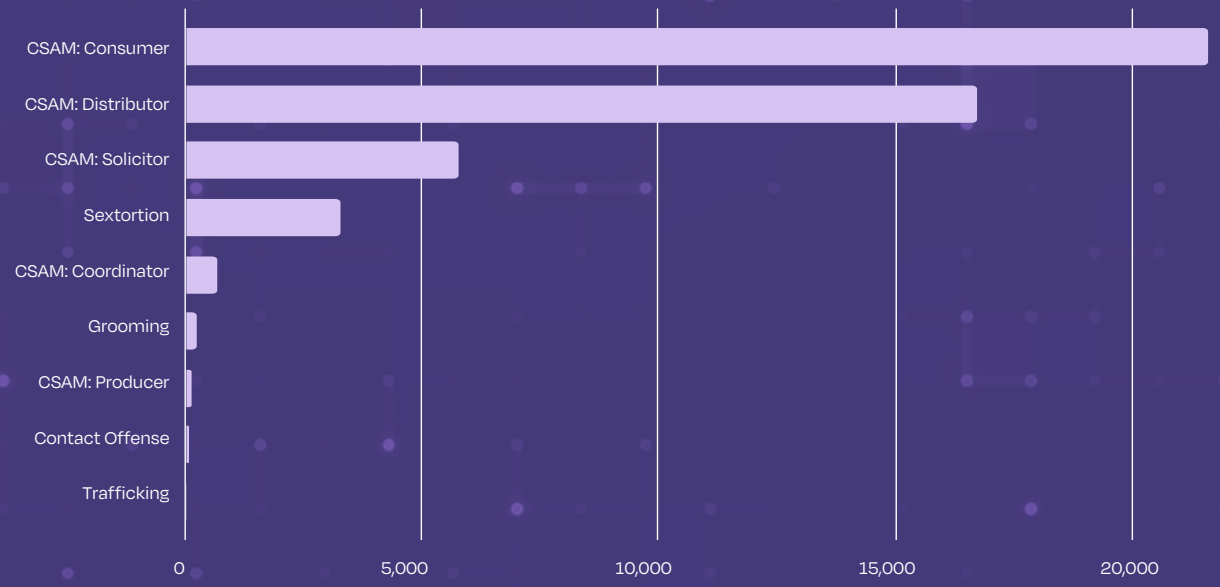
La colaboración a través de **Lantern** ya está demostrando su impacto y las empresas participantes están observando mejoras constantes en su capacidad para mitigar los riesgos para la seguridad infantil.[201] En 2024:

- Se compartieron casi 300 000 nuevas señales relacionadas con la CSEA en línea, lo que eleva el total a más de un millón de señales **de Lantern** hasta la fecha.
- Se tomaron medidas contra más de 100 000 cuentas por infracciones relacionadas con la explotación y el abuso sexual infantil.
- Se bloquearon o eliminaron más de 135 000 URL que alojaban o transmitían CSEA.
- Se eliminaron más de 7.000 piezas de CSAM.
- Se señalaron casos de alto riesgo, incluidos 81 incidentes de delitos sexuales con contacto y 45 casos relacionados con la trata de personas.

La mayoría de las señales basadas en incidentes involucraban a perpetradores que buscaban distribuir u obtener CSAM, a veces como precursores del grooming o el abuso con contacto.[201] La taxonomía de señales de **Lantern** permite una categorización más precisa de las amenazas, lo que respalda múltiples enfoques para la detección y la respuesta.[201]

Figura 7. Señales cargadas por tipo en 2024

Figura 8. Categorías de señales basadas en incidentes notificadas en 2024



Lantern demuestra el poder de la colaboración entre sectores para combatir la explotación y el abuso infantil en línea. Al romper los silos entre plataformas, el programa ha mejorado la detección, la responsabilidad de los autores y la rapidez de respuesta. Es importante destacar que también demuestra cómo el intercambio de señales relacionadas con el contenido y el comportamiento puede reforzar las defensas contra amenazas más amplias, como el grooming, la extorsión y la trata de personas, además de la distribución de CSAM.

> **« Lo que realmente me llamó la atención fue la importancia de que se necesita un pueblo... todo el mundo debe participar en la prevención. »**

Industria[7]

Ley, política y justicia

> **« Creo que necesitamos más regulación, más legislación. Y creo que lo mismo ocurre con el tabaquismo y el abuso de sustancias. No dejamos que los niños fumen. No dejamos que los niños beban. Tenemos legislación. Por lo tanto, hemos tardado demasiado en regular Internet. »**

Sociedad civil[11]

La armonización de la legislación es esencial para cerrar las lagunas jurídicas, garantizar la cooperación transfronteriza y mantenerse al día con las amenazas digitales emergentes.

La aplicación eficaz de las leyes depende de sistemas judiciales bien dotados de recursos, informados sobre los traumas y centrados en los supervivientes, que protejan a los niños y no les vuelvan a traumatizar.

Para hacer frente a la CSEA facilitada por la tecnología es necesaria una acción colaborativa entre el gobierno, los reguladores, la industria y la sociedad civil para que los responsables rindan cuentas.

Armonizar la legislación a nivel mundial de acuerdo con las normas sobre los derechos del niño

Los esfuerzos por armonizar la legislación nacional que aborda la CSEA facilitada por la tecnología están cobrando impulso a nivel mundial. La **Convención de las Naciones Unidas contra la Ciberdelincuencia** es un tratado multilateral histórico contra la delincuencia que promueve los esfuerzos para normalizar las leyes mundiales de protección de la infancia, entre otras cosas, tipificando como delito el CSAM y el *grooming* por primera vez a nivel mundial.[23] Las leyes exhaustivas, como la **Ley de Seguridad en Línea del Reino Unido**, ayudan a minimizar las inconsistencias que existen naturalmente cuando se legisla entre los distintos ministerios y áreas temáticas del gobierno.[8,202] La reciente Política Integral de Protección Infantil de Fiyi, promulgada en 2025, armonizó la anterior **Ley de Cuidado y Protección de 2024** y la **Ley de Justicia Infantil de 2024.** También trató de minimizar las lagunas jurídicas y mejorar la coordinación entre sectores.[203] Sin embargo, a nivel mundial, siguen existiendo incoherencias en los esfuerzos legislativos tanto dentro de los gobiernos como entre ellos. La falta de un sistema centralizado para supervisar la evolución legislativa y compartir los avances agrava aún más el desafío mundial que supone la incoherencia legislativa. Herramientas comparativas como **la tabla de puntuación de los países del G7 #BeBrave** del Movimiento Brave y el **Índice de Regulación de la Seguridad en Línea** ponen de relieve los avances y las deficiencias.[204,205]

> «Gran parte [de la extorsión sexual] proviene de países extranjeros... pero cada uno tiene sus propias jurisdicciones y leyes, y nadie quiere colaborar [por lo que] nos resulta muy difícil decir: "No le hagáis esto a los niños".»
>
> *Superviviente*[77]

Avances de Brasil en 2025 en materia de protección infantil en línea

En 2025, Brasil marcó un hito en la protección digital de los niños mediante medidas políticas que reflejan el creciente liderazgo de los países de la Mayoría Global en la creación de entornos en línea más seguros. En septiembre, Brasil promulgó una ley integral que establece obligaciones claras para las empresas y las plataformas con el fin de prevenir, detectar y responder a la CSEA en línea.[19] La ley introduce el deber de prevención, exige la eliminación inmediata de contenidos ilegales sin necesidad de órdenes judiciales y obliga a informar a las autoridades nacionales. La ley también incorpora principios de seguridad y privacidad desde el diseño, prohíbe la publicidad dirigida a los niños y establece normas estrictas de verificación de la edad, incluida la vinculación de cuentas parentales para los usuarios menores de 16 años. Las plataformas deben proporcionar herramientas de control parental en portugués, publicar informes de transparencia y permitir el acceso de los investigadores a los datos sobre el bienestar digital de los niños. La aplicación de la ley estará a cargo de la Agencia Nacional de Protección de Datos de Brasil.[19]

Las consultas multisectoriales, en las que participen la industria y las organizaciones de defensa de los derechos del niño, son esenciales para garantizar que las leyes se adapten a las nuevas amenazas tecnológicas y se ajusten a las normas sobre los derechos del niño, al tiempo que permiten la innovación que mejora la seguridad infantil. Las opiniones sobre la mejor manera de proteger a los niños mediante la legislación siguen siendo dispares: un experto del sector abogó por la creación de refugios legislativos (con salvaguardias estrictas) para poner a prueba y someter a pruebas de presión las herramientas de detección, mientras que un representante de la sociedad civil advirtió que algunas leyes de notificación obligatoria pueden restringir inadvertidamente la notificación voluntaria y oportuna.[7,11]

Garantía de la edad en la era digital: equilibrio entre protección y participación

- La verificación de la edad describe los métodos utilizados para verificar o estimar la edad de un usuario en línea con el fin de garantizar el acceso a contenidos adecuados para su edad. Los métodos implican un equilibrio entre la precisión, la privacidad y la equidad.
- Las recientes leyes que exigen la verificación de la edad han llamado la atención del público sobre los riesgos para la seguridad de los niños en línea y han puesto de manifiesto una serie de retos éticos, prácticos y políticos. Pueden tener consecuencias no deseadas, como que los usuarios eludan las restricciones o la exclusión de grupos marginados.
- La verificación de la edad puede mejorar la seguridad de los niños en Internet, pero sin una consulta significativa con los niños y los jóvenes, su aplicación corre el riesgo de socavar sus derechos.
- Las restricciones de edad no deben reducir la importancia de las intervenciones familiares, escolares y comunitarias, ni minimizar la importancia de la responsabilidad de las empresas y las evaluaciones del impacto sobre los derechos del niño en relación con los entornos digitales.

Tendencias legislativas mundiales

Desde la última Evaluación Global de Amenazas, muchos países han introducido leyes de verificación de la edad y seguridad en línea:[206]

- Brasil: aprobó una legislación que incluye obligaciones exhaustivas de verificación de la edad en septiembre de 2025.[19]
- Reino Unido: exigió a las plataformas que impidieran que los jóvenes se encontraran con contenidos nocivos, incluido el uso de sistemas de verificación de la edad «altamente eficaces» (por ejemplo, identificación o estimación facial) en sitios web pornográficos y grandes plataformas de redes sociales, a partir de julio de 2025.[202]
- Australia: restringirá el acceso de los menores de 16 años a las redes sociales a partir de diciembre de 2025.[207]
- Singapur: exigirá la verificación de la edad en las tiendas de aplicaciones para las descargas de Google Play, Apple y Huawei.[21]

Otras localidades que han considerado o adoptado recientemente una legislación similar son Dinamarca, Malasia, Mongolia, Nueva Zelanda, Corea del Sur, Turquía, la Unión Europea y Uzbekistán.[50,51]

> **«Muchas de las leyes elaboradas para los jóvenes no están [realmente] pensadas para los jóvenes. Por ejemplo, las prohibiciones actuales de las redes sociales para menores de 16 años: no se ha consultado lo suficiente a los jóvenes. Los jóvenes deberían estar presentes en la sala mientras se redactan y desarrollan las leyes, no solo en la fase de consulta.»**

Mujer de 22 años, Australia[38]

Perspectivas de los niños

Los niños y los jóvenes reconocen el valor de las leyes de seguridad en línea, al tiempo que hacen hincapié en la necesidad de matizar su diseño y aplicación. Una encuesta representativa a nivel nacional realizada a niños de entre 8 y 17 años en Australia reveló que casi el 90 % apoyaba los controles de edad para acceder a los sitios web, mientras que el 56 % de los adolescentes estadounidenses encuestados apoyaba los requisitos de verificación de edad en las redes sociales.[208,209] Sin embargo, los jóvenes también destacan sus preocupaciones sobre la privacidad, la seguridad y la inclusión digital.

> **«Si quieres protección, hay que sacrificar algo de libertad. Pero, como joven, también tengo derecho a explorar y descubrir cosas [en el mundo digital].»**

Joven[38]

Los detractores de las prohibiciones generales advierten de que restringir el acceso puede excluir o aislar a los jóvenes marginados, como las minorías sexuales y de género o los niños indocumentados, y empujarlos hacia espacios digitales no regulados.[210] Los datos del Reino Unido muestran que el uso de VPN se disparó tras las restricciones, lo que pone de relieve los retos que plantea la aplicación de la ley en un mundo conectado digitalmente.[211]

> «Cuando un niño necesita acceder a plataformas de streaming pero no tiene una cuenta, utiliza sitios ilegales que muestran anuncios emergentes inapropiados con contenido explícito.»

Defensor de los derechos de los niños, Kenia[38]

> «Las cuentas alternativas son un gran problema. Si a alguien le bloquean el acceso, puede crear una nueva cuenta. Hay muchas formas diferentes de eludir los bloqueos o las moderaciones.»

Niña de 13 años, Australia[38]

Equilibrio entre seguridad, privacidad y derechos

Los defensores argumentan que «la verificación de la edad no debería consistir en excluir a los niños, sino en permitirles el acceso de forma segura».[186] **La Política de Seguridad y Empoderamiento Infantil en Internet** de la Unión Africana (2024) adopta este enfoque basado en los derechos, promoviendo el acceso junto con la prevención.[212]

> «La verificación de la edad es una herramienta, no un fin en sí mismo, para que los jóvenes tengan experiencias positivas en línea. En el mejor de los casos, protege; en el peor, impide a los jóvenes acceder a información, expresión y conexión esenciales.»

Regulador[206]

Tabla 2. Métodos de verificación de la edad[213]

Método	Descripción	Preocupaciones principales
Autodeclaración	El usuario introduce su fecha de nacimiento o marca una casilla.	Fácil de implementar, pero poco fiable.[214]
Estimación de la edad	Predice la edad mediante algoritmos o datos biométricos.	Cómodo, pero propenso a sesgos y errores: los estudios muestran tasas de error de hasta el 34-73 % entre los adolescentes y sesgos raciales.[207,215]
Verificación de la edad	Requiere un documento de identidad oficial o una señal verificada.	Es el método más preciso, pero plantea problemas de privacidad, seguridad y exclusión, especialmente para quienes no disponen de un documento de identidad oficial.[216]

Aún no existe un estándar global para la verificación de la edad. Meta ha propuesto verificaciones en el dispositivo o en la tienda de aplicaciones, mientras que Google explora pruebas de conocimiento cero que confirman la elegibilidad sin revelar la identidad. Los responsables políticos y las empresas deben garantizar que los sistemas sean transparentes, respeten los derechos, preserven la privacidad, sean equitativos y se diseñen con los niños.

Desarrollo de capacidades, respuesta adaptada a los niños y justicia centrada en los supervivientes

Las leyes para proteger a los niños deben estar respaldadas por inversiones en formación, desarrollo de capacidades y reguladores dedicados. Los gobiernos deben garantizar que las fuerzas del orden, los fiscales y el poder judicial reciban formación continua en enfoques adaptados a los niños y sensibles al trauma, y que dispongan de los recursos necesarios para aplicarlos de manera eficaz. Los supervivientes de todas las regiones denuncian que las protecciones legislativas existentes son insuficientes o se aplican de forma deficiente, y reclaman una justicia centrada en los supervivientes.[60]

> **«Si lo denuncias a la policía... se reirán de ti. Por eso necesitamos unidades de delitos cibernéticos.»**
>
> *Defensor de los supervivientes*[60]

En Kenia, el Consejo Nacional de Administración de Justicia lanzó un manual de formación especializado para los actores del sector judicial sobre la investigación y el enjuiciamiento de los delitos sexuales contra menores facilitados por la tecnología.[217] Esta iniciativa refleja el

reconocimiento de la necesidad de prácticas adaptadas a los niños y sensibles al trauma dentro del sistema judicial, que vayan más allá de la legislación para apoyar respuestas eficaces centradas en las víctimas.

> **«Los sistemas jurídicos deben facilitarles la denuncia de los abusos sin miedo, y las plataformas en línea deben actuar con rapidez para eliminar cualquier contenido perjudicial.»**
>
> *Hombre de 15 años, Etiopía*[60]

Es fundamental la detección proactiva, independientemente de las denuncias de los supervivientes. Herramientas como el clasificador CSAM de Thorn (a través de Interpol) y el video basado en inteligencia artificial de Rigr AI mejoran la respuesta oportuna a los casos de abuso sexual infantil en directo.[218] [219]

Las fuerzas del orden señalan constantemente que se necesitan más recursos para gestionar el creciente número de denuncias recibidas por las líneas directas, ya que estas aumentan exponencialmente, en parte debido a la IA generativa. También se necesita capacidad adicional para apoyar el bienestar del personal de las líneas directas y de los primeros intervinientes, y para financiar investigaciones proactivas que puedan cortar la producción y el consumo de CSAM.[79] La formación de la policía de Camboya sobre la CSEA facilitada por la tecnología ilustra cómo crear sistemas inclusivos y centrados en los niños.[220]

Del mismo modo, la Asociación Canadiense de Jefes de Policía ha adoptado un marco para una policía informada sobre el trauma, basado en seis pasos, el **modelo de** las seis **«R»:** Realizar, Reconocer, Repensar, Responder, Reducir, Revisar.[221] Cuando los sistemas están informados sobre el trauma y son adaptados a la niñez, reducen el daño de culpar a la víctima, lo que desalienta la denuncia, empeora los impactos a largo plazo y debilita la detección y la respuesta.

> **«Especialmente en mi país, nunca he visto que culpen a la persona que está captando a los niños. Siempre es: "¿Por qué lo has hecho? Es tu propio teléfono, ¿por qué has dejado que esto ocurriera?".»**
>
> *Niña de 14 años, Etiopía*[60]

Coordinación intersectorial global para abordar la extorsión sexual financiera

La coordinación global entre sectores, incluyendo las fuerzas del orden, el gobierno, la industria y los proveedores de servicios, es esencial para una prevención eficaz, especialmente en los casos de extorsión sexual financiera. ECPAT recomienda reforzar aún más las medidas intersectoriales mediante:[222]

- Obligar a las instituciones financieras a detectar y denunciar activamente las transacciones relacionadas con la explotación sexual infantil.
- Adaptar las herramientas de vigilancia a las nuevas tendencias, como los monederos digitales y las criptomonedas.
- Reformar las leyes de secreto bancario para permitir la colaboración con los servicios policiales más allá de la policía financiera.

Prevención de la extorsión sexual de niños en línea: conclusiones del Centro Australiano para Combatir la Explotación Infantil, dirigido por la Policía Federal Australiana

Los datos publicados por el Centro Australiano para Combatir la Explotación Infantil (ACCCE) en 2023 identificaron una tendencia emergente: los delincuentes extranjeros se centran principalmente en los adolescentes varones para la extorsión sexual financiera.[223] Más del 90 % de las denuncias relacionadas con la extorsión sexual financiera involucraban a víctimas jóvenes de sexo masculino. Las denuncias de extorsión sexual financiera en línea dirigidas a niños australianos aumentaron casi un 60 % entre diciembre de 2022 y el comienzo del año escolar 2023, lo que sugiere un aumento durante las vacaciones escolares.[223]

Desde enero de 2024, la ACCCE ha registrado un descenso en las denuncias de extorsión sexual financiera, probablemente debido a la actividad coordinada de las fuerzas del orden, los mensajes de prevención y los esfuerzos educativos. Sin embargo, se cree que muchos incidentes no se denuncian, y la extorsión sexual de niños sigue siendo una preocupación y una prioridad importantes.

Una característica central del enfoque de la ACCCE es la colaboración intersectorial para difundir mensajes de prevención a gran escala.

> « Se necesita toda una red y un ecosistema para que la prevención tenga éxito. »
>
> *Agente de las fuerzas del orden*[79]

Las asociaciones reúnen a las fuerzas del orden, la industria, las ONG y las organizaciones comunitarias para llegar a públicos diversos con intervenciones personalizadas. Algunos ejemplos son:

- Divulgación dirigida a los jóvenes: la ACCCE ha colaborado con Kids Helpline, Meta y el programa estadounidense de prevención para jóvenes **NoFiltr** para publicar recursos educativos para jóvenes de entre 13 y 17 años, en los que se ofrece información sobre cómo prevenir y responder a la extorsión sexual. Estos materiales también orientan a los padres y cuidadores sobre cómo reconocer los riesgos, denunciar los incidentes y acceder a la ayuda necesaria.[223]
- Prevención centrada en la familia: la ACCCE colaboró con Project Paradigm en **It's Never Too Early**, una campaña que anima a los padres, cuidadores y familias que esperan un hijo a iniciar conversaciones tempranas sobre la prevención del abuso sexual infantil.[224]
- Campañas de comunicación masiva: para llegar directamente a los grupos de alto riesgo, la ACCCE desarrolló un anuncio animado de 30 segundos dirigido a chicos de entre 13 y 17 años, que se emitió en Snapchat y llegó a unos cinco millones de personas.[79, 225]

Figura 9. Campaña animada contra la extorsión sexual en Snapchat

- Educación y formación: **ThinkUKnow**, dirigido por la Policía Federal Australiana, dota a las escuelas, las familias y los grupos comunitarios de herramientas prácticas para abordar la seguridad en línea y los riesgos de extorsión sexual. Los recursos incluyen presentaciones, hojas informativas, tarjetas de conversación, paquetes de actividades y materiales adaptados culturalmente para comunidades lingüísticamente diversas, que ofrecen múltiples puntos de partida para debatir sobre los riesgos en línea.[152]

Aunque la ACCCE recopila activamente datos de participación, como el número de presentaciones realizadas y el público alcanzado, sigue siendo difícil medir el verdadero impacto de los esfuerzos de prevención, ya que muchos resultados no son directamente visibles en los datos. El enfoque de la ACCCE se centra en dotar a los padres y cuidadores de herramientas prácticas e información, reconociendo su papel clave en el apoyo a la seguridad de los niños en Internet. Los esfuerzos en curso tienen como objetivo llegar a las familias menos propensas a participar y reforzar las iniciativas de educación y sensibilización en todas las comunidades.

Conclusión

La CSEA facilitada por la tecnología es una amenaza global que se puede prevenir. La tarea que tenemos por delante es clara: cerrar las brechas de evidencia, identificar y ampliar lo que funciona, y acelerar la traducción del conocimiento en acción. En un entorno de financiación limitada, esto significa maximizar el impacto mediante el intercambio de conocimientos y pruebas, la coordinación de agendas y las lecciones extraídas de la CSEA fuera de línea y de los esfuerzos más amplios de prevención de la violencia. Para construir un mundo digital más seguro, debemos fortalecer los eslabones más débiles, reconociendo que los riesgos y los daños migran a los espacios menos protegidos, y garantizar que todos la niñez se beneficie del mismo nivel de protección. Una prevención eficaz depende de situar los derechos y las voces de los niños en el centro, invertir en medidas sostenibles y basadas en pruebas, y reforzar la colaboración entre todos los sectores y partes interesadas. A través de la responsabilidad compartida, la comunidad mundial puede acelerar el progreso hacia un entorno digital más seguro en el que los niños puedan aprender, jugar y conectarse sin sufrir explotación ni abusos.

> **«Del dolor al propósito, de la supervivencia a la fortaleza.»**
>
> *Superviviente, Filipinas*[138]

Agradecimientos

Cita sugerida: WeProtect Global Alliance (2025). Global Threat Assessment 2025, Preventing technology-facilitated child sexual exploitation and abuse: From insights to action (by Lau LS, Mayevskaya Y, Fanton d'Andon C, Ware M, and Hermosilla S). WeProtect Global Alliance: https://www.weprotect.org/global-threat-assessment-25/

Autores

WeProtect Global Alliance

WeProtect Global Alliance es un movimiento mundial que reúne a más de 350 organizaciones gubernamentales, del sector privado y de la sociedad civil que trabajan para transformar la respuesta mundial a la explotación y el abuso sexual infantil en línea.

Care and Protection of Children (CPC) Learning Network, Universidad de Columbia

La Red de Aprendizaje CPC, con sede en la Escuela Mailman de Salud Pública de la Universidad de Columbia, promueve la salud y el bienestar de los niños a través de la investigación, las políticas y la práctica. Con socios en más de 20 países, la CPC genera pruebas y herramientas rigurosas y basadas en la realidad local para fortalecer los sistemas de protección infantil y promover el bienestar de la niñez, la juventud y las familias en todo el mundo.

La investigación y redacción de este informe estuvieron a cargo de Ling San Lau, Yana Mayevskaya, Sabrina Hermosilla, Cécile Fanton d'Andon y Matthew Ware, con aportes adicionales de Claire Cunningham, Hannah Thompson, Cassie Landers, Hanna-Tina Fischer, Jonathan Huynh y Lisberma Peralta Aquino.

WeProtect Global Alliance desea agradecer a todas las organizaciones y personas que han apoyado la elaboración de la Evaluación de amenazas globales 2025. Agradecemos sinceramente a los niños y supervivientes cuyas experiencias y conocimientos han servido de base para este informe y guían los esfuerzos colectivos para garantizar la seguridad de la niñez. El apoyo prestado a la elaboración del informe, como miembro del Comité Directivo o colaborador, no implica el respaldo (total o parcial) del contenido.

Comité Directivo de Expertos

Aengus Ó Dochartaigh	MOORE | Prevención del abuso sexual infantil, Universidad Johns Hopkins
Afrooz Kavani Johnson	Unicef
Anil Raghuvanshi	ChildSafeNet
Beth Hepworth	PGI
Carolina Piñeros	RedPapaz
Dan Sexton	Fundación para la Vigilancia en Internet (IWF)
Debra Clelland	DeafKidz International
Elena Martellozzo	Childlight, Instituto Global para la Seguridad Infantil, Universidad de Edimburgo
James Smith	PGI
Jess Lishak	Tech Coalition
Nina Vaaranen-Valkonen	Protect Children
Ricardo de Lins e Horta	Gobierno de Brasil
Sambath Sokunthea	Gobierno de Camboya
Soyoung Park	Organismo regulador de Corea del Sur, KCSC
Wirawan Boom Mosby	Proyecto HUG Tailandia

Colaboradores

Las siguientes organizaciones proporcionaron información sobre los supervivientes y los jóvenes para nuestra investigación:

VoiceBox

Una empresa social con sede en el Reino Unido y dirigida por jóvenes que amplifica las voces de los jóvenes de entre 13 y 25 años. Organizó dos sesiones con jóvenes entre 14 y 18 años de siete países, entre los que se encontraban comunidades marginadas, refugiados y supervivientes de genocidios. Sus opiniones han servido de base para el informe y el marco de prevención.

Secrets Worth Sharing

Una organización con sede en el Reino Unido que promueve el debate abierto sobre el abuso sexual infantil a través de podcasts, talleres y eventos. Secrets Worth Sharing revisó las herramientas de investigación cualitativa y aportó las perspectivas de los supervivientes que se han incorporado al informe.

Fundación Marie Collins

Apoya a las víctimas y/o supervivientes de abusos sexuales infantiles asistidos por tecnología, así como a sus familias y a los profesionales que trabajan con ellos, proporcionando servicios de defensa, educación y recuperación. La Fundación Marie Collins revisó las herramientas de investigación cualitativa, aportó las opiniones de los supervivientes y facilitó un taller con ellos para revisar el marco de prevención.

Misión Internacional de Justicia (IJM) Filipinas

Organización mundial que lucha contra la trata de personas, la esclavitud moderna y la explotación y el abuso de niños. IJM aportó las opiniones de los supervivientes relevantes para el marco de prevención y las integró en todo el informe.

Footprints to Freedom

Organización con sede en los Países Bajos, dirigida por supervivientes, que empodera a las víctimas de la trata de personas; lleva a cabo intervenciones de base en Uganda, Kenia y Ruanda; y amplía iniciativas en toda África a través de su Coalición Africana de Supervivientes. Huellas hacia la libertad aportó las perspectivas de los supervivientes que se incorporaron en todo el informe.

Protect Children

Con sede en Helsinki, Protect Children defiende el derecho de todos los niños a no sufrir violencia sexual, desarrolla programas de prevención e investiga y rehabilita a los agresores. Protect Children contribuyó con un prólogo de un superviviente y aportó ideas adicionales que se incluyen a lo largo del informe.

Además de nuestro Comité Directivo de Expertos, las siguientes personas y organizaciones ofrecieron sus opiniones para orientar esta investigación:

- ECPAT
- Unión Europea
- Red Global de Reguladores de Seguridad en Internet (GOSRN)
- Google
- INHOPE
- Organización Internacional de Policía Criminal (Interpol)
- Fundación Lucy Faithfull
- Centro Nacional para Niños Desaparecidos y Explotados (NCMEC)
- Agencia Nacional contra el Crimen (NCA)
- Organización Nacional para el Tratamiento del Abuso (NOTA)
- Centro Safe Futures
- Snap
- Grupo de Trabajo Virtual Global (VGT)
- Foro Económico Mundial

Safe Futures Hub

El marco de prevención se desarrolló como parte del Safe Futures Hub, una iniciativa conjunta de la Iniciativa de Investigación sobre la Violencia Sexual (SVRI), Together for Girls y la Alianza Global WeProtect, que trabaja para promover soluciones para poner fin a la violencia sexual contra los niños.

El diseño visual y la maquetación del informe fueron desarrollados por Rec Design. El marco de prevención fue diseñado visualmente por Together Creative

Mantenerse al día con las pruebas emergentes

Tabla 3. Selección de publicaciones pendientes y recursos vivos

Nombre de la iniciativa	Descripción	Prevista
Disrupting Harm 2 (investigación realizada conjuntamente por Unicef, Innocenti, ECPAT e Interpol)	Ampliación de las encuestas poblacionales con niños y cuidadores, así como entrevistas en profundidad con jóvenes supervivientes en otros 12 países, para mejorar la comprensión global de la explotación y el abuso sexual infantil en línea.	**2025-2026**
Global Boys Initiative (ECPAT)	Una próxima publicación presentará un estudio de caso de Pakistán con testimonios de supervivientes y profesionales, en el que se destacarán las iniciativas para prevenir y responder a la explotación sexual de los niños.	**2025-2026**
INSPIRE: Siete estrategias para poner fin a la violencia contra los niños (desarrolladas por la OMS con socios mundiales)	**INSPIRE** es un paquete técnico basado en datos empíricos que describe siete estrategias y dos actividades transversales para prevenir la violencia contra los niños de 0 a 17 años. Ayuda a los países a coordinar acciones multisectoriales y a realizar un seguimiento de los progresos.	**En curso**
Prevención Global (impartido por MOORE | Prevención del abuso sexual infantil, la Escuela de Salud Pública Bloomberg de la Universidad Johns Hopkins y el Instituto Real de Investigación en Salud Mental)	Lanzada en 2024, **Prevention Global** es una plataforma de conocimiento y una ambiciosa iniciativa de investigación que evalúa siete programas desarrollados para prevenir el abuso sexual infantil y que lleva a cabo encuestas de referencia sobre la prevalencia de los abusos en cuatro continentes (Brasil, Alemania, Tanzania y Estados Unidos).[176] También publica productos de conocimiento que exploran aspectos clave de la prevención, entre ellos **Serving Youth**, que abarca la prevalencia de la victimización en entornos que atienden a jóvenes en Estados Unidos y ofrece una guía práctica para líderes; **Scalability,** que explora las barreras y oportunidades para ampliar los programas; y **Making The Case**, que revela la percepción pública del abuso sexual infantil como un problema prevenible.[125,176,226]	**2026**

Nombre de la iniciativa	Descripción	Prevista
Comportamiento responsable con jóvenes y niños (RBYC)[74]	**RBYC** es un programa para niños de 11 a 14 años que tiene como objetivo prevenir comportamientos sexuales problemáticos y ayudar a los adolescentes a desarrollar interacciones seguras y apropiadas, tanto con niños más pequeños como con sus compañeros y adultos, tanto en línea como fuera de línea. Se ha probado en Estados Unidos y actualmente se está adaptando y evaluando en 24 escuelas de Alemania (22 en ensayos controlados aleatorios y 2 en estudios piloto).	**2026**
Safe Futures Hub Revisión sistemática global y marco PbK	Safe Futures Hub, en colaboración con la Universidad de Oxford, está desarrollando una **revisión sistemática de la vida global** para proporcionar pruebas continuamente actualizadas sobre la prevención de la violencia sexual infantil, centrándose en los países de ingresos bajos y medios. En diciembre de 2025, el centro también pondrá en marcha su **marco de conocimientos basados en la práctica (PbK)**, que reconoce la experiencia vivida, incorpora las voces infrarrepresentadas y destaca por qué y cómo las intervenciones tienen éxito en contextos del mundo real.	**2025-2026**

Glosario de términos

Material de abuso sexual infantil (CSAM) generado por inteligencia artificial (IA)	El uso indebido de tecnologías de IA para crear, total o parcialmente, cualquier representación sexualizada o sexualmente explícita de un niño/a. Esto incluye imágenes, videos, audio, animaciones u otros medios producidos por IA. Es una forma de CSAM generado digitalmente (DG-CSAM) (véase el término relacionado «deepfakes»).[26]
Agrupación	Función que consolida los informes relacionados con incidentes generalizados, como contenidos virales, en un único informe o en un conjunto más reducido de informes, lo que reduce los envíos redundantes y permite conservar la información sobre todos los usuarios e incidentes denunciados.[12]
Chatbots	Herramienta conversacional automatizada, a menudo impulsada por IA, que puede simular a niños o adultos e interactuar con los usuarios como compañeros, asesores o amigos, pero que puede plantear riesgos como la desinformación, la recopilación de datos o la exposición a contenidos inapropiados.[59]
Material de abuso sexual infantil (CSAM)	Material, como imágenes o videos, que muestra y/o documenta actos de abuso sexual y/o explotación de menores. Este material puede utilizarse en investigaciones de inteligencia criminal y/o servir como prueba en juicios penales.[26]
Abuso sexual infantil en línea	Cualquier forma de abuso sexual infantil relacionada con el entorno digital. Esto incluye el abuso sexual infantil facilitado por la tecnología y cometido en otros lugares, que luego se repite al compartirlo en línea a través de las redes sociales u otras dimensiones digitales.[26]
Explotación sexual infantil en línea	Cualquier acto de carácter sexualmente explotador cometido contra un niño en relación con el entorno digital. Esto incluye cualquier uso de la tecnología que dé lugar a la explotación sexual o provoque que un niño/a sea explotado sexualmente, o que dé lugar o provoque la producción, compra, venta, posesión, distribución o transmisión de imágenes u otro material que documente dicha explotación sexual. En comparación con el abuso, el intercambio o la distribución de objetos de valor, incluyendo, entre otros, imágenes o videos, suelen ser componentes de la explotación.[26]
Deepfake	Un deepfake es un contenido generado por IA (por ejemplo, una foto, un video, una animación o un audio) que representa de forma realista a una persona haciendo o diciendo algo que nunca ha hecho.[227] Puede utilizarse para referirse a contenidos que representan a niños reales en situaciones sexualizadas simuladas.
Bienestar digital	Impacto de las tecnologías en la salud mental, física, social y emocional de una persona.[228]

Cifrado de extremo a extremo	Método de seguridad que garantiza que solo el remitente y el destinatario puedan acceder al contenido de una comunicación, impidiendo que terceros, incluidos los proveedores de servicios, vean o escaneen los datos.[229]
Inteligencia artificial generativa (IA)	La IA generativa es una forma de inteligencia artificial que utiliza modelos de aprendizaje automático para analizar los patrones y la estructura de sus datos de entrenamiento con el fin de crear nuevos contenidos, incluyendo texto, imágenes, audio u otros medios, que imitan esos inputs.[230]
Grooming	El grooming o grooming en línea se refiere al proceso de establecer/construir una relación con un niño/a, ya sea en persona o mediante el uso de Internet u otras tecnologías digitales, con el fin de facilitar el contacto sexual con esa persona. En el informe, el grooming sin calificativos se refiere al grooming con fines sexuales.[26]
Comportamientos sexuales perjudiciales	Acciones sexuales iniciadas por un niño o joven que son inapropiadas para su desarrollo, coercitivas o abusivas, y que pueden causar daño a sí mismos o a otros. El comportamiento sexual problemático se refiere a acciones sexuales que pueden ser inapropiadas o preocupantes, pero que no alcanzan el umbral de daño o abuso. Este informe utiliza el término «comportamientos sexuales dañinos» para abarcar todo el espectro de comportamientos preocupantes, al tiempo que reconoce que los comportamientos en fase inicial o menos graves siguen requiriendo intervención para evitar que se agraven.[108]
Coincidencia de hash	Se utiliza un algoritmo conocido como "función hash" para calcular una huella digital, conocida como hash, a partir de un archivo. La comparación de dicho hash con otro hash almacenado en una base de datos se denomina coincidencia de hash. En el contexto de la seguridad en línea, la coincidencia de hash puede ser un medio para la detección de imágenes y videos conocidos como ilegales o perjudiciales.[231]
Abuso transmitido en directo	A menudo transmitido a los espectadores a través de plataformas de transmisión en directo específicas o redes sociales, el contenido se entrega de forma instantánea, lo que permite a los espectadores verlo y participar mientras se produce el abuso. En comparación con otros formatos, esto puede dejar menos huellas digitales del abuso.[26]
Compartir imágenes íntimas sin consentimiento (NCII)	Término comúnmente asociado a los adultos que se refiere al intercambio de imágenes sexuales o sexualmente sugerentes sin el consentimiento de la persona representada. Esto puede ocurrir cuando el contenido compartido inicialmente de forma consensuada se comparte o reenvía posteriormente sin consentimiento, o cuando las imágenes se toman sin consentimiento (como en el contexto del grooming o la extorsión sexual). El concepto clave es la «pérdida de control» sobre las representaciones.[26] Este término requiere precaución cuando se utiliza en relación con niños que no han alcanzado la edad de consentimiento sexual (véase contenido sexual relacionado, generado/producido en primera persona, en el que participan niños).
Delincuente	Persona que ha cometido delitos o es culpable de un delito relacionado con la explotación y el abuso sexual infantil.[26]

Seducción en línea	Cuando una persona se comunica con un niño a través de Internet (u otra tecnología) con la intención de cometer un delito sexual o un secuestro.[232]
Perpetrador	Persona que puede haber participado en la explotación sexual de menores (independientemente de su participación en el proceso penal). Utilizamos los términos «autor» y «autor potencial» para referirnos a las personas que han cometido o pueden cometer estos actos, independientemente de si cumplen la definición específica de delito o han sido detenidas o condenadas por un delito.[26]
Contenido sexual autogenerado en el que participan niños	Los niños y adolescentes menores de 18 años pueden tomar fotos o grabar vídeos sexuales de sí mismos. Aunque esta conducta en sí misma no es necesariamente ilegal ni socialmente inaceptable, existe el riesgo de que dicho contenido pueda difundirse en línea o en persona para dañar a los niños o utilizarse como base para la extorsión. Utilizamos este término, así como «sexting», que es una referencia coloquial común para referirse a la toma y el intercambio de imágenes de naturaleza sexual. Los niños suelen decir que no se identifican con la noción de contenido «autogenerado» y, en contextos como el intercambio no consentido, puede resultar inútil.[233]
Extorsión sexual de niños	Proceso por el cual se coacciona a los niños para que sigan produciendo material sexual y/o realizando actos angustiosos bajo la amenaza de exponer ante otros el material en el que aparecen. Cuando la motivación es principalmente económica, también utilizamos el término «extorsión sexual económica».[26]
Superviviente	Personas que han sufrido daños y victimización. El uso del término «superviviente» puede reflejar un proceso de curación. Reconociendo la variedad de preferencias que tienen las personas con experiencia vivida en cuanto a la terminología, utilizamos los términos «víctima» y «superviviente» de forma intercambiable en el informe.[26]
Explotación y abuso sexual infantil facilitado por la tecnología (CSEA facilitado por la tecnología, también denominado TFCSEA)	La CSEA facilitada por la tecnología se refiere al uso de tecnologías digitales en cualquier etapa para preparar, cometer o difundir (en el caso del CSAM) la explotación sexual o el abuso sexual de un niño/a. Abarca los daños cometidos tanto en entornos digitales como no digitales (fuera de línea), incluyendo, por ejemplo, el intercambio de información, la coordinación de acciones y el contacto con niños para prepararlos o coaccionarlos. Este término reconoce que la tecnología desempeña un papel en la facilitación del abuso y en la perpetuación de los daños causados por el abuso, tanto en el espacio físico como en el digital.[26]
Víctima	Personas que han sido objeto de actos perjudiciales y/o delictivos como titulares de derechos. Reconociendo la variedad de preferencias que tienen las personas con experiencia vivida en cuanto a la terminología, utilizamos este término de forma intercambiable con «superviviente» en el informe.[26]

Referencias

1. Navigating the Unknown: Reflections on AI, the Metaverse, and Keeping Young People Safe | VoiceBox [Internet]. [cited 2025 Sept 27]. Available from: https://voicebox.site/article/navigating-unknown-reflections-ai-metaverse-and-keeping-young-people-safe
2. MOORE | Preventing Child Sexual Abuse | Johns Hopkins Bloomberg School of Public Health [Internet]. [cited 2025 Sept 27]. Available from: https://publichealth.jhu.edu/moore-center-for-the-prevention-of-child-sexual-abuse
3. United Nations Department of Economic and Social Affairs [Internet]. Global Internet Use Continues To Rise But Disparities Remain. [cited 2025 Nov 20]. Available from: https://social.desa.un.org/sdn/global-internet-use-continues-to-rise-but-disparities-remain
4. GSMA. Smartphone owners are now the global majority, New GSMA report reveals [Internet]. Newsroom. 2023 [cited 2025 Nov 4]. Available from: https://www.gsma.com/newsroom/press-release/smartphone-owners-are-now-the-global-majority-new-gsma-report-reveals/
5. ITU. Statistics [Internet]. [cited 2025 Nov 21] . Available from: https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx
6. Generative AI: Risks and opportunities for children | Innocenti Global Office of Research and Foresight [Internet]. [cited 2025 Aug 29]. Available from: https://www.unicef.org/innocenti/generative-ai-risks-and-opportunities-children
7. Industry. Data collected by the CPC Learning Network through key informant interviews.
8. Academic. Data collected by the CPC Learning Network through key informant interviews.
9. Intergovernmental. Data collected by the CPC Learning Network through key informant interviews.
10. Safe Online. Disrupting Harm [Internet]. Available from: https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf
11. Civil Society. Data collected by the CPC Learning Network through key informant interviews.
12. National Center for Missing and Exploited Children. CyberTipline Data [Internet]. [cited 2025 Sept 3]. Available from: https://ncmec.org/gethelpnow/cybertipline/cybertiplinedata
13. INHOPE Releases Annual Report 2024 [Internet]. [cited 2025 May 5]. Available from: https://inhope.org/EN/articles/inhope-annual-report-2024
14. IWF 2024 Annual Data & Insights Report [Internet]. [cited 2025 May 6]. Available from: https://www.iwf.org.uk/annual-data-insights-report-2024/
15. How AI is being abused to create child sexual abuse material (CSAM) online [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/
16. 118th Congress. S.474 - REPORT Act [Internet]. 2024. Available from: https://www.congress.gov/bill/118th-congress/senate-bill/474

17. UK Public General Acts. Online Safety Act 2023 [Internet]. 50 Oct 26, 2023. Available from: https://www.legislation.gov.uk/ukpga/2023/50

18. Social media ban in Australia | A simple guide [Internet]. UNICEF Australia. [cited 2025 Sept 27]. Available from: https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer?srsltid=AfmBOop6gJckegYUrtle7BkiDMa6ZKUVy0aaGjHrYShDthWRHUqp8_9A

19. Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos. LEI No 15.211, DE 17 DE SETEMBRO DE 2025 [Internet]. Available from: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm

20. Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos. LEI No 15.100, DE 13 DE JANEIRO DE 2025 [Internet]. Available from: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15100.htm

21. New Online Safety Code of Practice for App Distribution Services Enhances Protection for Singapore Users [Internet]. Infocomm Media Development Authority. [cited 2025 Aug 29]. Available from: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-code-of-practice-for-app-distribution-services

22. Making the digital and physical world safer: Why the Convention against Cybercrime matters | UN News [Internet]. 2024 [cited 2025 Sept 27]. Available from: https://news.un.org/en/story/2024/12/1158526

23. UN Cybercrime Convention - Full Text [Internet]. United Nations : Office on Drugs and Crime. [cited 2025 Aug 25]. Available from: //www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

24. Global Digital Compact | Office for Digital and Emerging Technologies [Internet]. [cited 2025 Sept 10]. Available from: https://www.un.org/digital-emerging-technologies/global-digital-compact

25. Lantern: advancing child safety through signal sharing [Internet]. https://technologycoalition.org/. [cited 2025 Sept 27]. Available from: https://technologycoalition.org/programs/lantern/

26. ECPAT. Terminology Guidelines [Internet]. 2025 [cited 2025 Aug 29]. Available from: https://ecpat.org/terminology/

27. Call for consultants, global Living Systematic Review consultant(s):... [Internet]. Safe Futures Hub. [cited 2025 Sept 27]. Available from: https://www.safefutureshub.org/call-for-consultants-global-living-systematic-review-consultants-what-works-to-prevent-childhood-sexual-violence

28. Prevention Global. Prevention Global launches with new online resource hub and landmark impact evaluations [Internet]. [cited 2025 Sept 27]. Available from: https://www.prevention.global/

29. Model National Response to end child sexual exploitation & abuse online - WeProtect Global Alliance [Internet]. 2020 [cited 2025 May 1]. Available from: https://www.weprotect.org/resources/frameworks/model-national-response/

30. Bronfenbrenner U. Toward an experimental ecology of human development. Am Psychol. 1977;32(7):513–31.

31. UNICEF. Corporate reporting on child rights in relation to the digital environment [Internet]. Available from: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/reporting

32. Workshop. Data collected by the CPC Learning Network through key informant interviews.

33. Convention on the Rights of the Child, 20 November 1989 [Internet]. [cited 2025 Sept 10]. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/crc-1989

34. OHCHR. General comment No. 25 (2021) on children's rights in relation to the digital environment [Internet]. OHCHR. [cited 2025 Nov 3]. Available from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

35. United Nations. Guiding Principles on Business and Human Rights : Implementing the United Nations "Protect, Respect and Remedy" Framework [Internet]. Available from: https://digitallibrary.un.org/record/720245?v=pdf

36. UNICEF. Children's Rights Business Principles 2012 [Internet]. [cited 2025 Nov 3]. Available from: https://www.unicef.org/media/96136/file/Childrens-Rights-Business-Principles-2012.pdf

37. WeProtect Global Alliance. Children and Young People present their roadmap for a safer digital world [Internet]. Available from: https://www.weprotect.org/news/children-and-young-people-present-their-roadmap-for-a-safer-digital-world/

38. SafetyNet: insights from young people around the world [Internet]. Safe Futures Hub. [cited 2025 Sept 22]. Available from: https://www.safefutureshub.org/resources/safetynet-insights-from-young-people-around-the-world

39. Thorn. Evolving Technologies Horizon Scan [Internet]. Available from: https://www.thorn.org/research/library/evolving-technologies-horizon-scan/

40. UNICEF. Childhood in a Digital World [Internet]. [cited 2025 Nov 20]. Available from: https://www.unicef.org/innocenti/reports/childhood-digital-world

41. 10 countries with the highest percentage of web traffic from mobile phones | Business Insider Africa [Internet]. [cited 2025 Aug 29]. Available from: https://africa.businessinsider.com/local/lifestyle/10-countries-with-the-highest-percentage-of-web-traffic-from-mobile-phones/04wvy3f

42. Facts and Figures 2024 - Youth Internet use [Internet]. [cited 2025 Aug 29]. Available from: https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-youth-internet-use

43. Slater SO, Arundell L, Grøntved A, Salmon J. Age of first digital device use and screen media use at age 15: A cross-sectional analysis of 384,591 participants from 55 countries. Public Health Pract [Internet]. 2025 June 1 [cited 2025 Sept 2];9:100596. Available from: https://www.sciencedirect.com/science/article/pii/S2666535225000151

44. Coded Companions: Young People's Relationships With AI Chatbots | VoiceBox [Internet]. [cited 2025 Sept 27]. Available from: https://voicebox.site/article/coded-companions-young-peoples-relationships-ai-chatbots

45. Snap Digital Well-Being Index | Snapchat Safety [Internet]. [cited 2025 Sept 27]. Available from: https://values.snap.com/safety/dwbi

46. Häubi RB. How the UN plans to connect every school to the internet by 2030 [Internet]. SWI swissinfo.ch. 2024 [cited 2025 Sept 2]. Available from: https://www.swissinfo.ch/eng/international-geneva/the-un-plans-to-connect-every-school-to-the-internet-by-2030/83325727

47. Peng D, Yu Z. A Literature Review of Digital Literacy over Two Decades. Educ Res Int [Internet]. 2022 [cited 2025 Sept 3];2022(1):2533413. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/2533413

48. World Health Organization. 1st Global Ministerial Conference on Ending Violence Against Children [Internet]. [cited 2025 Nov 4]. Available from: https://www.who.int/teams/social-determinants-of-health/violence-prevention/1st-global-ministerial-conference-on-ending-violence-against-children

49. INHOPE. Launching Version 3 of the Universal Classification Schema [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://inhope.org/EN/articles/what-s-new-in-version-3-of-the-universal-classification-schema

50. WeProtect Global Alliance. Child protection online: Global legislative, regulatory and policy update January 2025.

51. WeProtect Global Alliance. Child protection online: Global legislative, regulatory and policy update June 2025.

52. Patchin JW, Hinduja S. The nature and extent of youth sextortion: Legal implications and directions for future research. Behav Sci Law. 2024;42(4):401–16.

53. MikeHarrison. Global Taskforce on child sexual abuse online - WeProtect Global Alliance [Internet]. 2022 [cited 2025 Nov 3]. Available from: https://www.weprotect.org/global-taskforce-on-child-sexual-abuse-online/

54. Government. Data collected by the CPC Learning Network through key informant interviews.

55. Transparency reporting on child sexual exploitation and abuse online [Internet]. 2023 Sept [cited 2025 Sept 30]. (OECD Digital Economy Papers; vol. 357). Report No.: 357. Available from: https://www.oecd.org/en/publications/transparency-reporting-on-child-sexual-exploitation-and-abuse-online_554ad91f-en.html

56. Grossman S, Pfefferkorn R, Thiel D, Shah S, DiResta R, Perrino J, et al. The Strengths and Weaknesses of the Online Child Safety Ecosystem. 2024 Apr 22 [cited 2025 Sept 5]; Available from: https://purl.stanford.edu/pr592kc5483

57. Childlight Into the Light Index [Internet]. [cited 2025 Apr 30]. Available from: https://www.childlight.org/into-the-light

58. 2024 Annual Report [Internet]. National Center for Missing & Exploited Children. [cited 2025 Aug 25]. Available from: http://www.missingkids.org/content/ncmec/en/footer/about/annual-report.html

59. UNICEF. The risky new world of tech's friendliest bots [Internet]. Available from: https://www.unicef.org/innocenti/stories/risky-new-world-techs-friendliest-bots

60. Data from the youth consultations led by Voicebox.

61. Davis P. Spike in online crimes against children a "wake-up call" [Internet]. National Center for Missing & Exploited Children. [cited 2025 Sept 27]. Available from: http://www.ncmec.org/content/ncmec/en/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call.html

62. Deepfake Nudes & Young People: Navigating a New Frontier in Technology-facilitated Nonconsensual Sexual Abuse and Exploitation [Internet]. Thorn. [cited 2025 Sept 5]. Available from: https://www.thorn.org/research/library/deepfake-nudes-and-young-people/

63. Online child sex abuse material, boosted by AI, is outpacing Big Tech's regulation [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/iwf-in-the-news/online-child-sex-abuse-material-boosted-by-ai-is-outpacing-big-techs-regulation/

64. Thiel D, DiResta R, Stamos A. Cross-Platform Dynamics of Self-Generated CSAM. 2023 June 6 [cited 2025 Aug 25]; Available from: https://fsi.stanford.edu/publication/cross-platform-dynamics-self-generated-csam

65 How Instagram's Algorithm Connects and Promotes Pedophile Network - Tech News Briefing - WSJ Podcasts [Internet]. [cited 2025 Aug 25]. Available from: https://www.wsj.com/podcasts/tech-news-briefing/how-instagrams-algorithm-connects-and-promotes-pedophile-network/A683C0B4-2E6F-4661-9973-10BD455DB895

66. AI enabling 'DIY child abuse' tools, with child victims in models, IWF warns MPs [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/ai-giving-offenders-diy-child-sexual-abuse-tool-as-dozens-of-child-victims-used-in-ai-models-iwf-warns-mps/

67. Aws Ai, Hugging Face, Inflection, Metaphysic, Stability AI, Teleperformance. Safety by Design for Generative AI: Preventing Child Sexual Abuse. Thorn [Internet]. 2024; Available from: https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf

68. Thorn. Synthetic Media Framework Case Study: Thorn. [cited 2025 Nov 4]; Available from: https://partnershiponai.org/wp-content/uploads/2024/11/case-study-thorn.pdf

69. Sivathasan N, Clahane P, Kemoli D. TikTok profiting from sexual livestreams involving children, BBC told. BBC [Internet]. 2025 Mar 2; Available from: https://www.bbc.com/news/articles/cedl8eyy4pjo

70. Ovaska A, Insoll T, Soloveva V, Vaaranen-Valkonen N, Di GR. Findings from Italian language respondents to Re-Direction surveys of CSAM users on dark web search engine. JRC Publ Repos [Internet]. 2025 [cited 2025 Nov 3]; Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC138231

71. FATF Annual Report 2023-2024 [Internet]. [cited 2025 Sept 30]. Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html

72. Protect Children. Tech Platforms Used by Online Child Sexual Abuse Offenders [Internet]. 2024. Available from: https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

73. Ending the Scourge: The Need for the STOP CSAM Act — Testimony of Michelle DeLaune, President and CEO, National Center for Missing & Exploited Children (PDF) [Internet]. Room 226, Dirksen Senate Office Building, Washington, DC; 2025 [cited 2025 Sept 5]. p. 16. Available from: https://www.judiciary.senate.gov/imo/media/doc/2025-03-11_testimony_delaune.pdf

74. Responsible Behavior with Youth and Children | MOORE | Preventing Child Sexual Abuse [Internet]. [cited 2025 Sept 5]. Available from: https://publichealth.jhu.edu/moore-center-for-the-prevention-of-child-sexual-abuse/responsible-behavior-with-youth-and-children

75. The emergence of immersive technologies and Extended Reality - WeProtect Global Alliance [Internet]. [cited 2025 May 1]. Available from: https://www.weprotect.org/thematic/extended-reality/

76. Child safeguarding and immersive technologies [Internet]. NSPCC Learning. [cited 2025 Aug 25]. Available from: https://learning.nspcc.org.uk/research-resources/2023/child-safeguarding-immersive-technologies

77. Data from Marie Collins Foundation survivor consultation session.

78. Edwards G, Christensen L. Cyber strategies used to combat child sexual abuse material [Internet]. Australian Institute of Criminology; 2021 [cited 2025 Nov 4]. Available from: https://www.aic.gov.au/publications/tandi/tandi636

79. Law enforcement. Data collected by the CPC Learning Network through key informant interviews.

80. Walsh K, Mathews B, Parvin K, Smith R, Burton M, Nicholas M, et al. Prevalence and characteristics of online child sexual victimization: Findings from the Australian Child Maltreatment Study. Child Abuse Negl. 2025 Feb;160:N.PAG-N.PAG.

81. Under 10s groomed online 'like never before' in 2023 find IWF [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/under-10s-groomed-online-like-never-before-as-hotline-discovers-record-amount-of-child-sexual-abuse/

82. Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/resource/girls-young-women-led-assessment-on-online-sexual-exploitation-abuse-technology-facilitated-gender-based-violence-in-africa/

83. Protecting Children From Violence and Exploitation in Relation to the Digital Environment | UNICEF [Internet]. [cited 2025 Sept 5]. Available from: https://www.unicef.org/documents/protecting-children-violence-and-exploitation-relation-digital-environment

84. Huang TF, Chun-Yin H, Fong-Ching C, Fong-Ching C, Chiu CH, Ping-Hung C, et al. Adolescent Use of Dating Applications and the Associations with Online Victimization and Psychological Distress. Behav Sci [Internet]. 2023;13(11):903. Available from: https://pubmed.ncbi.nlm.nih.gov/37998650/

85. Technology-facilitated Child Sexual Exploitation and Sexual Abuse in Burkina Faso, Côte d'Ivoire, Guinea and Niger [Internet]. ECPAT. [cited 2025 Sept 5]. Available from: https://ecpat.org/resource/technology-facilitated-child-sexual-exploitation-and-sexual-abuse-in-burkina-faso-cote-divoire-guinea-and-niger/

86. Pinto Cortez, Cristián & Guerra, Cristobal. Parental styles and online sexual abuse prevention factors. 2024. Límite (Arica). 19. 1-9. 10.4067/s0718-50652024000100209. Available from: https://www.researchgate.net/publication/383135600_Parental_styles_and_ online_sexual_abuse_prevention_factors

87. Wright MF. The Associations among Cyberbullying Victimization and Chinese and American Adolescents' Mental Health Issues: The Protective Role of Perceived Parental and Friend Support. Int J Environ Res Public Health [Internet]. 2024;21(8). Available from: https://pubmed.ncbi.nlm.nih.gov/39200678/

88. Friedman-Hauser G, Katz C. "She has a history of making things up": Examining the disclosure and reporting of online sexual abuse among children with disabilities. Child Abuse Negl [Internet]. 2025;163 ((Friedman-Hauser G., galf@haruv.org.il) The Bob Shapell School of Social Work, Tel Aviv University, Israel). Available from: https://awspntest.apa.org/record/2026-05574-001

89. Wright MF, Wachs S. Longitudinal
Associations between Different Types of Sexting, Adolescent Mental Health, and Sexual Risk Behaviors: Moderating Effects of Gender, Ethnicity, Disability Status, and Sexual
Minority Status. Arch Sex Behav [Internet]. 2024 Mar 1 [cited 2025 Sept 30];53(3):1115–28. Available from: https://doi.org/10.1007/s10508-023-02764-7

90. Gemara N, Mishna F, Katz C. 'If my parents find out, I will not see my phone anymore': Who do children choose to disclose online sexual solicitation to? Child Fam Soc Work [Internet]. 2025 [cited 2025 Sept 5];30(1):4–14. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1111/cfs.13069

91. Lusky-Weisrose E, Klebanov B, Friedman-Hauser G, Avitan I, Katz C. Online sexual abuse of children with disabilities: Analyzing reports of social workers' case files in Israel. Child Abuse Negl. 2024 Aug;154:N.PAG-N.PAG.

92. Hong JS, Kim J, Lee JM, Saxon S, Thornberg R. Pathways from Polyvictimization to Offline and Online Sexual Harassment Victimization Among South Korean Adolescents. Arch Sex Behav. 2023 Oct;52(7):2779–88.

93. Tanaya NLTP, Puteri NMM. Child Sexual Abuse and Exploitation through Livestreaming in Indonesia: Unequal Power Relations at the Root of Child Victimization. J Int Womens Stud [Internet]. 2023 Apr;25(3):1–14. Available from: https://vc.bridgew.edu/jiws/vol25/iss3/6

94. Children P. What Drives Online Child Sexual Abuse Offending? Understanding Motivations, Facilitators, Situational Factors, and Barriers [Internet]. Protect Children. 2024 [cited 2025 Aug 31]. Available from: https://www.suojellaanlapsia.fi/en/post/2know-final-report-1

95. Napier SS, Seto MC, Cashmore J, Shackel R. Characteristics that predict exposure to and subsequent intentional viewing of child sexual abuse material among a community sample of Internet users. Child Abuse Negl. 2024 Oct;156:106977.

96. Lahtinen HM, Honkalampi K, Insoll T, Nurmi J, Quayle E, Ovaska AK, et al. Investigating the disparities among child sexual abuse material users: Anonymous self-reports from both charged and uncharged individuals. Child Abuse Negl. 2025 Mar;161:107299.

97. Chauviré-Geib K, Gerke J, Fegert JM, Rassenhofer M. The Digital Dimension: Victim's Experiences of Technology's Impact on Penetrative Child Sexual Abuse. J Child Sex Abuse. 2025 Apr 28;1–21.

98. Christensen LS, Woods J. "It's Like POOF and It's Gone": The Live-Streaming of Child Sexual Abuse. Sex Cult. 2024 Aug 1;28(4):1467–81.

99. Ringrose J, Regehr K. Recognizing and addressing how gender shapes young people's experiences of image-based sexual harassment and abuse in educational settings. J Soc Issues. 2023 Dec;79(4):1251–81.

100. 20 arrested in international operation targeting child sexual abuse material [Internet]. [cited 2025 Sept 30]. Available from: https://www.interpol.int/News-and-Events/News/2025/20-arrested-in-international-operation-targeting-child-sexual-abuse-material

101. 25 arrested in global hit against AI-generated child sexual abuse material [Internet]. Europol. [cited 2025 Sept 30]. Available from: https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

102. UNICEF. Who Perpetrates Online Child Sexual Exploitation and Abuse? [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf

103. Child sexual abuse material (CSAM) [Internet]. Thorn. [cited 2025 Sept 30]. Available from: https://www.thorn.org/research/child-sexual-abuse-material-csam/

104. Salter M, Wong T. Parental Production of Child Sexual Abuse Material: A Critical Review. Trauma Violence Abuse. 2024 July;25(3):1826–37.

105. Finkelhor D, Turner H, Colburn D. The prevalence of child sexual abuse with online sexual abuse added. Child Abuse Negl. 2024;149.

106. Finkelhor D, Shattuck A, Turner HA, Hamby SL. The lifetime prevalence of child sexual abuse and sexual assault assessed in late adolescence. J Adolesc Health. 2014;55(3):329-333.

107. Russell DH, Trew S, Smith R, Higgins DJ, Walsh K. Primary prevention of harmful sexual behaviors by children and young people: A systematic review and narrative synthesis. Aggress Violent Behav. 2025 Apr;81:N.PAG-N.PAG.

108. Safe Futures Hub. Children Displaying Harmful Sexual Behaviour: Evidence and Responses [Internet]. 2025 [cited 2025 Nov 4]. Available from: https://cdn.safefutureshub.org/files/Children-displaying-harmful-sexual-behaviour-Evidence-and-responses.pdf

109. Tunagur MT, Oksal H, Büber Ö, Kurt Tunagur EM, Sarıgedik E. Risk Factors and Predictors of Penetrative Online Child Sexual Abuse. J Pediatr Health Care. 2025;39(2):198–205.

110. Leaked: Understanding and Addressing Self-Generated Sexual Content involving Young People in Thailand [Internet]. Evident. [cited 2025 Sept 6]. Available from: https://www.itsevident.org/major-projects

111. Disrupting Harm country reports | Innocenti Global Office of Research and Foresight [Internet]. 2022 [cited 2025 Sept 6]. Available from: https://www.unicef.org/innocenti/reports/disrupting-harm-country-reports

112. Trends and insights from a unique helpline preventing child sexual abuse [Internet]. Lucy Faithfull Foundation. [cited 2025 Sept 5]. Available from: https://www.lucyfaithfull.org.uk/research/trends-and-insights-from-a-unique-helpline-preventing-child-sexual-abuse/

113. Bailey A, Allen L, Stevens E, Dervley R, Findlater D, Wefers S. Pathways and Prevention for Indecent Images of Children Offending: A Qualitative Study. Sex Offending Theory Res Prev [Internet]. 2022 Dec 2 [cited 2025 Sept 5];17:1–24. Available from: https://sotrap.psychopen.eu/index.php/sotrap/article/view/6657

114. Protect Children. Our Voice Male Survivors: Experiences of Victims and Survivors of Child Sexual Abuse and Exploitation [Internet]. 2025. Available from: https://www.suojellaanlapsia.fi/en/post/our-voice-male-survivors

115. Tech Coalition | Assessing OCSEA Harms in Product Development [Internet]. Tech Coalition. [cited 2025 May 1]. Available from: https://www.technologycoalition.org/knowledge-hub/assessing-ocsea-harms-in-product-development

116. Detecting, Disrupting and Investigating Online Child Sexual Exploitation [Internet]. [cited 2025 Aug 30]. Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html

117. Internet Watch Foundation. Teenage boys targeted as hotline sees 'heartbreaking' increase in child 'sextortion' reports [Internet]. 2024 [cited 2025 Nov 10]. Available from: https://www.iwf.org.uk/news-media/news/teenage-boys-targeted-as-hotline-sees-heartbreaking-increase-in-child-sextortion-reports/

118. Self-Generated Child Sexual Abuse Fieldwork Findings Report by PIER [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/about-us/our-campaigns/self-generated-child-sexual-abuse-fieldwork-findings-report/

119. MikeHarrison. Link-sharing and child sexual abuse: understanding the threat - WeProtect Global Alliance [Internet]. 2023 [cited 2025 May 1]. Available from: https://www.weprotect.org/resources/library/link-sharing-and-child-sexual-abuse-understanding-the-threat/

120. Iyer C, Mehra S. Not a Child's Play: Taking Stock of Children's Gaming in India, Gaps, Emerging Risks and Responses [Internet]. Space2Grow; 2025 June. Available from: https://www.space2grow.in/_files/ugd/fcdbc5_0dead6ef6615455280abdbded0c2c605.pdf

121. Situation Analysis of Child Online Protection in Pakistan | UNICEF Pakistan [Internet]. [cited 2025 May 1]. Available from: https://www.unicef.org/pakistan/documents/situation-analysis-child-online-protection-pakistan

122. Online sexual abuse of primary children 1000% worse since lockdown [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/sexual-abuse-imagery-of-primary-school-children-1-000-per-cent-worse-since-lockdown/

123. CDC. A Public Health Approach to Community Violence Prevention [Internet]. Community Violence Prevention. 2025 [cited 2025 Sept 22]. Available from: https://www.cdc.gov/community-violence/php/public-health-strategy/index.html

124. Emery CR, Wong PWC, Haden-Pawlowski V, Pui C, Wong G, Kwok S, et al. Neglect, online invasive exploitation, and childhood sexual abuse in Hong Kong: Breaking the links. Child Abuse Negl. 2024 Jan;147:N. PAG-N.PAG.

125. Scalability | Prevention Global [Internet]. [cited 2025 Sept 22]. Available from: https://www.prevention.global/scalability

126. 2024: A Year of Urgency, Vision, and Partnership in Safeguarding Children Online – Safe Online [Internet]. [cited 2025 Sept 22]. Available from: https://safeonline.global/2024-a-year-of-urgency-vision-and-partnership-in-safeguarding-children-online/

127. Safe Online. Financing a Safe Digital Future: Safer Internet Day 2025 – Safe Online [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/financing-a-safe-digital-future-safer-internet-day-2025/

128. Ending Online Child Sexual Exploitation and Abuse | UNICEF [Internet]. [cited 2025 May 1]. Available from: https://www.unicef.org/documents/ending-online-child-sexual-exploitation-and-abuse

129. Kardefelt-Winther D, Maternowska C. Addressing violence against children online and offline. Nat Hum Behav. 2020;4:227–30.

130. Data for Change – Safe Online [Internet]. [cited 2025 Sept 27]. Available from: https://safeonline.global/data-for-change/

131. UNICEF. Data brief on Measuring Technology-facilitated Violence against Children in line with the International Classification of Violence against Children (ICVAC) [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://data.unicef.org/resources/data-brief-on-measuring-technology-facilitated-violence-against-children-in-line-with-the-international-classification-of-violence-against-children-icvac/

132. Safe Future Hub [Internet]. Available from: https://www.safefutureshub.org

133. Sexual Violence Research Initiative. SVRI Building the Field [Internet]. Available from: https://www.svri.org

134. Together for Girls [Internet]. Available from: https://www.togetherforgirls.org/

135. WeProtect Global Alliance. A global commitment to every child [Internet]. Available from: https://www.weprotect.org

136. General comment No. 24 (2019) on children's rights in the child justice system | OHCHR [Internet]. [cited 2025 Sept 22]. Available from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-24-2019-childrens-rights-child

137. Reason J. The contribution of latent human failures to the breakdown of complex systems. Philos Trans R Soc Lond B Biol Sci [Internet]. 1997 Jan [cited 2025 Sept 27];327(1241):475–84. Available from: https://royalsocietypublishing.org/doi/10.1098/rstb.1990.0090

138. Data from the Philippines Survivor Network consultations with survivors.

139. Lundy L. 'Voice' is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child. Br Educ Res J. 2007;33(6):927–42.

140. O'Kane C. Active and Safe: The Global Program Guide for Meaningful Participation of Children and Young People in Advocacy and Prevention and Protection from Online Violence [Internet]. kindernothilfe; 2025 [cited 2025 Nov 6]. Available from: https://fliphtml5.com/dcrxp/efpp/Active_%26amp%3B_Safe_GUIDE/

141. O'Kane C. Active and Safe: Accompanying Toolkit for Meaningful Participation of Children and Young People in Advocacy and Prevention and Protection from Online Violence [Internet]. kindernothilfe; 2025 [cited 2025 Nov 6]. Available from: https://fliphtml5.com/dcrxp/kqad/Active_%26_Safe_TOOLKIT_web_19Aug2025/

142. UNICEF. Spotlight guidance on best practices for stakeholder engagement with children in D-CRIAs [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://www.unicef.org/childrightsandbusiness/reports/D-CRIA-Spotlight-guidance-stakeholder-engagement

143. Diagram adapted from Lansdown G, Haj-Ahmead J, Rusinow T, Sukura Y Friscia. Conceptual Framework for Measuring Outcomes of Adolescent Participation [Internet]. 2018 [cited 2025 Nov 4]. Available from: https://www.unicef.org/media/59006/file

144. WeProtect Global Alliance. Visualising child and survivor participation [Internet]. Available from: https://www.weprotect.org/response/child-survivor-participation/mapping-participation-initiatives/#dataviz

145. European Union. BeSmartOnline - Maltese Safer Internet Centre [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://better-internet-for-kids.europa.eu/en/saferinternetday/malta

146. Be Smart Online. A Safer Internet for Malta [Internet]. [cited 2025 Oct 29]. Available from: https://www.besmartonline.info

147. VoiceBox. VoiceBox | By young people, for young people [Internet]. [cited 2025 Nov 4]. Available from: https://voicebox.site/

148. How can service providers work with boys at-risk and survivors of sexual exploitation and abuse in a gender-sensitive way? [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/story/global-boys-initiative-case-studies/

149. SecretsWorthSharing. Secrets Worth Sharing | How to talk about childhood sexual abuse [Internet]. SecretsWorthSharing. [cited 2025 Nov 4]. Available from: https://www.secretsworthsharing.com

150. CPC Learning Network. Secrets Worth Sharing founder testimony.

151. Global Threat Assessment 2023 Data - WeProtect Global Alliance [Internet]. 2023 [cited 2025 May 1]. Available from: https://www.weprotect.org/global-threat-assessment-23/data/

152. Resources | ThinkUKnow [Internet]. [cited 2025 Sept 22]. Available from: https://www.thinkuknow.org.au/resources-tab

153. World Vision. Tackling Online Child Sexual Exploitation [Internet]. [cited 2025 Oct 29]. Available from: https://wvi.org.vn/special-projects/tackling-online-child-sexual-exploitation-ene29.html

154. End Violence. More progress and impact from our grantees [Internet]. End Violence. [cited 2025 Nov 4]. Available from: https://www.end-violence.org/node/7971

155. UNICEF. Parenting for the Digital Age | UNICEF [Internet]. [cited 2025 Nov 4]. Available from: www.unicef.org/documents/parenting-digital-age

156. National Crime Agency. National Crime Agency launches online campaign to tackle "sextortion" among young teenage boys [Internet]. Available from: https://www.nationalcrimeagency.gov.uk/news/national-crime-agency-launches-online-campaign-to-tackle-sextortion-among-young-teenage-boys

157. Think Before You Share Campaign from IWF [Internet]. [cited 2025 Sept 17]. Available from: https://www.iwf.org.uk/about-us/our-campaigns/think-before-you-share/

158. UNODC. Beware The Share [Internet]. [cited 2025 Nov 4]. Available from: www.unodc.org/roseap/uploads/documents/beware-the-share/index.html

159. Safe Online. Grantee Highlight – Safe Online [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/grantee-highlight/

160. Letourneau EJ, Schaeffer CM, Bradshaw CP, Ruzicka AE, Assini-Meytin LC, Nair R, et al. Responsible Behavior With Younger Children: Results From a Pilot Randomized Evaluation of a School-Based Child Sexual Abuse Perpetration Prevention Program. Child Maltreat [Internet]. 2024 Feb 1 [cited 2025 Sept 6];29(1):129–41. Available from: https://doi.org/10.1177/10775595221130737

161. Ruzicka AE, Assini-Meytin LC, Schaeffer CM, Bradshaw CP, Letourneau EJ. Responsible Behavior with Younger Children: Examining the Feasibility of a Classroom-Based Program to Prevent Child Sexual Abuse Perpetration by Adolescents. J Child Sex Abuse [Internet]. [cited 2025 Nov 7];30(4). Available from: https://www.prevention.global/resources/responsible-behavior-younger-children-examining-feasibility-classroom-based-program

162. Forum EEC. Cultural Adaptation and Evaluation of the RBYC Program in Germany: Towards Offender-Focused and School-Based Prevention of Child Sexual Abuse [Internet]. Preventing disease and ill health. 2025 [cited 2025 Sept 6]. Available from: https://euspr.hypotheses.org/2100

163. Schatz J, Deesawade R, Mosby W, Kavenagh M. Leaked: Understanding and Addressing Self-Generated Sexual Content Involving Young People in Thailand [Internet]. Evident & HUG Project: Bangkok; 2025 [cited 2025 Nov 4]. Available from: www.itsevident.org/_files/ugd/0bd10b_86d0e7f3921645f7bebc0fa399371860.pdf

164. Dodge A, Lockhart E. "Young People Just Resolve It in Their Own Group": Young People's Perspectives on Responses to Non-Consensual Intimate Image Distribution. Youth Justice J Natl Assoc Youth Justice. 2022 Dec;22(3):304–19.

165. Our story [Internet]. World Childhood Foundation - 25 Years. [cited 2025 Sept 27]. Available from: https://childhood.org/about-childhood/our-story/

166. The HUG Project - Protecting Thai children from sexual abuse and online sex trafficking [Internet]. The HUG Project. [cited 2025 Sept 22]. Available from: https://www.hugproject.org/

167. Evident | Translating evidence into action for social change [Internet]. Evident. [cited 2025 Sept 22]. Available from: https://www.itsevident.org

168. Deterring online child sexual abuse and exploitation: lessons from seven years of campaigning) - Lucy Faithfull Foundation [Internet]. [cited 2025 Sept 27]. Available from: https://www.lucyfaithfull.org.uk/research/deterring-online-child-sexual-abuse-and-exploitation-lessons-from-seven-years-of-campaigning/

169. ReDirection | Protect Children [Internet]. [cited 2025 Sept 22]. Available from: https://www.suojellaanlapsia.fi/en/redirection

170. Help Wanted. Help Wanted Prevention Intervention [Internet]. Help Wanted. [cited 2025 Nov 4]. Available from: https://staging.wp.helpwantedprevention.org/

171. Chatbots and Warning Messages - Innovations in the Fight Against Online Child Sexual Abuse [Internet]. Lucy Faithfull Foundation. [cited 2025 Sept 27]. Available from: https://www.lucyfaithfull.org.uk/research/chatbots-and-warning-messages-innovations-in-the-fight-against-online-child-sexual-abuse/

172. Rati. Meri Trustline [Internet]. Rati Foundation. [cited 2025 Nov 4]. Available from: https://ratifoundation.org/meri-trustline/

173. Internet Watch Foundation. IWF 2024: Meri Trustline – Supporting Children Facing Online Harms [Internet]. [cited 2025 Nov 4]. Available from: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/meri-trustline/

174. UNICEF. Multidisciplinary Models of Care for Child Victims and Survivors of Sexual Abuse and Exploitation in the Digital Age | UNICEF [Internet]. [cited 2025 Nov 4]. Available from: https://www.unicef.org/documents/multidisciplinary-models-care-child-victims-and-survivors-sexual-abuse-and-exploitation

175. Prevention Global. Serving Youth Animation, Brieg, Infographic [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://www.prevention.global/insight/serving-youth-animation-brief-infographic

176. Prevention Global. Serving Youth [Internet]. [cited 2025 Oct 29]. Available from: https://www.prevention.global/serving-youth

177. MyVoiceMySafety-global-poll-of-children.pdf [Internet]. [cited 2025 Sept 22]. Available from: https://www.weprotect.org/wp-content/uploads/MyVoiceMySafety-global-poll-of-children.pdf

178. ECPAT. Guidelines for ethical research on sexual exploitation involving children [Internet]. 2019 [cited 2025 Oct 29]. Available from: https://ecpat.org/guidelines-for-ethical-research/

179. Disrupting Harm: Conversations with Young Survivors about Online Child Sexual Exploitation and Abuse [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/resource/disrupting-harm-conversations-with-young-survivors-about-online-child-sexual-exploitation-and-abuse/

180. Luciana C. Assini-Meytin, McPhail I, Sun Y, Matthews B, Kaufman KL, Letourneau E. Child Sexual Abuse and Boundary Violating Behaviors in Youth Serving Organizations: National Prevalence and Distribution by Organizational Type. Child Maltreat [Internet]. 2024 [cited 2025 Oct 29];20(3):499–511. Available from: https://journals.sagepub.com/doi/10.1177/10775595241290765

181. Alliance WG. Health and wellbeing of frontline responders. 2025 [cited 2025 Sept 27]; Available from: https://www.weprotect.org/wp-content/uploads/Health-and-wellbeing-of-frontline-responders_May-2025.pdf

182. Towards digital safety by design for children | OECD [Internet]. [cited 2025 Sept 22]. Available from: https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html

183. Tech Coalition | Child Safety Best Practices [Internet]. Tech Coalition. [cited 2025 May 1]. Available from: https://www.technologycoalition.org/knowledge-hub/child-safety-best-practices

184. Child Rights Impact Assessment: A Policy Tool for a Rights Respecting Digital Environment - Livingstone - 2025 - Policy & Internet - Wiley Online Library [Internet]. [cited 2025 Sept 22]. Available from: https://onlinelibrary.wiley.com/doi/10.1002/poi3.70008

185. UNICEF. Assessing child rights impacts in relation to the digital environment | UNICEF Child Rights and Business [Internet]. [cited 2025 Nov 4]. Available from: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA

186. Digital Futures Commission. Child Rights by Design - 5Rights Foundation & Digital Futures Commission [Internet]. Child Rights By Design | Digital Futures Commission. [cited 2025 Nov 4]. Available from: https://childrightsbydesign.5rightsfoundation.com/

187. Thorn & ATIH. Safety by Design for Generative AI: Preventing Child Sexual Abuse. 2024. Thorn Repository. Available at https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf.

188. Thorn. Safety by Design for responsible AI | Safer by Thorn [Internet]. Purpose-Built Trust and Safety Solutions | Safer by Thorn. 2025 [cited 2025 Nov 4]. Available from: https://safer.io/resources/safety-by-design-a-responsible-ai-framework/

189. Australian Government. Be Secure Quiz | eSafety Commissioner [Internet]. [cited 2025 Nov 4]. Available from: https://www.esafety.gov.au/educators/classroom-resources/be-secure/quiz

190. Human Mobile Devices. HMD Fuse | The phone that grows with your kids [Internet]. HMD - Human Mobile Devices. [cited 2025 Nov 4]. Available from: https://www.hmd.com/en_int/hmd-fuse

191. Apple Support. About Communication Safety on your child's Apple device [Internet]. Apple Support. [cited 2025 Nov 4]. Available from: https://support.apple.com/en-us/105069

192. Snapchat. Parents - Safeguards For Teens [Internet]. [cited 2025 Nov 4]. Available from: https://parents.snapchat.com/safeguards-for-teens

193. Google. Be Internet Awesome [Internet]. Be Internet Awesome. [cited 2025 Nov 4]. Available from: https://beinternetawesome.withgoogle.com/en-us

194. Lego. LEGO® - Code of conduct [Internet]. [cited 2025 Nov 4]. Available from: https://kids.lego.com/en-us/legal/kids-code-of-conduct

195. Instagram. Partner With Instagram to Keep Your Students Safe | About Instagram [Internet]. [cited 2025 Nov 4]. Available from: https://about.instagram.com/community/educators

196. Ngo VM, Gajula R, Thorpe C, Mckeever S. Discovering child sexual abuse material creators' behaviors and preferences on the dark web. Child Abuse Negl. 2024 Jan;147:106558.

197. Haluska R, Badovska M, Pleva M. Concept of Speaker Age Estimation Using Neural Networks to Reduce Child Grooming. Elektron Ir Elektrotechnika. 2024 Aug 26;30(4):61–7.

198. Thorn. Generative AI: Now is the Time for Safety By Design [Internet]. Thorn. 2023 [cited 2025 Nov 4]. Available from: https://www.thorn.org/blog/now-is-the-time-for-safety-by-design/

199. Tech Coalition. Insights to Action: Asia-Pacific Briefing on Combating OCSEA [Internet]. https://technologycoalition.org/. [cited 2025 Nov 4]. Available from: https://technologycoalition.org/news/insights-to-action-tech-coalition-asia-pacific-briefing-on-combating-ocsea/

200. National Center for Missing & Exploited Children. Take It Down [Internet]. Take It Down. [cited 2025 Nov 3]. Available from: https://takeitdown.ncmec.org/

201. Lantern 2024 Transparency Report [Internet]. https://technologycoalition.org/. [cited 2025 Aug 31]. Available from: https://technologycoalition.org/resources/lantern-2024-transparency-report/

202. U.K. Government. Online Safety Act: explainer [Internet]. GOV.UK. [cited 2025 Nov 4]. Available from: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

203. Fiji approves 1st national child safeguarding policy [Internet]. [cited 2025 Sept 22]. Available from: https://english.news.cn/asiapacific/20250822/3042a592ecb344bb8eaa4bd2bf0ebebf/c.html

204. G7 #BeBrave Scorecard Report 2025 [Internet]. Brave Movement. [cited 2025 Sept 27]. Available from: https://www.bravemovement.org/resources/g7-scorecard-2025

205. Global Online Safety Regulators Network. GOSRN Regulatory Index 2024 [Internet]. [cited 2025 Nov 3]. Available from: https://www.esafety.gov.au/sites/default/files/2024-10/GOSRN-Regulatory-Index-2024-final.pdf

206. Tracking the shifts: Age assurance in motion | IAPP [Internet]. [cited 2025 Sept 27]. Available from: https://iapp.org/news/a/tracking-the-shifts-age-assurance-in-motion

207. Taylor J. Not just under-16s: all Australian social media users will need to prove their age – and it could be complicated and time consuming. The Guardian [Internet]. 2025 Sept 1 [cited 2025 Sept 28]; Available from: https://www.theguardian.com/technology/2025/sep/02/under-16s-ban-how-hard-will-it-be-for-australian-social-media-users-to-prove-their-age

208. Department of Infrastructure T. Age assurance consumer research findings [Internet]. Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts; 2025 [cited 2025 Sept 27]. Available from: https://www.infrastructure.gov.au/department/media/publications/age-assurance-consumer-research-findings

209. Faverio MA and M. 81% of U.S. adults – versus 46% of teens – favor parental consent for minors to use social media [Internet]. Pew Research Center. 2023 [cited 2025 Sept 27]. Available from: https://www.pewresearch.org/short-reads/2023/10/31/81-of-us-adults-versus-46-of-teens-favor-parental-consent-for-minors-to-use-social-media/

210. International A. Social media ban: what is it and what will it mean for young people? [Internet]. Amnesty International Australia. 2024 [cited 2025 Sept 27]. Available from: https://www.amnesty.org.au/social-media-ban-explained/

211. VPNs top App Store charts as UK age verification kicks in [Internet]. 2025 [cited 2025 Sept 27]. Available from: https://www.bbc.com/news/articles/cn72ydj70g5o

212. African Union. African Union Child Online Safety and Empowerment Policy | African Union [Internet]. 2024 [cited 2025 Nov 3]. Available from: https://au.int/en/documents/20240521/african-union-child-online-safety-and-empowerment-policy

213. Commonwealth of Australia. Age Assurance Technology Trial [Internet]. Age Assurance Technology Trial. [cited 2025 Nov 3]. Available from: https://ageassurance.com.au/report/

214. Eltaher F, Gajula R, Miralles-Pechuán L, Thorpe C, McKeever S. The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media. Conf Pap [Internet]. 2025 Jan 1; Available from: https://arrow.tudublin.ie/scschcomcon/442

215. Evershed N, Nicholas J. Social media ban trial data reveals racial bias in age checking software: just how inaccurate is it? The Guardian [Internet]. 2025 Sept 18 [cited 2025 Sept 23]; Available from: https://www.theguardian.com/news/2025/sep/19/how-accurate-are-age-checks-for-australias-under-16s-social-media-ban-what-trial-data-reveals

216. School SL. The "Segregate-and-Suppress" Approach to Regulating Child Safety Online [Internet]. Stanford Law School. 2025 [cited 2025 Sept 28]. Available from: https://law.stanford.edu/publications/the-segregate-and-suppress-approach-to-regulating-child-safety-online/

217. Safe Online. Kenya launches groundbreaking training handbook to combat online child sexual exploitation and abuse [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/kenya-launches-groundbreaking-training-handbook-to-combat-online-child-sexual-exploitation-and-abuse/

218. Thorn. For Victim Identification [Internet]. Thorn. [cited 2025 Nov 3]. Available from: https://www.thorn.org/solutions/victim-identification/

219. Rigr AI. Video Summarisation Tool by Rigr AI [Internet]. Video Summarisation Tool by Rigr AI. [cited 2025 Nov 3]. Available from: https://www.vst.rigr.ai

220. Safe Online Report 2024 – Safe Online [Internet]. [cited 2025 Sept 22]. Available from: https://safeonline.global/safe-online-report-2024/

221. Canadian Framework For Trauma-Informed Response in Policing – Introduction | Barrie Police Service [Internet]. [cited 2025 Sept 27]. Available from: https://www.barriepolice.ca/cftirp-introduction/

222. Landry G. Mobilising the Financial Sector Against the Sexual Exploitation of Children. ECPAT;

223. AFP records spike in financial sextortion reports over the school holidays | Australian Federal Police [Internet]. 2023 [cited 2025 Sept 22]. Available from: https://www.afp.gov.au/news-centre/media-release/afp-records-spike-financial-sextortion-reports-over-school-holidays

224. It's Never Too Early - Early education Project Paradigm collaboration | ACCCE [Internet]. [cited 2025 Sept 22]. Available from: https://www.accce.gov.au/resources/parents-carers/its-never-too-early-early-education-project-paradigm-collaboration

225. Sextortion Campaign [Internet]. Available from: https://www.accce.gov.au/sites/default/files/2022-11/sextortion%20campaign%20video.mp4

226. Prevention Global. Making The Case | Prevention Global [Internet]. [cited 2025 Nov 3]. Available from: https://prevention.global/making-the-case

227. U.S. Government Accountability Office. Science & Tech Spotlight: Deepfakes [Internet]. 2025 [cited 2025 Nov 3]. Available from: https://www.gao.gov/assets/gao-20-379sp.pdf

228. JISC. Digital wellbeing [Internet]. Digital wellbeing. [cited 2025 Nov 3]. Available from: https://digitalcapability.jisc.ac.uk/what-is-digital-capability/digital-wellbeing/

229. Knodel M, Baker F, Kolkman O, Celi S, Grover G. Definition of End-to-end Encryption [Internet]. Internet Engineering Task Force; [cited 2025 Nov 3]. Report No.: draft-knodel-e2ee-definition-04. Available from: https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition-04

230. INHOPE. What is generative AI? [Internet]. 2024 [cited 2025 Nov 3]. Available from: https://inhope.org/EN/articles/what-is-generative-ai

231. Overview of Perceptual Hashing Technology [Internet]. www.ofcom.org.uk. 2022 [cited 2025 Nov 3]. Available from: https://www.ofcom.org.uk/online-safety/safety-technology/overview-of-perceptual-hashing-technology

232. Know2Protect, US Department of Homeland Security. ONLINE ENTICEMENT INFORMATIONAL BULLETIN [Internet]. Available from: https://www.dhs.gov/sites/default/files/2025-01/25_0121_K2P_online-enticement.pdf

233. 'Self-generated' sexual material - WeProtect Global Alliance [Internet]. 2022 [cited 2025 May 1]. Available from: https://www.weprotect.org/issue/self-generated-sexual-material/

weprotect
Global Alliance

CPC
LEARNING
NETWORK

COLUMBIA | MAILMAN SCHOOL OF PUBLIC HEALTH