HERRAMIENTAS PARA LA SEGURIDAD DE NIÑAS, NIÑOS Y ADOLESCENTES EN INTERNET

GARANTIZAR LA SEGURIDAD DE NIÑAS, NIÑOS Y ADOLESCENTES EN INTERNET

5RIGHTS FOUNDATION

End Violence Against Children

Acerca de 5Rights Foundation

Creemos el mundo digital que se merecen los jóvenes

5Rights desarrolla nuevas políticas, crea marcos de trabajo innovadores, desarrolla estándares técnicos, publica investigaciones, desafía las narrativas comunes y garantiza que los derechos y las necesidades de niñas, niños y adolescentes se reconozcan y traten con prioridad en el mundo digital.

Nos centramos en cambios implementables y nuestro trabajo se cita y utiliza por todo el mundo. Trabajamos con gobiernos, instituciones intergubernamentales, asociaciones profesionales, académicos, empresas, ONG y niñas, niños y adolescentes para que los productos y servicios digitales puedan influir positivamente en las experiencias vividas por los jóvenes. Un niño o joven es cualquier persona menor de 18 años, según se define en la Convención sobre los Derechos del Niño de la ONU.

Esta publicación se ha elaborado con el apoyo financiero del Fondo para poner fin a la violencia a través de la iniciativa Safe Online. El Fondo para poner fin a la violencia proporciona apoyo financiero a programas que ofrecen soluciones prácticas e innovadoras para proteger a los niños de la explotación y el abuso en línea. Las opiniones, hallazgos, conclusiones y recomendaciones que se expresan en este material pertenecen a 5Rights Foundation y no reflejan necesariamente los puntos de vista del Fondo para poner fin a la violencia.

5RIGHTS FOUNDATION

End Violence Against Children

Índice de contenidos

= Dirígete aquí para consultar información clave

PRÓLOGO

«En estos momentos sin precedentes, no podemos subestimar el poder, la promesa y el peligro de la tecnología digital. Unir fuerzas permitirá a la comunidad internacional garantizar que la tecnología se utilice para el bien, buscar oportunidades para gestionar su impacto y garantizar que ofrezca igualdad de condiciones para todos.

Las generaciones futuras se encargarán de juzgar si la generación actual aprovechó las oportunidades que ofrece la era de la interdependencia digital. Ahora es momento de actuar».

António Guterres
Secretario general de las Naciones Unidas
Hoja de ruta del secretario general para la cooperación digital, junio de 2020

PRÓLOGO

«No podemos crear un futuro sostenible a menos que seamos capaces de garantizar que los niños puedan crecer de forma segura y protegidos de la violencia y el daño, incluso en los entornos digitales. A pesar de que todos tenemos una visión de cómo debería ser un mundo digital seguro y propicio para los niños, la situación se complica al empezar a traducir dicha visión en políticas, normativas, acciones, y productos y servicios concretos.

Nuestra esperanza es que estas Herramientas para la seguridad de niñas, niños y adolescentes en Internet sean una solución a este problema: una guía práctica para los responsables de formular las políticas que "simplifique" las cuestiones clave que debemos abordar para hacer de Internet un lugar seguro para los niños».

Dr. Howard Taylor
Director ejecutivo
Fondo para poner fin a la violencia

CARPETA DEL SISTEMA

8 ELEMENTOS | 105 MB EN EL DISCO | SECCIÓN 1

SIGUIENTE SECCIÓN >

Introducción

En un mundo cada vez más conectado, la necesidad de un entorno digital seguro y propicio para los niños nunca había sido mayor. Los responsables de formular las políticas de todo el mundo están trabajando para definir las normas que rijan la interacción de los niños con el mundo digital. En la hoja de ruta del secretario general de la ONU para la cooperación digital queda patente de forma clara esta necesidad.[1] Este kit de herramientas está diseñado para apoyar a los responsables de formular y ejecutar las políticas con el objetivo de ofrecer un enfoque accesible y práctico para crear un mundo digital que apoye a los niños y les permita prosperar en línea y más allá.

Este kit de herramientas describe la hoja de ruta necesaria para garantizar que el mundo digital sea un lugar seguro para los niños donde se respeten sus derechos. Divide sus obligaciones en diez áreas temáticas para apoyar la implementación de los siguientes acuerdos y marcos de trabajo internacionales clave: los Objetivos de Desarrollo Sostenible (ODS); la Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital; el Modelo de Respuesta Nacional de la Alianza Mundial de WeProtect; y las Directrices sobre la protección de la infancia en línea de la Unión Internacional de Telecomunicaciones.

El objetivo de este kit de herramientas no es reemplazar ningún acuerdo o marco de trabajo regional, nacional o internacional, sino proporcionar ejemplos de prácticas recomendadas de todo el mundo, identificar enfoques detallados en todos los ámbitos de aplicación y establecer las medidas que deben tomar las personas y equipos encargados de proteger la seguridad de los niños en línea. Como tal, es una herramienta para que los responsables de formular las políticas de todo el mundo adopten las obligaciones que ya tienen.

Garantizar la seguridad en línea no consiste únicamente en responder a los riesgos y daños, implica diseñar activamente un entorno digital que sea seguro para todos los niños. Una de cada tres personas que navegan por Internet son menores de 18 años. La tecnología digital forma parte central de la vida de los niños, por lo que el entorno digital debe diseñarse por defecto con su privacidad, su seguridad y sus derechos en mente. Este enfoque preventivo e integral se refleja en el kit de herramientas, que ofrece una hoja de ruta para que los gobiernos, las naciones estado y las organizaciones creen, revisen o mejoren sus políticas y prácticas en lo relevante a los derechos del niño. Esto permitirá que todos los actores de la cadena de responsabilidades cumplan con su parte en la labor encaminada a garantizar la protección de los niños en línea, que irá desarrollándose a lo largo del tiempo. El kit de herramientas está diseñado para los responsables de formular las políticas de todo el mundo, incluidos los de los países con un acceso a Internet más reciente, y para ser accesible y transferible a distintos contextos y entornos.

En nombre de 5Rights y de nuestra comunidad, me gustaría darle las gracias al secretario general *António Guterres* por su liderazgo visionario al proporcionar una hoja de ruta para un mundo conectado y por reconocer que si el mundo conectado no es seguro ni respeta los derechos de los niños, no cumplirá con su promesa de ofrecer un mundo mejor para todos. También quiero dejar constancia de que el trabajo inicial en el que se basa este kit de herramientas se llevó a cabo en nombre del Gobierno de Ruanda, y agradecemos su apoyo al permitirnos utilizarlo aquí. También queremos dar las gracias a la catedrática Julia Davidson OBE y a la Dra. Susie Alegre por sus contribuciones a este documento. Asimismo, queremos reconocer el generoso apoyo del Fondo para poner fin a la violencia, que nos permitió elaborar la Política de protección infantil en línea para el Gobierno de Ruanda, y que posteriormente vio la posibilidad de convertirla en algo de lo que todo los países pudieran beneficiarse.

Este kit de herramientas no habría sido posible sin el trabajo de muchas otras personas y organismos, entre los que se encuentran el Comité de los Derechos del Niño de la ONU, la Alianza Mundial WeProtect, el Fondo para poner fin a la violencia, la Universidad del Este de Londres, la Universidad de Ruanda, 5Rights Foundation y muchos estados, organizaciones intergubernamentales globales y comunidades académicas, de protección infantil y de aplicación de la ley. Reconocemos su labor y les damos las gracias por su trabajo, compromiso y contribuciones. Ante todo, este kit de herramientas ha sido posible gracias a los cientos de niños y jóvenes que nos han dicho que quieren formar parte del mundo digital de forma creativa, segura y sin miedo. Este kit de herramientas es para ellos.

Baronesa Beeban Kidron OBE
Fundadora y presidenta de 5Rights Foundation

1. Hoja de ruta del secretario general de las Naciones Unidas para la cooperación digital, Naciones Unidas, 2020.

SIGUIENTE SECCIÓN >

CARPETA DEL SISTEMA

8 ELEMENTOS | 105 MB EN EL DISCO | SECCIÓN 2

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

Cómo utilizarlas

Las Herramientas para la seguridad de niñas, niños y adolescentes en Internet ayudan a los responsables de formular las políticas a cumplir sus obligaciones internacionales en materia de derechos y seguridad de la infancia en Internet.

Para algunos, este documento será un punto de partida; para otros, será la oportunidad de comparar sus políticas e implementación con las prácticas recomendadas a nivel internacional. Está diseñado para poder utilizarse en cualquier país y que los responsables de formular las políticas puedan utilizarlo para evaluar y fundamentar su propio recorrido para integrar los derechos de la infancia y adolescencia en el entorno digital, junto con los análisis de su propio contexto nacional.

El kit de herramientas incluye:

- Un «modelo» sólido e integral de política pública en seguridad infantil en Internet como orientación para que los responsables de formular las políticas puedan implementar para garantizar una coordinación eficaz entre todas las jurisdicciones
- Diez áreas de acción de la política para que los responsables de formular las políticas las utilicen en el desarrollo de su propia política de seguridad infantil en Internet
- Listas de verificación y otras herramientas de auditoría que los responsables de formular las políticas pueden utilizar para evaluar y mejorar las medidas actuales y planificadas de su país en materia de seguridad infantil en Internet
- Resúmenes y directrices de los documentos básicos internacionales
- Glosario de términos clave empleados en las políticas de seguridad en línea, tanto para adultos como para niños
- Ejemplos de prácticas recomendadas e información de varios países
- Diagramas y otros materiales explicativos para ayudar a comunicar las ideas de las políticas a otras audiencias, incluidos los funcionarios públicos y la sociedad civil.

Responde al llamado del secretario general de las Naciones Unidas en su Hoja de ruta para la cooperación digital (2020) agrupando recursos básicos: la Observación general núm. 25 (2021) de la CDN de las Naciones Unidas; las Directrices sobre la protección de la infancia en línea de la Unión Internacional de Telecomunicaciones, y el Modelo de respuesta nacional de la Alianza Mundial WeProtect, para ofrecer un recurso práctico a los responsables de formular las políticas que les permite garantizar la seguridad de la infancia y la adolescencia en Internet.

El kit de herramientas y sus recursos están disponibles en línea en childonlinesafetytoolkit.org y enviando un correo electrónico a info@5rightsfoundation.com.

El lenguaje es importante. Las palabras que utilizamos influyen en la forma en que pensamos sobre los derechos de niñas, niños, adolescentes y su seguridad en línea. Las palabras que utilizamos influyen en la forma de dar prioridad a determinadas cuestiones, cómo respondemos y, lo que es más importante, nuestra capacidad para colaborar y hacer efectivos los derechos del niño a nivel internacional. A pesar de que los contextos nacionales sean en esencia diferentes, es fundamental que las leyes y su regulación utilicen en la medida de lo posible conceptos, términos y definiciones que estén en consonancia y que permitan la cooperación entre los organismos encargados de hacer cumplir la ley, así como la cooperación transfronteriza y una mayor comprensión general.[2] El kit de herramientas incluye glosarios reconocidos a nivel internacional del Comité de los Derechos del Niño de las Naciones Unidas y las Directrices de Luxemburgo, que ayudan a proporcionar una plantilla para el lenguaje empleado.[3]

El kit de herramientas complementa y destaca modelos bien desarrollados para apoyar aspectos específicos de la seguridad de la infancia y la adolescencia en Internet.

Estos son algunos de los recursos básicos:

- La Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital es una herramienta fundamental para entender los derechos de niñas, niños y adolescentes en el contexto de la seguridad en Internet. En ella, el Comité de los Derechos del Niño de las Naciones Unidades explica cómo deberían implementar los Estados la Convención sobre los Derechos del Niño en relación con el entorno digital y ofrece asesoramiento sobre las leyes, políticas y otras medidas pertinentes para garantizar el pleno cumplimiento de sus obligaciones en virtud de la Convención y los Protocolos Facultativos.[4]

- El *Modelo de respuesta nacional* (MNR, por sus siglas en inglés) de la Alianza Mundial WeProtect es de particular importancia en relación con la explotación y el abuso sexuales infantiles (EASI). El MNR es una parte clave de cualquier kit de herramientas nacional para la seguridad de la infancia y adolescencia en Internet.[5] El MNR se centra en ayudar a los países a desarrollar su respuesta a la explotación y el abuso sexuales infantiles en Internet, pero señala que no puede abordarse de forma aislada y establece que se necesita un conjunto más amplio de capacidades para prevenir y abordar la explotación y el abuso sexuales infantiles para garantizar una respuesta nacional completa. Este kit de herramientas proporciona recursos que apoyan la implementación del MNR. Las Herramientas para la seguridad de niñas, niños y adolescentes en Internet pueden ayudar a los signatarios del MNR de la Alianza Mundial WeProtect a garantizar que disponen de la capacidad institucional necesaria para cumplir sus objetivos y garantizar que se cumplan las obligaciones en virtud de la Observación general.

- Las *Directrices sobre la protección de la infancia en línea 2020 de la Unión Internacional de Telecomunicaciones* (UIT) son un compendio completo de recomendaciones y herramientas para todas las partes interesadas relevantes sobre cómo contribuir al desarrollo de un entorno en línea seguro y empoderador para niñas, niños y adolescentes. Están adaptadas a

2. «El Comité recomienda que los Estados parte tengan en cuenta los avances tecnológicos a la hora de establecer sus marcos de trabajo jurídicos, para garantizar que puedan seguir aplicándose en un futuro junto con los nuevos desarrollos y para evitar vacíos con cuestiones emergentes, incluidas nuevas formas de venta y explotación sexual en línea. Habida cuenta de la evolución de la cuestión, los Estados parte deben evaluar periódicamente y, cuando sea necesario, revisar la legislación y las políticas para garantizar que sus marcos de trabajo jurídicos se adapten a una realidad en constante cambio». Directrices relativas a la aplicación del Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, Comité de los Derechos del Niño de las Naciones Unidas, 2019.
3. Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, ECPAT International, 2016
4. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prevenir y abordar la explotación sexual de niñas, niños y adolescentes (ESIA): modelo de respuesta nacional), Alianza Mundial WeProtect, 2015.
5. Observación general núm. 25 relativa a los derechos del niño en relación con el entorno digital, CDN, 2021.

cuatro públicos clave: niños y niños, padres, madres, cuidadores y educadores, industria y finalmente responsables de formular las políticas. Para cada una de estas audiencias, las directrices pretenden ser un plan que puede adaptarse y utilizarse de forma coherente con las costumbres y leyes nacionales o locales, y abordar de esta forma cuestiones que pueden afectar a las personas menores de 18 años.[6]

Otros recursos y marcos de trabajo importantes y relevantes para los responsables de formular las políticas en materia de seguridad de los niños en Internet son:

- **Los *Objetivos de Desarrollo Sostenible* de las Naciones Unidas.** Los 17 Objetivos de Desarrollo Sostenible (ODS) son la base de la Agenda 2030 para el Desarrollo Sostenible,[7] adoptada por todos los Estados Miembros de las Naciones Unidas en 2015.

- **Los *Principios Rectores sobre las Empresas y los Derechos Humanos* de las Naciones Unidas.**[8] Estos principios establecen las obligaciones de los Estados partes y de las empresas de proteger y respetar los derechos humanos, incluidos los derechos del niño.

- **Organización Mundial de la Salud. *INSPIRE: Siete estrategias para poner fin a la violencia contra los niños y las niñas.***[9] INSPIRE es un paquete técnico con base empírica para apoyar a los países en sus esfuerzos para prevenir la violencia contra los niños y responder a ella.

- Borrador de **UNICEF de *Policy Guidance on AI for Children (Orientación normativa sobre IA para niños).***[10] La guía está diseñada para promover los derechos del niño en las políticas y prácticas de IA del gobierno y el sector privado, y para crear conciencia sobre cómo pueden defender o socavar estos derechos los sistemas de IA.

Hay muchos otros a nivel regional, nacional e internacional que pueden ser relevantes para contextos nacionales específicos o proporcionar modelos relevantes a nivel internacional, muchos de los cuales se citan en las secciones relevantes de este kit de herramientas.

> **Otra gran preocupación es la prevalencia de la explotación y el abuso sexuales de niñas, niños y adolescentes. En 2020, se denunciaron 65 millones de casos de material de explotación sexual de niñas, niños y adolescentes al Centro Nacional para Niños Desaparecidos y Explotados de los Estados Unidos, y hubo muchos más que pasaron inadvertidos.[11] Desde hace mucho tiempo, la comunidad internacional se mantiene unida en su empeño común de proteger a niñas, niños y adolescentes, lo que ha permitido que aumente la cooperación entre las fuerzas del orden y las principales empresas de tecnología, pero se puede ir aún más lejos.**
>
> **Las empresas deben adoptar medidas de inspección más rigurosas y acelerar los métodos de detección centrados en la prevención. Este enfoque se debe apoyar con medidas legislativas de peso. A este respecto, hay asociaciones de múltiples interesados que resultan sumamente útiles, como la Alianza Mundial WeProtect y la Alianza mundial para poner fin a la violencia contra los niños.**
>
> Fuente: hoja de ruta del secretario general de las Naciones Unidas para la cooperación digital, junio de 2020[12]

6. Directrices sobre la protección de la infancia en línea, Unión Internacional de Telecomunicaciones, 2020.
7. Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible, Naciones Unidas, 2021.
8. Principios Rectores sobre las Empresas y los Derechos Humanos, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2011.
9. INSPIRE: Siete estrategias para poner fin a la violencia contra los niños y las niñas, Organización Mundial de la Salud, 2021.
10. Policy guidance on AI for children (Orientación normativa sobre IA para niños), Fondo de las Naciones Unidas para la Infancia, 2020.
11. Informe de CyberTipline, Centro Nacional para Niños Desaparecidos y Explotados, 2020.
12. Hoja de ruta del secretario general de las Naciones Unidas para la cooperación digital, Naciones Unidas, junio de 2020.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

Cómo lo conseguimos

El mundo digital está en constante cambio. La política de seguridad infantil en Internet debe basarse en un enfoque centrado en los derechos del niño y debe ser lo suficientemente flexible para hacer frente a los riesgos y oportunidades en constante cambio a medida que surjan. El objetivo de las Herramientas para la seguridad de niñas, niños y adolescentes en Internet es satisfacer esta necesidad proporcionando un conjunto completo de medidas para una política que pueda adaptarse, ejemplos de prácticas recomendadas y recursos que se pueden compartir.

Este kit de herramientas es el resultado de consultas realizadas por todo el mundo, teniendo en cuenta datos de todos los continentes y ubicaciones, desde pequeños estados insulares en desarrollo hasta grandes naciones industriales.[13] Hemos hablado con expertos internacionales de distintos sectores, incluidos trabajadores industriales, responsables de la formulación de políticas y académicos. 5Rights, con sede el Reino Unido, se encargó de la redacción con la ayuda de colegas en Europa, América del Norte y Australia, y de socios [14] que permitieron la formación de grupos focales en América Latina, África y Asia, para garantizar que el kit de herramientas fuera práctico y relevante para una amplia gama de contextos locales. El texto se basa en estándares globales, en particular la Convención de las Naciones Unidas sobre los Derechos del Niño, pero el kit de herramientas también puede adaptarse para reflejar las culturas y los valores de las constituciones nacionales de todo el mundo.

Se trata de un kit de herramientas integral, práctico y accesible para que los responsables de la formulación de políticas sienten las bases de un mundo en el que los niños puedan sentirse seguros y realizados: un mundo que respete completamente sus derechos tanto dentro como fuera del entorno digital.

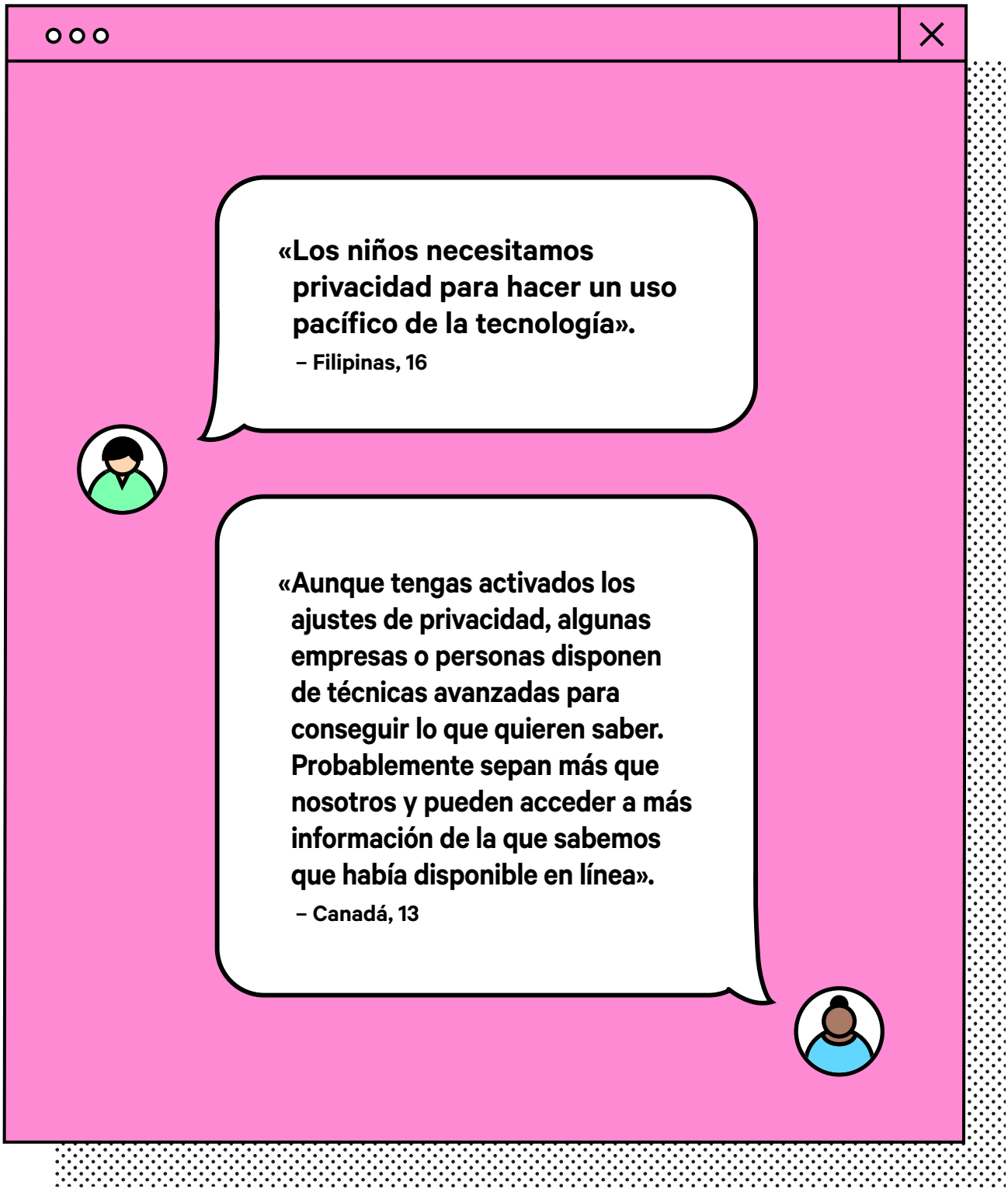
Durante las consultas, los niños comentaron que el entorno digital debería apoyar, promover y proteger su participación segura y equitativa:

«Nos gustaría que el gobierno, las empresas de tecnología y los maestros nos ayudaran a gestionar la información poco fiable en línea».
- Ghana, edad desconocida

«Me gustaría saber con certeza qué pasa con mis datos. ¿Por qué se recopilan? ¿Cómo lo hacen?».
- Alemania, 16

«Me preocupa que se compartan mis datos».
- Canadá, 15

13. Incluidas consultas de grupos focales en Brasil, Camboya, Colombia, Ghana, Sri Lanka y Zimbabue, para garantizar su relevancia a nivel internacional.
14. Entre los socios locales figuran RedPapaz en Colombia, Alana Foundation en Brazil, African Digital Rights Hub en Ghana, UNICEF en Zimbabue, UNICEF en Camboya y Save the Children International en Sri Lanka.


«Los niños necesitamos privacidad para hacer un uso pacífico de la tecnología».
– Filipinas, 16
«Aunque tengas activados los ajustes de privacidad, algunas empresas o personas disponen de técnicas avanzadas para conseguir lo que quieren saber. Probablemente sepan más que nosotros y pueden acceder a más información de la que sabemos que había disponible en línea».
– Canadá, 13

CARPETA DEL SISTEMA

8 ELEMENTOS | 105 MB EN EL DISCO | SECCIÓN 3

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

Por qué son importantes los derechos del niño

Los derechos del niño son un hilo conductor que recorre todas las políticas que afectan a la vida de los niños, dentro y fuera de Internet. El objetivo de una política de seguridad infantil en Internet es, fundamentalmente, garantizar que se ejerciten los derechos del niño a la protección y a la participación a medida que interactúan con el mundo digital.

Los niños y sus familias tienen derechos humanos en virtud de la Carta Internacional de Derechos Humanos, incluida la Declaración Universal de Derechos Humanos de 1948, el Pacto Internacional de Derechos Civiles y Políticos de 1966 y el Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966, así como las estructuras regionales y nacionales de derechos humanos.

Concretamente en el caso de los niños, la *Convención sobre los Derechos del Niño de las Naciones Unidas de 1989* («la Convención» o CDN)[15] y sus *Protocolos facultativos relativos a la venta de niños y niñas*[16] y a la *participación de niños en conflictos armados*[17] proporcionan un marco de trabajo práctico para comprender cómo se aplican los derechos humanos a los niños. La Convención es el tratado de derechos humanos más ampliamente ratificado en la historia y su Protocolo Facultativo relativo a un procedimiento de comunicaciones contribuye a que pueda aplicarse para que los derechos del niño sean reales y efectivos.

Todos los derechos de la CDN tienen importancia en materia de seguridad infantil en Internet y hablar con los niños es fundamental para comprender qué significan en la práctica dichos derechos. Por ejemplo, debe tenerse en cuenta el derecho de los niños a jugar, a participar y a la vida familiar en Internet. Todos aquellos que participen en las consultas deben recibir una formación adecuada sobre los derechos del niño y sobre lo que significan en la práctica las opiniones y la inclusión de los niños.

El Comité de los Derechos del Niño de las Naciones Unidas[18] ofrece orientación —en la Observación general núm. 25 (2021)— sobre medidas legislativas, políticas y otras medidas apropiadas para garantizar el total cumplimiento de las obligaciones en virtud del Convenio y de sus Protocolos Facultativos en vista de las oportunidades, riesgos y desafíos para los derechos del niño en el entorno digital. La Observación general núm. 25 (2021) será una herramienta clave que tener en cuenta a la hora de desarrollar una política de seguridad infantil en Internet.

> **Los derechos de todos los niños deben respetarse, protegerse y hacerse efectivos en el entorno digital. Las innovaciones en las tecnologías digitales tienen consecuencias de carácter amplio e interdependiente para la vida de los niños y para sus derechos, incluso cuando los propios niños no tienen acceso a Internet. La posibilidad de acceder a las tecnologías digitales de forma provechosa puede ayudar a los niños a ejercer efectivamente toda la gama de sus derechos civiles, políticos, culturales, económicos y sociales. Sin embargo, si no se logra la inclusión digital, es probable que aumenten las desigualdades existentes y que surjan otras nuevas.**
>
> Fuente: Observación general núm. 25 (2021), párr. 4[19]

15. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
16. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
17. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
18. Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital, Comité de los Derechos del Niño (CDN) de las Naciones Unidas, 2021.
19. Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital, Comité de los Derechos del Niño (CDN) de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

La CDN establece cuatro principios rectores para la protección de los derechos del niño, y la Observación general núm. 25 (2021) describe cómo se aplica en el mundo digital:

1. El derecho a la no discriminación (artículo 2):

El artículo 2 de la Convención sobre los Derechos del Niño[20] establece que todos los niños tienen derecho a disfrutar de sus derechos en condiciones de igualdad, «sin discriminación alguna, independientemente de la raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional, étnico o social, propiedad, discapacidad, nacimiento o cualquier otra condición del niño, de sus padres o de sus representantes legales». Los párrafos 10 y 11 de la Observación general núm. 25 (2011) describen cómo se aplica lo anterior en el mundo digital.

> **Los niños pueden sufrir discriminación si son excluidos del uso de las tecnologías y los servicios digitales o si reciben comunicaciones que transmiten odio o un trato injusto cuando utilizan esas tecnologías. Otras formas de discriminación pueden surgir cuando los procesos automatizados que dan lugar al filtrado de información, la elaboración de perfiles o la adopción de decisiones se basan en datos sesgados, parciales o injustamente obtenidos sobre un niño.**
>
> **El Comité exhorta a los Estados parte a que adopten medidas proactivas para prevenir la discriminación por motivos de sexo, discapacidad, situación socioeconómica, origen étnico o nacional, idioma o cualquier otro motivo, así como la discriminación contra los niños pertenecientes a minorías y los niños indígenas, los niños solicitantes de asilo, refugiados y migrantes, aquellos con orientación sexual lesbiana, gay, bisexual, transexual e intersexual, los que son víctimas y supervivientes de la trata o la explotación sexual, los que están acogidos en modalidades alternativas de cuidado, los privados de libertad y los que se encuentran en otras situaciones de vulnerabilidad. Se necesitarán medidas específicas para cerrar la brecha digital relacionada con el género en el caso de las niñas y para garantizar que se preste especial atención al acceso, la cultura digital, la privacidad y la seguridad en línea.**
>
> Fuente: Observación general núm. 25 (2021), párr. 10-11[21]

20. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Naciones Unidas, 1989.
21. Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital, CDN, 2021.

2. El interés superior del niño (párrafo 1 del artículo 3):

El artículo 3 de la Convención sobre los Derechos del Niño[22] establece que «en todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño». Los párrafos 12 y 13 de la Observación general núm. 25 (2011) describen cómo se aplica lo anterior en el mundo digital.

El interés superior del niño es un concepto dinámico que debe evaluarse adecuadamente en cada contexto. El entorno digital no fue diseñado en un principio para los niños y, sin embargo, desempeña un papel importante en sus vidas. Los Estados parte deben cerciorarse de que, en todas las actuaciones relativas al suministro, la regulación, el diseño, la gestión y la utilización del entorno digital, el interés superior de todos los niños sea una consideración primordial.

En esas actividades, los Estados parte deben recabar la participación de los órganos nacionales y locales encargados de vigilar que se hagan efectivos los derechos de los niños. Al considerar el interés superior del niño, deben tener en cuenta todos los derechos del niño, incluidos su derecho a buscar, recibir y difundir información, a recibir protección contra todo daño y a que sus opiniones se tengan debidamente en cuenta, y deben asimismo garantizar la transparencia en lo tocante a la evaluación del interés superior del niño y a los criterios aplicados al respecto.

Fuente: Observación general núm. 25 (2021), párr. 12-13[23]

3. Derecho a la vida, a la supervivencia y al desarrollo (artículo 6):

El artículo 6 de la Convención sobre los Derechos del Niño[24] exige a los Estados parte que «reconozcan que cada niño tiene el derecho intrínseco a la vida» y que deben «garantizar, en la máxima medida posible, la supervivencia y el desarrollo del niño». El párrafo 15 de la Observación general núm. 25 (2021) describe cómo se aplica lo anterior en el mundo digital.

El uso de dispositivos digitales no debe ser perjudicial, ni sustituir las interacciones personales entre los niños o entre estos y sus padres o cuidadores. Los Estados parte deben prestar especial atención a los efectos de la tecnología en los primeros años de vida, cuando la plasticidad del cerebro es máxima y el entorno social, en particular las relaciones con los padres y cuidadores, es esencial para configurar el desarrollo cognitivo, emocional y social de los niños. En esos primeros años, puede ser necesario tomar precauciones, según el diseño, la finalidad y los usos de las tecnologías. Se debería impartir formación y asesoramiento sobre la utilización adecuada de los dispositivos digitales a los padres, cuidadores, educadores y otros agentes pertinentes, teniendo en cuenta las investigaciones sobre los efectos de las tecnologías digitales en el desarrollo del niño, especialmente durante los tramos críticos de crecimiento neurológico en la primera infancia y en la adolescencia.

Fuente: Observación general núm. 25 (2021), párr. 15[25]

22. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
23. Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital, Comité de los Derechos del Niño (CDN) de las Naciones Unidas, 2021.
24. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
25. Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital, Comité de los Derechos del Niño (CDN) de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

4. El respeto de las opiniones del niño (artículo 12):

El artículo 12 de la Convención sobre los Derechos del Niño[26] exige a los Estados parte que garanticen que «todos los niños que estén en condiciones de formarse un juicio propio» deberán disfrutar «del derecho de expresar su opinión libremente en todos los asuntos que les afectan», y que dichas opiniones deben «tenerse debidamente en cuenta, en función de su edad y madurez». El párrafo 17 de la Observación general núm. 25 (2021) describe cómo se aplica lo anterior en el mundo digital. En el Recurso 1 a continuación también se puede encontrar más información sobre cómo implementar este derecho.

> **Al elaborar leyes, políticas, programas, servicios y formación sobre los derechos del niño en relación con el entorno digital, los Estados parte deben recabar la participación de todos los niños, escuchar sus necesidades y conceder la debida importancia a sus opiniones. Deben asegurarse de que los proveedores de servicios digitales colaboren activamente con los niños, aplicando salvaguardias apropiadas, y tengan debidamente en cuenta las opiniones de estos al concebir sus productos y servicios.**
>
> Fuente: Observación general núm. 25 (2021), párr. 17 [27]

Estos principios son indivisibles y todos deben tenerse en cuenta al desarrollar una política de seguridad en línea para niños. Proporcionan una perspectiva útil para considerar qué significan las otras cinco cuestiones transversales en la práctica y cómo deben implementarse las diez áreas de acción de la política descritas en el kit de herramientas.

Los derechos del niño no solo figuran en el derecho internacional. La mayoría de constituciones o marcos jurídicos nacionales incluyen disposiciones generales de derechos humanos que protegen a los niños. Estas leyes nacionales de derechos humanos también deberían utilizarse para elaborar políticas de seguridad en línea para los niños que den prioridad a la protección y promoción de los derechos del niño.

El Comité de los Derechos del Niño de las Naciones Unidas insta a los Estados a garantizar que las políticas nacionales relativas a los derechos del niño aborden específicamente el entorno digital y que la protección de los niños en línea se integre en las políticas nacionales de protección de la infancia. Este kit de herramientas está diseñado para facilitar esta labor.

26. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Naciones Unidas, 1989.
27. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

Los Estados parte deben cerciorarse de que las políticas nacionales relativas a los derechos del niño aborden específicamente el entorno digital y deben aplicar reglamentaciones, códigos industriales, normas de diseño y planes de acción pertinentes, todo lo cual debe ser evaluado y actualizado periódicamente. Esas políticas nacionales deben tener como objetivo ofrecer a los niños la oportunidad de sacar provecho del entorno digital y garantizar su acceso seguro a él.

La protección digital de los niños debe ser parte integrante de las políticas nacionales de protección de la infancia. Los Estados parte deben aplicar medidas para proteger a los niños de los riesgos asociados con ese entorno, como la ciberagresión y la explotación y los abusos sexuales de niños en línea facilitados por la tecnología digital, asegurarse de que se investiguen esos delitos y ofrecer reparación y apoyo a los niños que sean víctimas de esos actos. Asimismo, deben atender a las necesidades de los niños en situaciones desfavorecidas o de vulnerabilidad, entre otras formas proporcionando información adaptada a los niños y, cuando proceda, traducida a los idiomas minoritarios pertinentes.

Los Estados parte deben garantizar la aplicación de mecanismos eficaces de protección digital de los niños, así como de normativas de salvaguardia, respetando al mismo tiempo los demás derechos del niño, en todos los ámbitos en que estos acceden al entorno digital y que incluyen el hogar, los entornos educativos, los cibercafés, los centros juveniles, las bibliotecas y los centros de atención sanitaria y modalidades alternativas de cuidado.

Fuente: Observación general núm. 25 (2021), párr. 24-26 [28]

Recursos para los derechos del niño:

1. Implementar el respeto de las opiniones del niño a la hora de desarrollar la política de seguridad infantil en Internet:

El respeto de las opiniones del niño debe ocupar un lugar central en la elaboración de políticas prácticas sobre la seguridad de los niños en Internet. Los niños y los jóvenes tienen opiniones fundadas sobre el entorno digital[29] y tienen derecho a expresarlas y a participar en todos los asuntos que les afectan.[30] Para que las políticas de seguridad en línea para niños aborden las necesidades de los niños, los responsables de la formulación de políticas deben escuchar sus opiniones e incluir sus puntos de vista en dichas políticas. Los puntos de vista de los niños sobre el riesgo, los daños, los beneficios y las oportunidades en el entorno digital pueden ser distintos de los de los adultos que los rodean. Por lo tanto, es fundamental contar con la participación de los niños[31] a lo largo del desarrollo, la implementación, la monitorización y la evaluación de las políticas de seguridad infantil en Internet, con el objetivo de garantizar que sus necesidades se satisfagan adecuadamente y que la política les resulte realmente favorable.[32]

28. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
29. En nuestras propias palabras: los derechos del niño en el mundo digital, 5Rights Foundation, 2021.
30. El derecho de las personas a ser escuchadas figura en el Artículo 13 de la Convención.
31. Se deben tener en cuenta los cuatro elementos del modelo Lundy: espacio, voz, audiencia, influencia. Véase «El modelo Lundy de participación infantil».
32. The Digital Futures Commission.

El modelo Lundy presenta un método para comprender «cómo» permitir la participación de los niños, a través de cuatro áreas de enfoque:

Fuente: The Lundy model of child participation (El modelo de participación infantil de Lundy)[33]

Las Directrices sobre la protección de la infancia en línea de la Unión Internacional de Telecomunicaciones reiteran la importancia de escuchar las opiniones y experiencias de los niños para elaborar una política de seguridad infantil en Internet. Garantizar que las voces de los niños se incorporen en cualquier decisión en materia de seguridad infantil en Internet permite elaborar una política más sólida, diversa e inclusiva.

> **Los niños y jóvenes quieren participar en la conversación y pueden compartir su valiosa experiencia como «nativos digitales». Los responsables de formular y ejecutar las políticas deben escuchar en todo momento las opiniones de los niños y los jóvenes sobre el entorno digital para poder apoyar sus derechos.**
>
> Fuente: Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas, Unión Internacional de Telecomunicaciones, 2020.[34]

33. El modelo Lundy de participación infantil, Comisión Europea, 2007.
34. Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas, Unión Internacional de Telecomunicaciones, 2020.

< SECCIÓN ANTERIOR

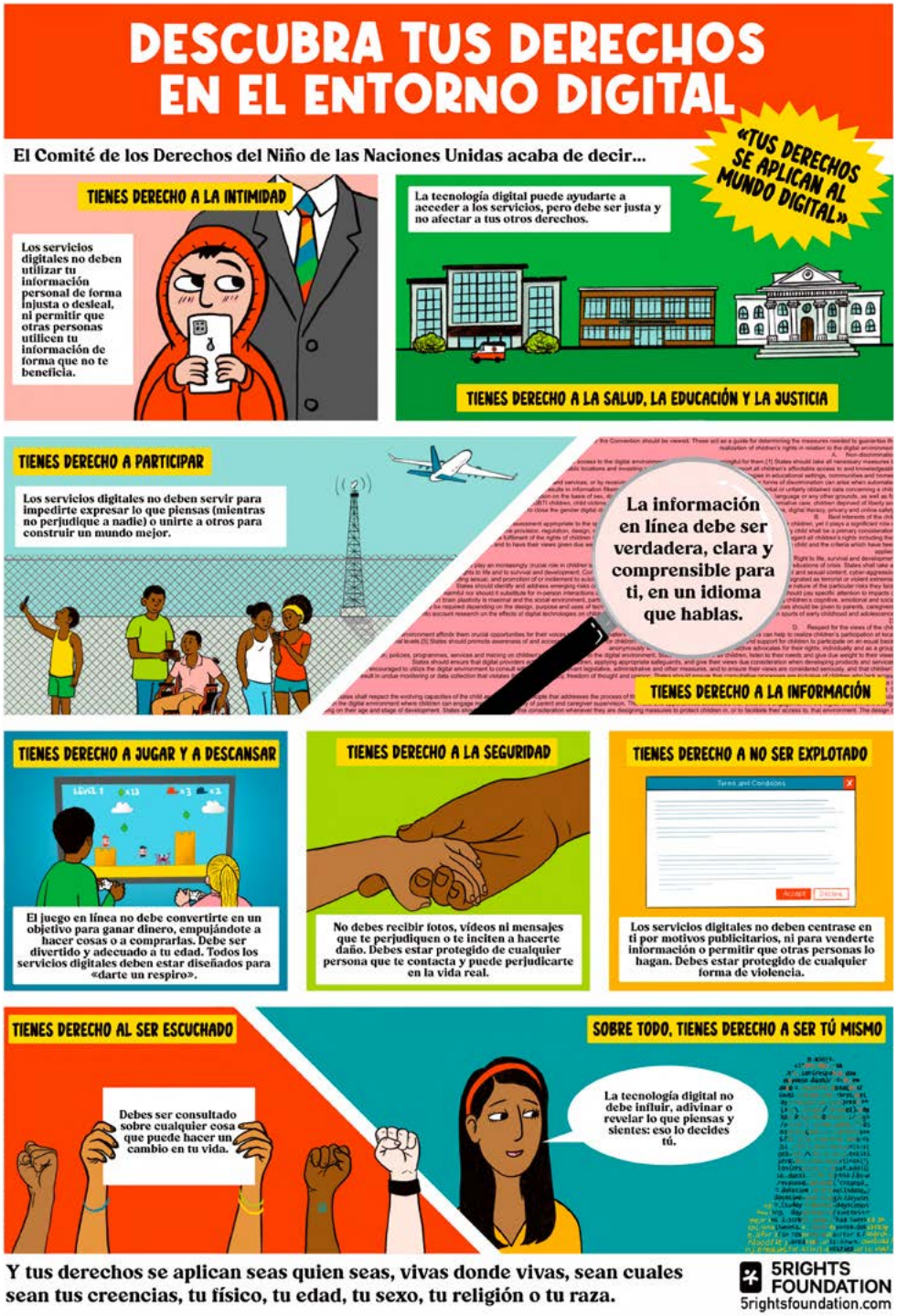
SIGUIENTE SECCIÓN >

2. Ayudar a las personas a entender la Convención sobre los Derechos del Niño:

Fuente: Convención sobre los Derechos del Niño de las Naciones Unidas: versión para niños[35].

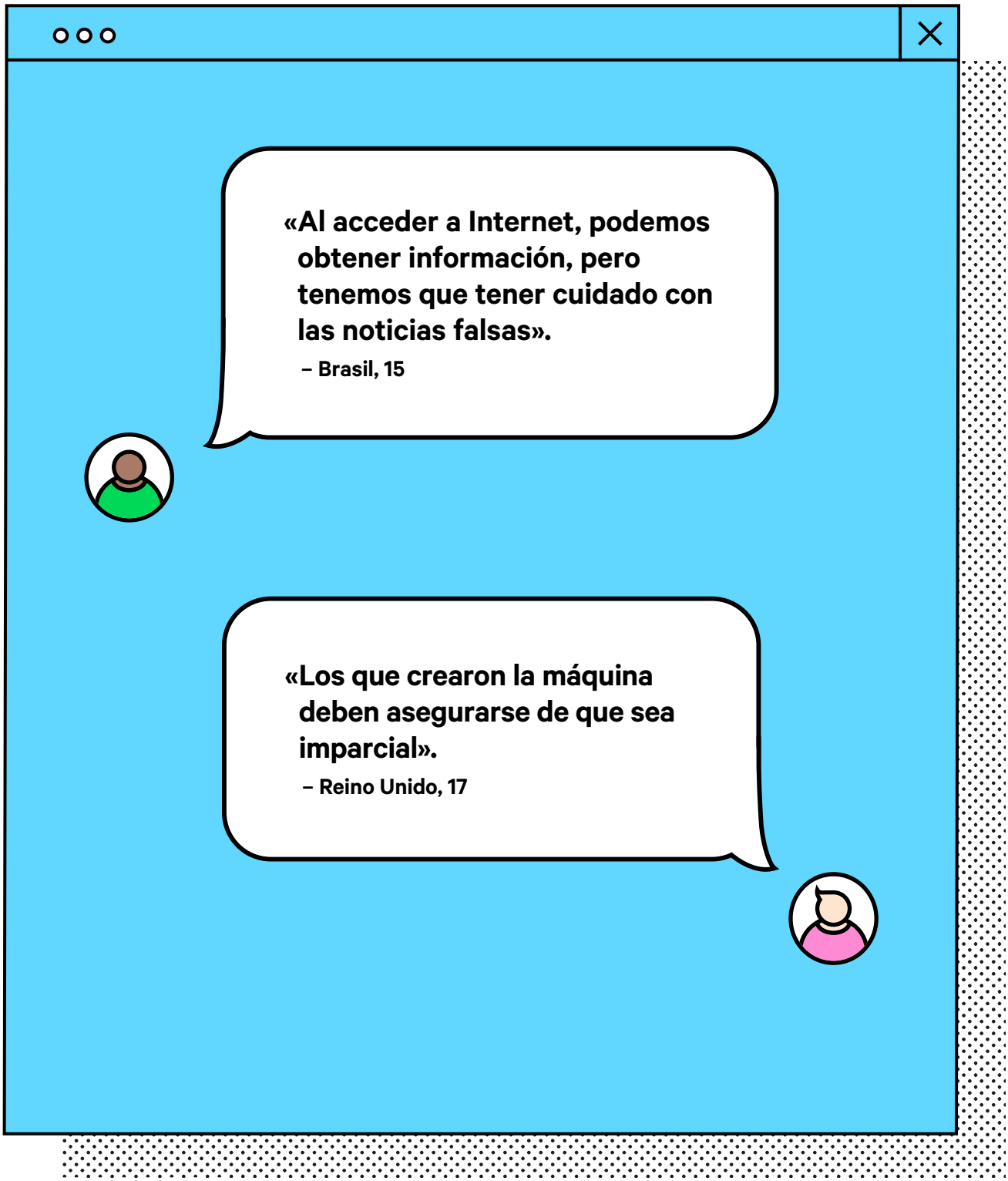
35. La Convención sobre los Derechos del Niño de las Naciones Unidas: versión para niños, Save the Children, 2019.

3. Ayudar a los niños a entender la Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital:



Fuente: Cartel «Know Your Rights!». Observación general núm. 25 (2021)[36]

36. Carteles ¡Know Your Rights! de la Observación general núm. 25 (2021), 5Rights Foundation, 2021.


«Al acceder a Internet, podemos obtener información, pero tenemos que tener cuidado con las noticias falsas».
– Brasil, 15
«Los que crearon la máquina deben asegurarse de que sea imparcial».
– Reino Unido, 17

CARPETA DEL SISTEMA

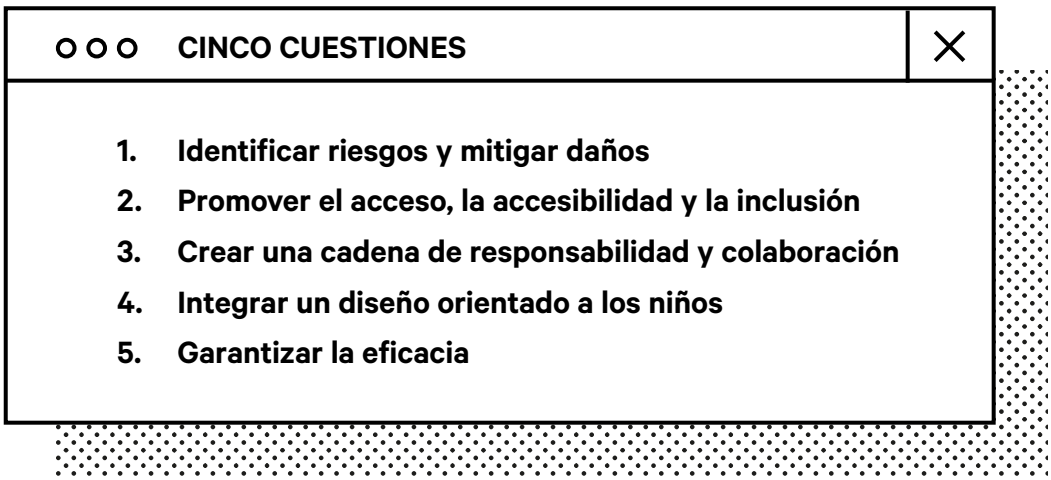
8 ELEMENTOS | 105 MB EN EL DISCO | SECCIÓN 4

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

Cuestiones importantes para los responsables de formular las políticas

Esta sección explora cinco cuestiones transversales que los responsables de la formulación de las políticas deben tener en cuenta a la hora de diseñar, desarrollar e implementar políticas de seguridad infantil en Internet.



Cada una de estas cuestiones debería tenerse en cuenta a la hora de implementar las diez áreas de acción de la política que figuran en la página 38.

1. Identificar riesgos y mitigar daños:

> **Las oportunidades que ofrece el entorno digital desempeñan un papel cada vez más decisivo en el desarrollo de los niños y pueden ser fundamentales para su vida y su supervivencia, especialmente en situaciones de crisis. Los Estados parte deben adoptar todas las medidas apropiadas para proteger a los niños frente a todo riesgo para su derecho a la vida, su supervivencia y su desarrollo. Los riesgos relacionados con los contenidos, los contactos, las conductas y los contratos en ese ámbito abarcan, entre otras cosas, los contenidos violentos y sexuales, la ciberagresión y el acoso, los juegos de azar, la explotación y el maltrato, incluidos la explotación y los abusos sexuales, y la promoción del suicidio o de actividades que pongan en peligro la vida, o la incitación a estos, por parte, entre otros, de delincuentes o grupos armados identificados como terroristas o extremistas violentos. Los Estados parte deben determinar y abordar los nuevos riesgos que afrontan los niños en diversos contextos, por ejemplo escuchando sus opiniones sobre el carácter de los riesgos concretos a los que se enfrentan.**
>
> Fuente: Observación general núm. 25 (2021), párr. 14[37]

Las estrategias de seguridad infantil en Internet deben desarrollarse principalmente para maximizar los beneficios que los niños pueden obtener de las tecnologías digitales. Esto implica necesariamente que existe una responsabilidad primordial de mitigar los riesgos, minimizar la probabilidad de que se produzcan daños, abordar los daños en caso de producirse y considerar cómo pueden afectar los productos y los servicios al usuario final si ese usuario es (o es probable que sea) un menor de 18 años. Es fundamental diseñar productos y servicios en los que se tenga en cuenta a priori la participación segura de los niños.

37. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

Mientras que algunos niños sufren daños graves, millones más experimentan daños en línea de una forma u otra. Por ejemplo, existe una amplia gama de riesgos derivados de la vigilancia o explotación comerciales, la exposición a información falsa, estafas, depredadores o intimidación. Un número menor sufre los graves daños del abuso sexual infantil. Muchos de los riesgos son acumulativos. Los daños repercuten en cada niño de forma distinta y cualquier tipo de daño puede ser la antesala de otro.[38]

Dada la naturaleza global del mundo digital, los niños se enfrentan a muchos riesgos similares en Internet, independientemente de su ubicación geográfica. Pero cada contexto puede plantear cuestiones específicas. En algunos casos, un niño puede estar en desventaja por la falta de acceso al entorno digital. En otros casos, puede haber un vínculo entre los daños causados en Internet y la experiencia del niño fuera del entorno digital. A menudo, determinados riesgos y daños se dan de forma simultánea. Hay muy pocas líneas rectas y las divisiones no suelen estar claras.

Factores como el género, la edad, las circunstancias familiares, el nivel socioeconómico, la ubicación, las experiencias y la disponibilidad de la tecnología digital, pueden alterar los riesgos y las formas en que los niños experimentan los daños. Algunos riesgos y daños afectan a comunidades y clases enteras de niños: por ejemplo, las niñas suelen atraer más abusos pero los casos de abuso en niños tienden a ser más graves.[39] Las normas culturales en torno a la masculinidad también impiden que se detecten y comuniquen muchos casos de abuso sexual de niños varones.[40] Los riesgos y daños también pueden verse potenciados por plataformas diseñadas de una forma que fomenta el intercambio de contenido impactante y sensacionalista, o que perfile o promueva determinados tipos de comportamiento de sus usuarios ya que les ayuda a generar una interacción lucrativa.

Los responsables de formular las políticas deben tener en cuenta todos los riesgos para los niños y dar los pasos necesarios para mitigarlos. Una herramienta clave para identificar el riesgo es el marco de trabajo de «las 4 C».

La clasificación 4C de CO:RE pone de relieve que los riesgos en Internet surgen cuando un niño:

- Interactúa con **contenido** potencialmente dañino o se expone a él.
- Experimenta un contacto potencialmente dañino o es el objetivo de dicho **contacto**.
- Es testigo, partícipe o víctima de una **conducta** potencialmente dañina.
- Ha firmado un **contrato potencialmente dañino o está siendo explotando por el mismo**.

CO:RE	CONTENIDO Niño como destinatario	CONTACTO Niño como participante	CONDUCTA Niño como actor	CONTRATO Niño como consumidor
Agresivo	Contenido violento, sangriento, explícito, racista, lleno de odio y extremista	Acoso, comportamiento de odio, vigilancia no deseada	Acoso escolar, actividad de odio u hostil entre compañeros (por ejemplo, trolling, exclusión, humillación)	Robo de identidad, fraude, phishing, estafas, apuestas, chantaje, riesgos de seguridad
Sexual	Pornografía (legal e ilegal), sexualización de la cultura, normas de imagen corporal	Acoso sexual, engaño por parte de pederastas (o «grooming»), crear y compartir material de explotación sexual infantil	Acoso sexual, mensajes sexuales no consentidos, presiones sexuales	Extorsión sexual, trata con fines de explotación sexual, transmisión en línea de abusos sexuales infantiles
Valores	Contenido generado por el usuario o de marketing inapropiado para la edad, información errónea/ desinformación	Persuasión ideológica, radicalización y reclutamiento extremista	Comunidades de usuarios potencialmente dañinas (por ejemplo, autolesiones, antivacunas, presión de grupo)	Filtrado de información, elaboración de perfiles sesgada, polarización, diseño persuasivo
Transversal	Abusos en materia de privacidad y protección de datos, riesgos para la salud física y mental, formas de discriminación			

Fuente: CO:RE Content, Contact, Conduct, Contract – Updating the 4Cs of online risk (Contenido, Contacto, Conducta, Contrato: actualización de las 4 «C» del riesgo en Internet), 2021 [41]

38. Building the digital world that young people deserve (Creando el mundo digital que merece la juventud), 5Rights Foundation, 2020.
39. Safe Online Investment Portfolio Results 2020 (Resultados 2020 de la cartera de inversión segura en Internet), Alianza mundial para poner fin a la violencia contra niñas, niños y adolescentes, 2020. pág. 2.
40. Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse (Daños perturbadores en Kenia: evidencias de explotación y abuso sexuales infantiles), Alianza mundial para poner fin a la violencia contra niñas, niños y adolescentes, 2021. pág. 68.
41. Content, Contact, Conduct, Contract - Updating the 4Cs of Online Risk (Contenido, Contacto, Conducta, Contrato; actualización de las 4 «C» del riesgo en Internet), CO:RE 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

Con la expansión de la banda ancha asequible a los países en vías de desarrollo, existe una necesidad apremiante de poner en marcha medidas para minimizar los riesgos y las amenazas para estos niños, sin impedir que puedan aprovechar todas las ventajas del mundo digital.

Fuente: Directrices sobre la protección de la infancia en línea de la Unión Internacional de Telecomunicaciones 2020[42]

Los Estados parte deben tener en cuenta la constante evolución de los niños y de su nivel de autonomía en el mundo moderno, así como su grado de competencia y comprensión, que se desarrollan de forma desigual en las distintas esferas de aptitud y actividad, y la diversa naturaleza de los riesgos posibles. Ahora bien, debe lograrse un equilibrio entre estas consideraciones y la importancia de que los niños ejerzan sus derechos en entornos que les proporcionen el apoyo necesario, por un lado, y la variedad de experiencias y circunstancias individuales, por otro. Los Estados parte deben garantizar que los proveedores de servicios digitales ofrezcan servicios acordes con la evolución de las facultades de los niños.

Fuente: Observación general núm. 25 (2021), párr. 20[43]

2. Promover el acceso, la accesibilidad y la inclusión

Los derechos de todos los niños deben respetarse, protegerse y hacerse efectivos en el entorno digital. Las innovaciones en las tecnologías digitales tienen consecuencias de carácter amplio e interdependiente para la vida de los niños y para sus derechos, incluso cuando los propios niños no tienen acceso a Internet. La posibilidad de acceder a las tecnologías digitales de forma provechosa puede ayudar a los niños a ejercer efectivamente toda la gama de sus derechos civiles, políticos, culturales, económicos y sociales. Sin embargo, si no se logra la inclusión digital, es probable que aumenten las desigualdades existentes y que surjan otras nuevas.

Fuente: Observación general núm. 25 (2021), párr. 4[44]

Hoy en día, el acceso al mundo de Internet es crucial para que los niños ejerzan sus derechos y alcancen su máximo potencial. Una política de seguridad infantil en Internet debe ser inclusiva, tanto en su ambición como en la práctica.[45] Esto significa que debe contar con recursos suficientes y basarse en las mejores prácticas y marcos de trabajo existentes, en particular en situaciones en las que los recursos son limitados. Tanto si la implementación de la política de seguridad infantil en Internet implica adaptar la legislación existente (por ejemplo, en lo relativo a la protección del niño, la protección del consumidor o las normativas de telecomunicaciones) al contexto de la seguridad infantil en Internet, como si se deben crear nuevos organismos jurídicos, debe promover la inclusión y la igualdad de todas los niñas, niños y adolescentes sin importar quiénes sean o dónde se encuentren.

Los Estados parte deben promover las innovaciones tecnológicas que satisfagan las necesidades de los niños con diferentes tipos de discapacidad y garantizar que los productos y servicios digitales están diseñados en función de la accesibilidad universal para que puedan ser utilizados por todos los menores de 18 años sin excepción y sin necesidad de adaptación. Los niños con discapacidad deben participar en el diseño y la implementación de políticas, productos y servicios que contribuyan a hacer efectivos sus derechos en el entorno digital.

Fuente: Observación general núm. 25 (2021), párr. 91[46]

42. Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas, Unión Internacional de Telecomunicaciones, 2020.
43. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
44. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN, 2021.
45. Por ejemplo: niños con discapacidades o niños de grupos minoritarios y marginados, niños que viven en la calle, desplazados o migrantes. Esta cuestión se analiza más a fondo en los temas intersectoriales que figuran a continuación. Hay más información sobre el modelo y la lista de verificación en «"Voice" is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child», Laura Lundy, 2013.
46. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

Los niños no son un grupo homogéneo. Las políticas de seguridad infantil en Internet deben ser accesibles e inclusivas para llegar a todas las niñas, niños y adolescentes, sean quienes sean y vivan donde vivan. Es muy probable que surja una «brecha digital» y que algunos niños dispongan de fácil acceso al entorno digital mientras que otros queden completamente excluidos. Los marcos de trabajo deben ser apropiados a las distintas edades y funcionar para todos los niños, independientemente de su género, raza, religión, nacionalidad, origen étnico, discapacidad o cualquier otra característica. El lenguaje debe ser accesible e inclusivo y, en caso de ser necesario, los materiales deben estar disponibles en una amplia gama de idiomas. Los materiales de seguridad infantil en Internet deben diseñarse previa consulta con niñas, niños y sus figuras parentales/cuidadores. Como mínimo, deben resultar apropiados para las distintas edades, utilizar un lenguaje inclusivo y ser fácilmente accesibles para niños de distintas edades y para sus padres/cuidadores. En lugares con una baja tasa de alfabetización, los materiales visuales servirán para transmitir los mensajes de una forma más eficaz. El uso de términos coherentes en todas las plataformas ayuda a que la seguridad infantil en Internet se entienda mejor y sea accesible para los niños, para sus familias y sus cuidadores.[47]

Los responsables de la formulación de políticas deben garantizar que están promoviendo el acceso de los niños a Internet e incluirlos en sus decisiones para lograr que los entornos digitales sean seguros.

> **Tanto los adultos como los niños están expuestos a una serie de riesgos y peligros en línea. No obstante, los niños son una población mucho más vulnerable. Algunos grupos de niños también son más vulnerables que otros, como los niños con discapacidades o los niños en movimiento. Los responsables de formular las políticas deben garantizar que todos los niños puedan crecer y formarse en un entorno digital seguro. La idea de que los niños son vulnerables y deben ser protegidos de todas las formas de explotación está expresada en la Convención de los Derechos del Niño de las Naciones Unidas.**
>
> Fuente: Directrices sobre la protección de la infancia en línea de la Unión Internacional de Telecomunicaciones 2020[48]

3. Crear una cadena de responsabilidad:

> **A fin de abarcar las consecuencias transversales que tiene el entorno digital en los derechos del niño, los Estados parte deben asignar a un órgano gubernamental el mandato de coordinar las políticas, las directrices y los programas relacionados con dichos derechos entre los departamentos de la administración central y los distintos niveles de gobierno. Ese mecanismo de coordinación nacional debe implicarse con las escuelas y el sector de la tecnología de la información y las comunicaciones y cooperar con las empresas, la sociedad civil, el mundo académico y las organizaciones a fin de hacer efectivos los derechos del niño en relación con el entorno digital en los planos intersectorial, nacional, regional y local. Asimismo, debe aprovechar los conocimientos tecnológicos y otros conocimientos especializados pertinentes dentro y fuera de la administración, según sea necesario, y ser sometido a evaluación de forma independiente para comprobar su eficacia en el cumplimiento de sus obligaciones.**
>
> Fuente: Observación general núm. 25 (2021), párr. 27[49]

La responsabilidad de la seguridad infantil en Internet está en manos de muchos actores; desde especialistas a organizaciones, incluidos el Gobierno, las fuerzas del orden, las empresas, los educadores, las redes de apoyo psicosocial, las familias y los niños. Algunos eslabones de la cadena tienen una mayor responsabilidad.[50] Por ejemplo, un servicio al que es probable que accedan los niños o que tenga un impacto en ellos debe plantearse si alguna de sus características representa un riesgo para ellos. Se deben tomar medidas a este respecto antes de interactuar con cualquier usuario infantil. Esto suele denominarse como «seguridad por diseño» o «diseño centrado en niñas, niños y adolescentes». La seguridad por defecto debería ser la norma.

47. Véase la introducción sobre la importancia del lenguaje y las definiciones y la sección del glosario.
48. Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas, Unión Internacional de Telecomunicaciones, 2020.
49. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
50. Véase, por ejemplo, los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

Cadena de responsabilidad de las partes interesadas

Asumir la responsabilidad de la seguridad infantil en Internet implica tanto prevenir los daños antes de que se produzcan como tomar medidas cuando las cosas no vayan bien. Los mecanismos de quejas y denuncias deben ser accesibles y estar claramente identificados para que los niños, los cuidadores y los profesionales que los necesiten puedan encontrarlos y utilizarlos con facilidad. En los sistemas empresariales en línea deben establecerse mecanismos que permitan el seguimiento y la evaluación de las denuncias, de modo que puedan identificarse y abordarse rápidamente las cuestiones problemáticas.

Las leyes y los reglamentos deben establecer marcos de trabajo claros para la prevención y la responsabilidad y para la reparación, en caso de que algo salga mal. Esto incluye la recopilación de datos sobre denuncias y quejas con el fin de realizar un seguimiento y analizarlos de cara a introducir mejoras en el sistema. No se debe hacer responsables a los niños ni a los padres o a los cuidadores de prevenir o abordar riesgos y daños que apenas entienden o sobre los que no tienen casi ningún control. El consentimiento no puede esgrimirse para eximir a las organizaciones públicas o privadas de sus responsabilidades en lo relativo a la seguridad infantil en Internet. Integrar la seguridad de los niños en Internet en los marcos de trabajo existentes para la seguridad de los productos[51], la protección de la infancia[52], los derechos del niño[53] y los derechos de los consumidores[54] puede ayudar a evitar lagunas en la responsabilidad y la duplicación de recursos, roles y responsabilidades. No debería ni debe hacer vacíos legales que socaven la seguridad de los niños en Internet.

Es fundamental que la seguridad infantil en Internet se incorpore y se integre en todos los ámbitos políticos relacionados, desde los planes nacionales de banda ancha hasta los planes de estudio, de forma transparente, responsable y ejecutable. La creación de silos puede dar lugar a conflictos normativos y a una fragmentación de la formulación y de la aplicación de las políticas.

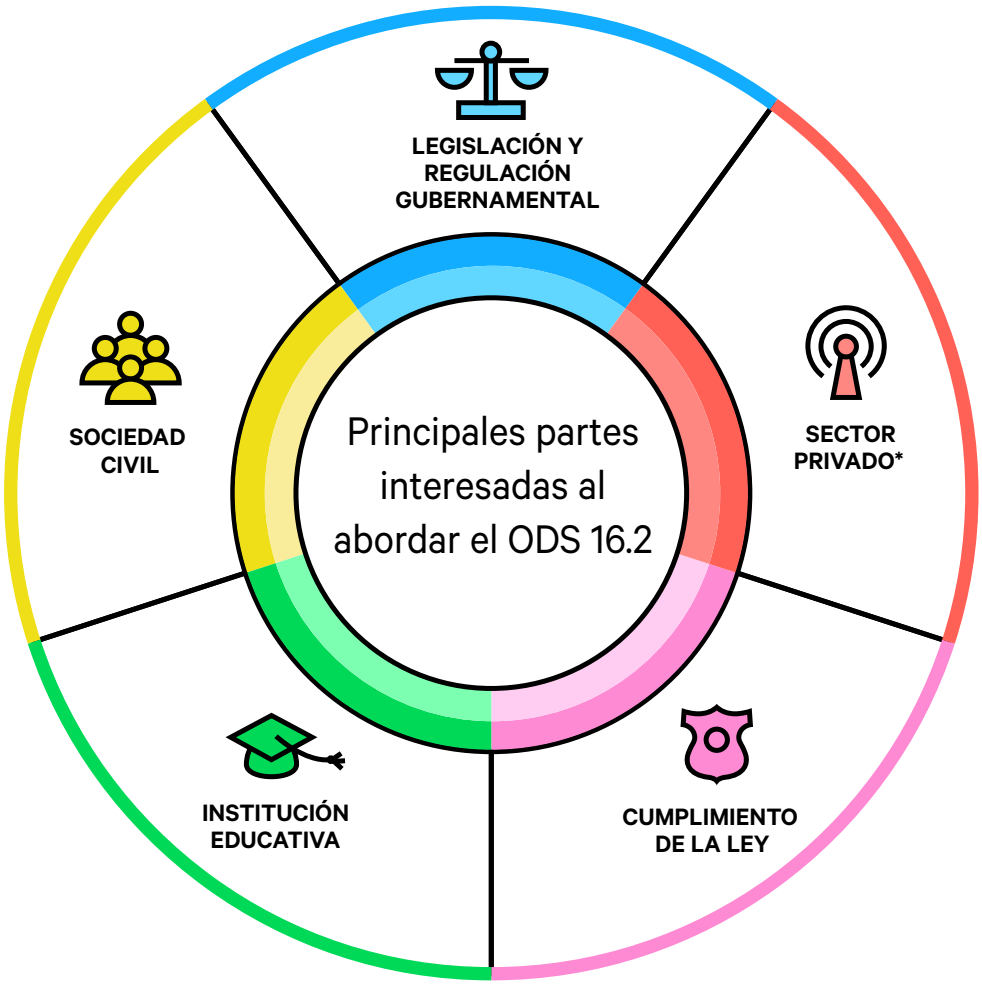
Los responsables de la formulación de políticas deben asumir la complejidad de la responsabilidad de la seguridad infantil en Internet y garantizar que existan mecanismos de cooperación y ayuda para todos los miembros de la cadena, para que puedan desempeñar su papel en la protección de la infancia. También es fundamental comprender claramente las funciones, las responsabilidades y los principales actores en ámbitos específicos.

> **La protección de los niños y jóvenes es una responsabilidad compartida y todas las partes interesadas deben garantizar un futuro sostenible para todos. Para que esto suceda, los responsables de formular las políticas, la industria, los padres, los cuidadores, los educadores y otras partes interesadas deben garantizar que los niños y los jóvenes puedan desarrollar su potencial, tanto dentro como fuera del entorno digital.**
>
> Fuente: Directrices sobre la protección de la infancia en línea de la Unión Internacional de Telecomunicaciones 2020[55]

> **Una buena gobernanza reúne a los actores responsables de proteger a los niños de la explotación sexual en Internet y es un organismo (u organismos) nacional, multisectorial y de múltiples partes interesadas. No existe un modelo único que el organismo de múltiples partes interesadas deba adoptar: podría ser responsable de la gobernanza y supervisión generales de la capacidad de un país para prevenir y responder a la explotación sexual de niños, niñas y adolescentes (ESIA) en línea o simplemente actuar como un organismo para coordinar los trabajos del gobierno, la industria y la sociedad civil.**
>
> Fuente: Modelo de respuesta nacional de la Alianza Mundial WeProtect 2016[56]

51. Standards and risks for specific products (Estándares y riesgos de productos específicos), Comisión Europea, 2014.
52. Child Protection Hub (Central de protección infantil), Comisión Europea, 2021.
53. Estrategia del Consejo de Europa para los derechos de los niños y las niñas, 2021.
54. Directiva sobre los derechos de los consumidores, Comisión Europea, 2014.
55. Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas, Unión Internacional de Telecomunicaciones, 2020.

Estas responsabilidades también se reflejan en otros compromisos, incluidos los Objetivos de Desarrollo Sostenible codificados como Objetivo 16.2: «Poner fin al maltrato, la explotación, la trata y todas las formas de violencia y tortura contra los niños».



*Incluye operadores, ISP, proveedores de contenido, redes sociales y plataformas de mensajería

Fuente: Broadband Commission – Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (Seguridad infantil en Internet: minimizar el riesgo de violencia, acoso y explotación en Internet) 2019[57]

56. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Evitar y abordar la explotación sexual de niños, niñas y adolescentes (ESIA), Alianza Global WeProtect, 2016.
57. Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online, Broadband Commission, 2019.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

4. Integrar un diseño orientado a los niños:

> **Los Estados parte deben establecer normas para evitar los daños conocidos y tener en cuenta de forma proactiva las nuevas investigaciones y pruebas en el sector de la salud pública a fin de evitar la difusión de información errónea y de materiales y servicios que puedan dañar la salud mental o física de los niños. También puede ser necesario adoptar medidas para prevenir cualquier participación perjudicial en juegos digitales o en las redes sociales, por ejemplo, reglamentaciones que prohíban los programas digitales que menoscaben el desarrollo y los derechos del niño.**
>
> Fuente: Observación general núm. 25 (2021), párr. 96[58]

La seguridad infantil en Internet debe integrarse en el diseño y en el desarrollo de la tecnología. El diseño centrado en niñas, niños y adolescentes incorpora la seguridad infantil en Internet en los servicios y productos desde el principio. También se debería garantizar que la seguridad infantil en Internet se tenga en cuenta en los requisitos normativos para el diseño y la concesión de licencias de nuevas tecnologías[59]. El diseño centrado en niñas, niños y adolescentes también puede denominarse seguridad/derechos/privacidad/ética por diseño.

Aplicar el principio de cautela[60] a las tecnologías que pueden afectar a los niños y jóvenes garantiza que la seguridad del niño se tenga en cuenta desde una fase temprana. La Comisión Mundial de Ética del Conocimiento Científico y la Tecnología (COMEST, por sus siglas en inglés) de la UNESCO presentó una «definición práctica» del principio de cautela:

> **«Cuando las actividades humanas pueden acarrear un daño moralmente inaceptable que es científicamente plausible pero incierto, se adoptarán medidas para evitar o disminuir ese daño.**
>
> **Un perjuicio moralmente inaceptable es aquel que se causa a seres humanos o al medioambiente y que es:**
>
> - **una amenaza contra la salud o la vida humanas, o**
> - **grave e irreversible, o**
> - **injusto para las generaciones presentes o futuras, o**
> - **impuesto sin tener debidamente en cuenta los derechos humanos de los afectados».[61]**

El principio de cautela debe servir de guía para crear un marco de trabajo para la seguridad y la privacidad por diseño que garantice que la seguridad infantil en Internet y los derechos del niño se incorporen a la tecnología en la fase de diseño. El diseño centrado en niñas, niños y adolescentes no debe ser únicamente un concepto ético, sino un requisito legal.[62] También debería incorporarse en los criterios para financiar la investigación y el desarrollo que puedan afectar a los derechos del niño en línea.

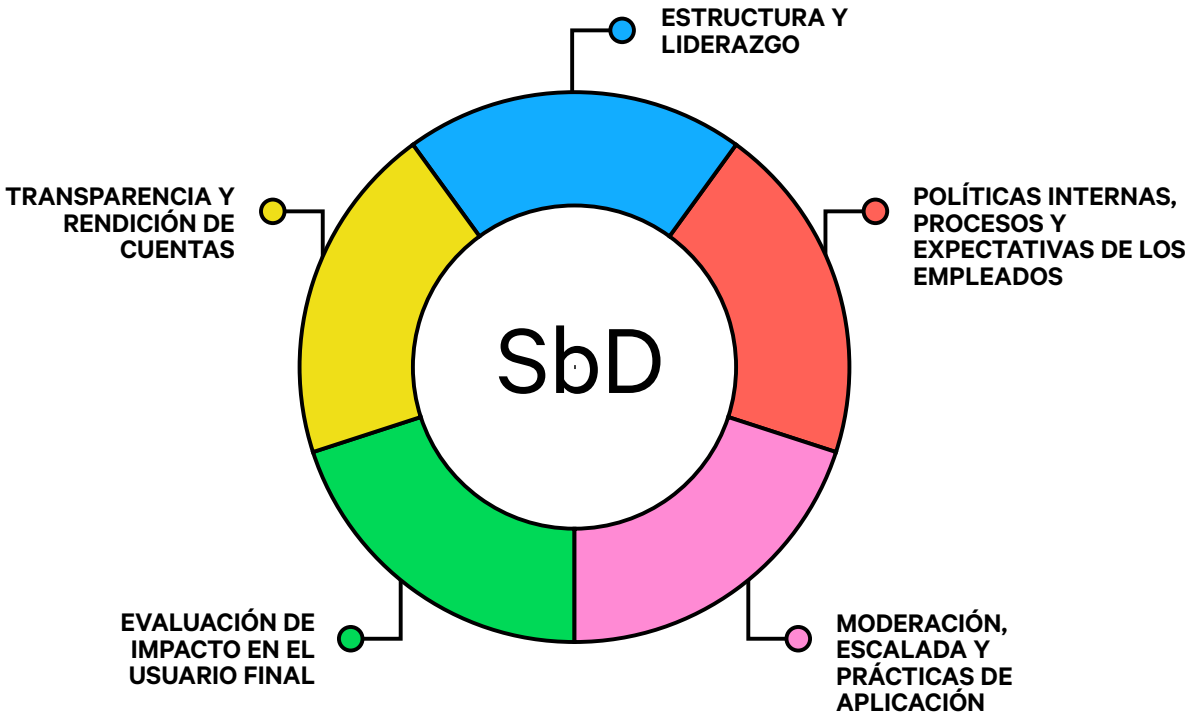
La tecnología y la inteligencia artificial (IA) tienen la capacidad de mejorar la seguridad infantil en Internet y de proteger sus derechos. Respaldar el desarrollo de herramientas tecnológicas para hacer efectivos los derechos del niño y mejorar la seguridad infantil en Internet es un aspecto importante de cualquier política de seguridad infantil en Internet. Se deben evaluar las repercusiones generalizadas de la IA y otras tecnologías para proteger a los niños considerando sus derechos[63] para evitar socavar otros derechos como la privacidad y la no discriminación.

58. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
59. Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principios voluntarios para contrarrestar la explotación y abuso sexuales infantiles en Internet), GOV.UK, 2021.
60. Véanse los siguientes documentos: Comunicación de la Comisión sobre el recurso al principio de cautela EUR-Lex, 2000; The precautionary principle: Definitions, applications and governance (El principio de cautela: definiciones, aplicaciones y gobernanza), Parlamento Europeo,2015.
61. Informe del Grupo de Expertos sobre el principio de cautela, Comisión Mundial de Ética del Conocimiento Científico y la Tecnología, 2005.
62. Véase, por ejemplo, el artículo 25 del Reglamento General de Protección de Datos, Unión Europea, 2018.
63. Véase, por ejemplo, la Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

Los niños son extremadamente diversos de por sí y se debe tener en cuenta todo el abanico de características, experiencias y contextos de los niños en la elaboración y la aplicación de las políticas, así como en la supervisión de su eficacia. Unas medidas eficaces en materia de seguridad infantil en Internet deberían abordar las tensiones que se perciban. Por ejemplo, en los debates sobre el cifrado, los defensores de la protección contra la explotación sexual de niños, niñas y adolescentes (ESIA) podrían encontrarse con que sus argumentos entran en conflicto con los relacionados con la privacidad y la protección de datos. Esos conflictos deben resolverse para alcanzar conclusiones prácticas y de esta manera evitar un círculo vicioso de años de debates mientras los niños corren peligro o sufren daños. En dichos casos, el «interés superior» del niño debe anteponerse a cualquier otra cuestión.[64]

Existen varios marcos de trabajo y procesos que apoyan la aplicación del diseño centrado en niñas, niños y adolescentes en la formulación de políticas, incluidos el principio de cautela, las evaluaciones de impacto infantil[65] y las consultas a los niños.[66] Además, el Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) ha creado una norma con pasos prácticos que las empresas pueden seguir para diseñar productos y servicios digitales que sean apropiados para cada edad,[67] y la Digital Futures Commission ha establecido cómo se podría apoyar el derecho de los niños a jugar libremente en un mundo digital mejorando el diseño de los productos y servicios digitales. Los responsables de la formulación de políticas deben procurar siempre que los productos y servicios reduzcan al mínimo los riesgos antes de ponerlos a disposición de los niños. La seguridad por diseño y los derechos por diseño son de naturaleza sistémica y, por lo tanto, su objetivo es proteger a millones de niños desde el principio, no después de los hechos.



Source: Iniciativa Safety by Design[68] de eSafety: Self-Assessment Tools and Principles (Herramientas y principios de autoevaluación)[69]

64. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989. (Véase, en concreto, la sección 1 del artículo 3 de los Derechos del Niño).
65. Child Rights Impact Assessment (Evaluación del impacto en los derechos del niño), Digital Futures Commission, 2021.
66. Child Rights Impact Assessment, Digital Futures Commission, 2021.
67. IEEE 2089-21 Standard for Age-Appropriate Digital Services Framework, IEEE SA, 2021.
68. Principios de Safety by Design, eSafety Commissioner, 2021.
69. Principios de Safety by Design, eSafety Commissioner, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5. Garantizar la eficacia:

> **Los Estados parte deben movilizar, asignar y utilizar recursos públicos para aplicar leyes, políticas y programas que permitan hacer plenamente efectivos los derechos del niño en el entorno digital y mejorar la inclusión digital, que es necesaria para hacer frente al creciente impacto del entorno digital en la vida de los niños y para promover la igualdad de acceso a los servicios y la conectividad, así como su asequibilidad.**
>
> **Los Estados parte deben cerciorarse de que los mandatos de las instituciones nacionales de derechos humanos y otras instituciones independientes pertinentes abarquen los derechos del niño en el entorno digital y que estas puedan recibir, investigar y atender las denuncias presentadas por niños y sus representantes. Cuando existan órganos de supervisión independientes encargados de vigilar las actividades relacionadas con el entorno digital, las instituciones nacionales de derechos humanos deben colaborar estrechamente con esos órganos para garantizar el cumplimiento efectivo de su mandato en relación con los derechos del niño.**
>
> Fuente: Observación general núm. 25 (2021), párr. 28 y 31[70]

La seguridad de los niños en Internet y los derechos del niño en el entorno digital solo pueden ser verdaderamente eficaces a través de intervenciones normativas prácticas, los recursos adecuados y la aplicación de la ley.

La seguridad de los niños en Internet es importante para una amplia gama de ámbitos normativos, incluidas las tecnologías de la información y la comunicación (TIC), la educación, la justicia penal, la salud, las regulaciones del sector, el apoyo social y familiar, el mundo empresarial, los derechos humanos y la igualdad, el desarrollo internacional y muchos otros. Por lo tanto, la cooperación entre los distintos ministerios y organismos que trabajan en ámbitos normativos es fundamental para la adopción de medidas eficaces en materia de seguridad de los niños en Internet. Será necesario elaborar presupuestos para dotar de recursos a las políticas, tanto dentro de los distintos departamentos como entre ellos. Las políticas sin suficientes fondos o las alianzas sin capacidad de acción —es decir, que solo existen sobre el papel— no lograrán proteger eficazmente a los niños en Internet.

Si se quieren desarrollar soluciones eficaces, se deben valorar las repercusiones de las políticas de seguridad infantil en Internet. El seguimiento, la evaluación y la recopilación de datos son esenciales para permitir un desarrollo satisfactorio de las políticas. Estudiar las políticas que funcionan en otros países y compartir las experiencias propias es una buena manera de maximizar la eficacia. Comprobar la eficacia de la una política de seguridad en línea para los niños no solo requiere realizar una consulta a los actores clave involucrados, sino también a los niños, para comprender cómo les afectan o podrían afectarles en un futuro las medidas.[71] Se trata de un proceso continuo.

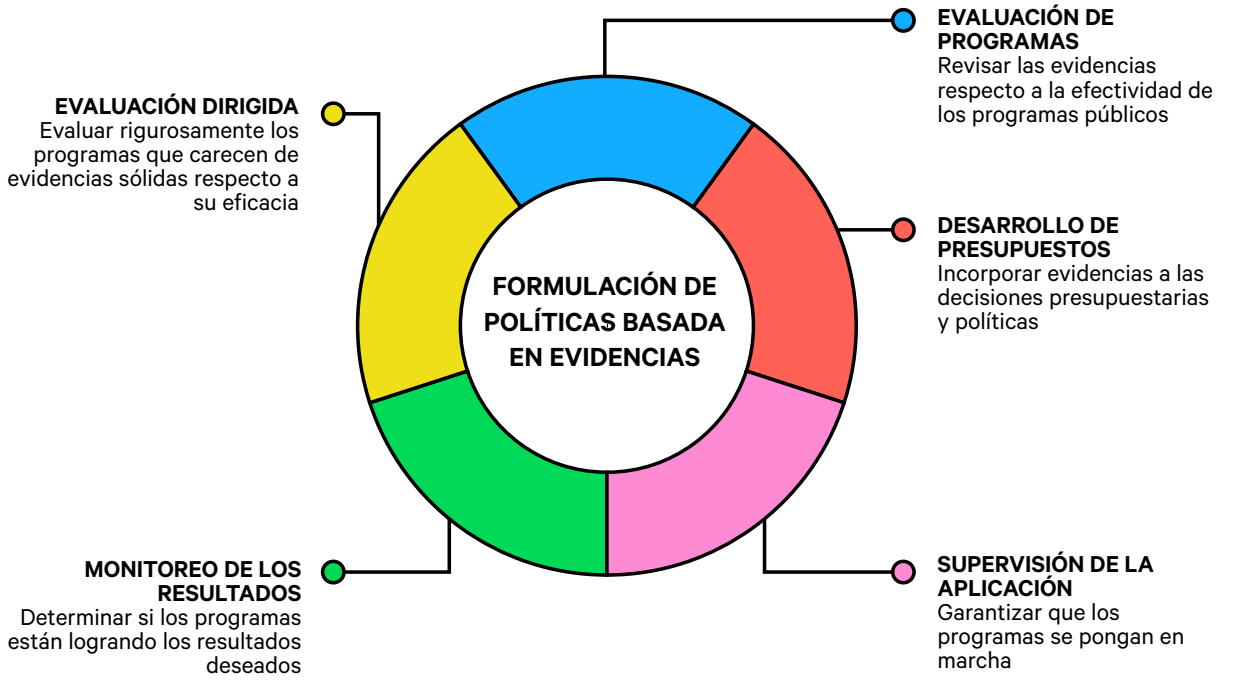
Las políticas deben basarse en datos y evidencias. Debería exigirse tanto a las autoridades pertinentes como a las empresas privadas que recopilen y compartan datos para comprender mejor las cuestiones relativas a la protección de los niños en Internet, de conformidad con las leyes y los principios de protección de datos. La seguridad infantil en Internet es un ámbito de actuación relativamente nuevo, por lo que cuando no se disponga de evidencias o estas se rebatan, los responsables de la formulación de políticas deberán adoptar un enfoque preventivo o analizar otros contextos y adoptar un enfoque sobre «lo que funciona». Por ejemplo, con principios de salud y de seguridad o con marcos de trabajo como «INSPIRE: siete estrategias para poner fin a la violencia contra los niños y las niñas».[72]

70. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
71. Digital Futures Commission, 5Rights Foundation, 2021.
72. INSPIRE Indicator Guidance and Results Framework (Guía de indicadores y marco de resultados de INSPIRE), Organización Mundial de la Salud, 2018.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

La seguridad infantil en Internet no es un problema aislado. La eficacia de una política de seguridad infantil en Internet dependerá de la eficacia general de las instituciones clave y de su capacidad para colaborar con miras a una protección eficaz. Para garantizar un sistema eficaz de rendición de cuentas en relación a la seguridad infantil en Internet y, en particular, respecto a la prevención de la explotación sexual de niñas, niños y adolescentes se debe contar con el amparo de sistemas judiciales sólidos a nivel nacional. El Modelo de respuesta nacional ofrece una serie de orientaciones sobre esta cuestión. Además, para que el enfoque de la seguridad infantil en Internet sea eficaz, las instituciones involucradas deben disponer de recursos suficientes, incluidos ámbitos como la asistencia psicosocial, las normativas en materia de TIC u otros campos relacionados. Para poder defender los derechos del niño de forma eficaz mediante una política de seguridad en línea para los niños, se requieren legislaciones eficaces de derechos humanos y leyes y normativas específicas con organismos de supervisión para garantizar los derechos del niño tanto dentro como fuera del entorno digital.

Los responsables de formular las políticas deben garantizar que la capacidad institucional, los recursos y los mecanismos de rendición de cuentas sustenten las políticas de seguridad infantil en Internet. En caso de que surjan conflictos, la prioridad debe ser el «interés superior» de los niños. Si no se tiene en cuenta esta premisa, ni siquiera la mejor política resultará eficaz.

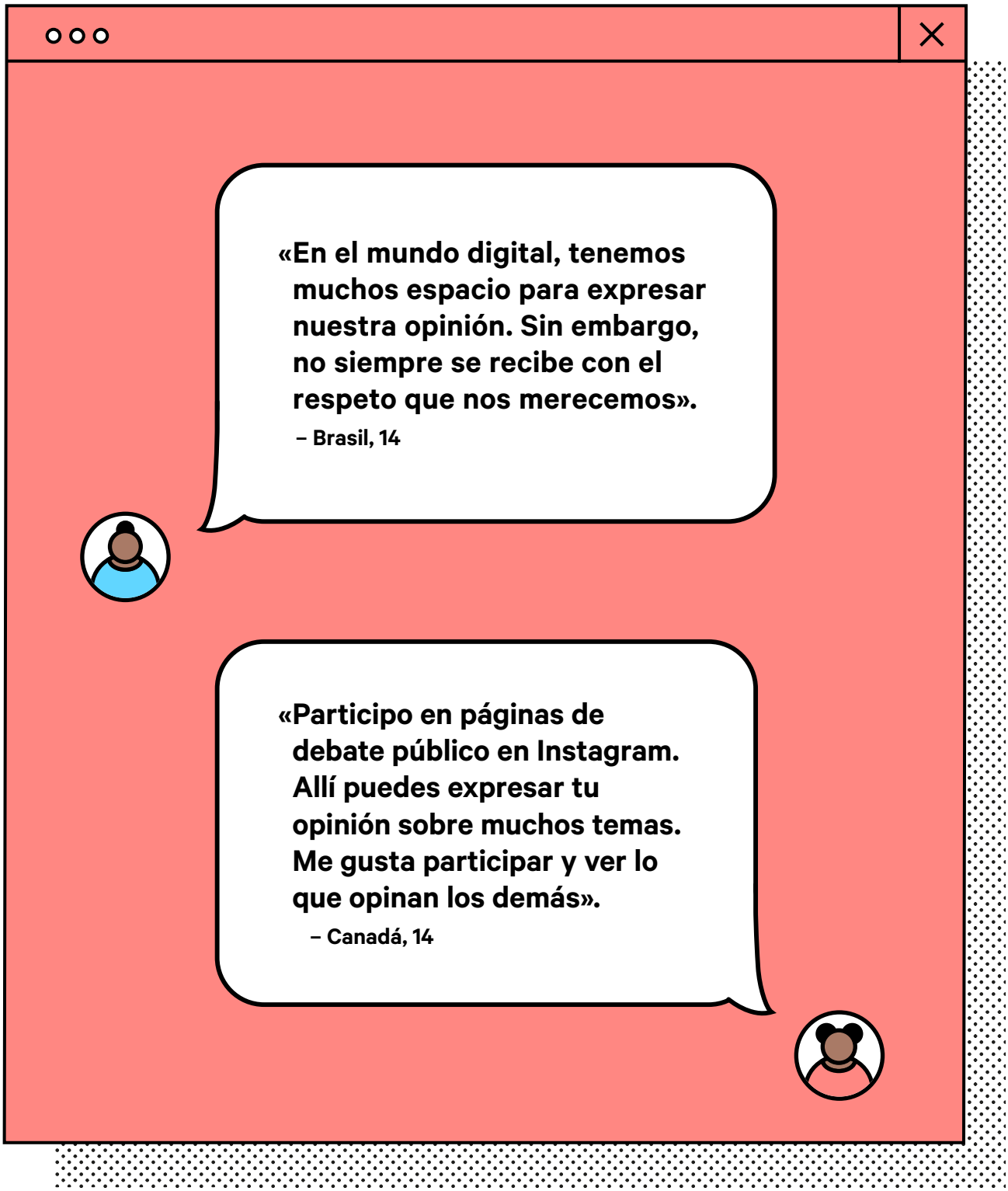


Fuente: Pew Charitable Trusts/MacArthur Foundation: Evidence-Based Policymaking (Formulación de políticas basadas en la evidencia)[73]

73. Evidence-Based Policymaking (Formulación de políticas basadas en la evidencia), MacArthur Foundation, 2014.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >



CARPETA DEL SISTEMA

8 ELEMENTOS | 105 MB EN EL DISCO | SECCIÓN 5

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

Diez áreas de acción de la política

En esta sección se ofrecen políticas modelo que describen las acciones prácticas necesarias para elaborar una política eficaz de seguridad infantil en Internet, así como herramientas para que los responsables de formular las políticas diseñen e implementen mecanismos eficaces y relevantes para su contexto nacional.

POLÍTICAS MODELO

1. Capacidad institucional
2. Marcos jurídicos y reguladores
3. Datos personales, identidad y autonomía
4. Sistemas de respuesta y de apoyo
5. Responsabilidad corporativa
6. Formación
7. Educación
8. Sensibilización del público y comunicación
9. Investigación y desarrollo
10. Cooperación global

A la hora de implementarse cada una de estas áreas de acción de la política, se deben tener en cuenta los cuatro principios rectores sobre los derechos del niño mencionados en el capítulo 3:

PRINCIPIOS

- El derecho a la no discriminación
- El interés superior del niño
- El derecho a la vida, a la supervivencia y al desarrollo
- El respeto de las opiniones del niño

Y las otras cinco cuestiones transversales presentadas en la Sección A:

CINCO CUESTIONES

- Riesgo y daño
- Accesibilidad e inclusión
- Cadena de responsabilidad
- Diseño orientado a los niños
- Eficacia

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

> **Los Estados parte deben adoptar medidas legislativas y administrativas para proteger a los niños contra la violencia en el entorno digital, incluidas la revisión periódica, la actualización y la aplicación de marcos legislativos, reglamentarios e institucionales sólidos que protejan a los niños frente a los riesgos reconocidos y emergentes de todas las formas de violencia en el entorno digital.**
>
> Fuente: Observación general núm. 25 (2021), párr. 82[74]

Objetivo:

Identificar un ministerio u organismo que se encargue de establecer un comité directivo nacional de seguridad infantil en Internet y un grupo de expertos interesados para que cubran todas las áreas de la política de seguridad infantil en Internet. Proporcionar los recursos, el liderazgo y la capacidad institucional adecuados para garantizar una acción y cooperación efectivas.

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

1a. Reafirmar el compromiso público con la seguridad de los niños en Internet al más alto nivel
Los dirigentes nacionales, incluidos el primer ministro o el presidente, deben comprometerse a velar por la seguridad de los niños en Internet tanto en el plano nacional como en el internacional.

1b. Designar a un ministerio o a un organismo para que tome la iniciativa en el desarrollo de una política nacional de seguridad infantil en Internet
En el mundo, la responsabilidad en relación a las políticas de seguridad infantil en Internet la ostentan diferentes organismos y ministerios. La elección de un determinado organismo o ministerio puede afectar al desarrollo de las políticas de seguridad infantil en Internet y a cómo se priorizan las distintas cuestiones. Por regla general, la seguridad infantil en Internet suele ser una cuestión que involucra a varios ministerios, pero es importante que exista un organismo concreto que lleve las riendas. En algunos países, las políticas de seguridad infantil en Internet están a cargo del ministerio responsable de las TIC; en otros, el peso recae sobre el ministerio responsable de la infancia y las familias; y en otros la voz cantante la lleva el Ministerio de Justicia. En caso de que haya grupos trabajando en cuestiones relacionadas con la violencia contra los niños (VCN) o la ciberseguridad, pueden ampliarse para incluir a determinados expertos y evitar así trabajar «en una burbuja». *Se puede seleccionar el organismo responsable en función de su autoridad, experiencia, recursos, capacidad o entusiasmo, pero deberá trabajar con otros ministerios y organismos.* Sea cual sea el ministerio que lleve la iniciativa, deberá comprometerse con un enfoque holístico que refleje las necesidades generales de la seguridad infantil en Internet.

1c. Publicar un manual de definiciones y términos
El ministerio responsable deberá publicar una lista completa de definiciones y términos que refleje las definiciones utilizadas en las prácticas recomendadas internacionales.[75] ▶

74. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
75. Véase, por ejemplo, las Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, ECPAT International, 2016.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1d. Crear un comité directivo nacional de seguridad infantil en Internet

El comité directivo nacional de seguridad infantil en Internet se encargará de aplicar y desarrollar políticas y actuará como punto de enlace para la cooperación a nivel nacional y regional. Deberá desarrollar una estrategia para implementar las «Herramientas para la seguridad de niñas, niños y adolescentes en Internet». Esto podría denominarse «plan de acción». El comité se ocupará de un amplio abanico de competencias que abarcan varios ámbitos normativos, entre ellos la educación, la sanidad, la justicia, la protección de los consumidores, la protección de datos, la aplicación de la ley, las TIC y los servicios sociales. Además, supervisará la aplicación y el cumplimiento de las normas. Se exigirá formalmente al comité que coopere con todos aquellos que velen por la seguridad infantil o la ciberseguridad, y deberá mantener un contacto periódico con el ministerio pertinente.

1e. Comprender a las partes interesadas en la seguridad infantil en Internet

Las fuerzas de seguridad, las empresas, las instituciones del sector terciario, las organizaciones de derechos del niño, las instituciones de enseñanza, los padres/cuidadores y los círculos académicos disponen de información valiosa y un interés importante en materia de seguridad infantil en Internet. En algunos contextos, crear un grupo de partes interesadas puede ser útil para ayudar al comité en sus actividades y basar su plan de acción en situaciones reales. En otros contextos, podrían resultar más útiles las conversaciones informales o solicitar los testimonios de una red abierta de partes interesadas. En cualquier caso, el comité directivo nacional de seguridad infantil en Internet debe tratar de entablar relaciones con partes interesadas de relevancia que puedan respaldar sus actividades. Se debe promover la cooperación entre organismos. El objetivo de involucrar a las partes interesadas tiene que ver con la aplicación de las políticas, no con el desarrollo de estas.

1f. Definir las funciones y las responsabilidades de las partes interesadas

Debe existir un marco de trabajo corregulador que defina tanto las funciones y las responsabilidades de todas las organizaciones que desarrollen y gestionen la infraestructura, las redes y los servicios digitales como las obligaciones de los departamentos gubernamentales. Se deben establecer normas básicas para todos en la cadena de valor, incluidos tanto los responsables de la infraestructura, del hardware y de los productos y los servicios digitales como aquellos que los gestionan o los utilizan cuando interactúan con los niños. Estas normas deben centrarse en la seguridad infantil y en hacer efectivos los derechos del niño en el mundo digital. Debe garantizarse la participación en los grupos de interesados de la sociedad civil y la consulta a los niños.

1g. Definir indicadores de rendimiento y evaluación

Cada aspecto del plan de implementación debe tener una autoridad responsable (persona, institución u organismo) y recursos humanos y financieros para completar con éxito la tarea prevista. La misma autoridad puede ser responsable de más de un área de la política o de un único ámbito de especialización. Deben introducirse indicadores clave de rendimiento (KPI), mecanismos de evaluación y estructuras claras de presentación de informes para que el comité directivo pueda supervisar y gestionar los progresos. Ya que el entorno digital evoluciona a gran velocidad, los KPI deberán revisarse constantemente.

1h. Garantizar la integración de la seguridad infantil en Internet en todas las áreas de la política gubernamental

Cualquier plan nacional relevante, como un plan nacional de banda ancha o un marco de trabajo para la cultura digital, debe incluir la política de seguridad infantil en Internet como parte de su estrategia de implementación. Los planes que se desarrollen a lo largo de varios años deberán revisarse cuando se alcancen objetivos importantes.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

Hoja de ruta para hacer efectivas las políticas:

A **Reafirmar el compromiso público con la seguridad de los niños en Internet al más alto nivel**

Los dirigentes nacionales, como el primer ministro, el presidente o los ministros, deberían comprometerse a velar por la seguridad de los niños en Internet tanto en el plano nacional como en el internacional.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente desarrollar un plan plenamente acreditado con un amplio grupo de partidarios y presentarlo a los dirigentes nacionales. Este plan deberá:

1. Exponer los fundamentos con pruebas y datos relevantes; en caso de no haber datos disponibles para su país, utilice datos internacionales.
2. Identificar a los órganos responsables de la toma de decisiones y dirigir los esfuerzos de promoción para establecer su comprensión y sus compromisos.
3. Identificar y colaborar con defensores y expertos (a nivel interno, local e internacional) para respaldar sus argumentos.
4. Analizar el estado de las iniciativas y políticas nacionales que abordan la seguridad de los niños en Internet y otras formas de violencia contra los niños (VCN), las mujeres y las niñas (VCM), y la ciberseguridad.
5. Con base en lo anterior, acordar (en consulta con las partes interesadas clave) cómo redactar una política de seguridad infantil en Internet integral que se incluya en los programas existentes y se base en ellos.
6. Identificar los deberes y obligaciones existentes en consonancia con los marcos de trabajo actuales y otros planes de acción nacionales relevantes y comités intersectoriales (p. ej., VCN, VCM o ciberseguridad).
7. En consulta con las partes interesadas clave, crear un plan de acción: presupuestado, programado y con un organismo a cargo y una persona u organización responsables de cada acción.
8. Presentar su hoja de ruta a los responsables de la toma de decisiones con el máximo apoyo, para obtener su consentimiento y aprobación.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

B **Designar a un ministerio o a un organismo para que tome la iniciativa en el desarrollo de una política nacional de seguridad infantil en Internet**

En el mundo, la responsabilidad en relación a las políticas de seguridad infantil en Internet la ostentan diferentes organismos y ministerios. La elección de un determinado organismo o ministerio puede afectar al desarrollo de las políticas de seguridad infantil en Internet y a cómo se priorizan las distintas cuestiones. Por regla general, la seguridad infantil en Internet suele ser una cuestión que involucra a varios ministerios, pero es importante que exista un organismo concreto que lleve las riendas. En algunos países, las políticas de seguridad infantil en Internet están a cargo del ministerio responsable de las TIC; en otros, el peso recae sobre el ministerio responsable de la infancia y las familias; y en otros la voz cantante la lleva el Ministerio de Justicia. Se puede seleccionar el organismo responsable en función de su autoridad, experiencia, recursos, capacidad o entusiasmo, pero deberá trabajar con otros ministerios y organismos. Sea cual sea el ministerio que lleve la iniciativa, deberá comprometerse con un enfoque holístico que refleje las necesidades generales de la seguridad infantil en Internet.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente utilizar la herramienta FODA. Véase Herramientas de apoyo 1 (pág. 47) para escoger un ministerio u organismo dirigentes.

C **Publicar un manual de definiciones y términos**

El ministerio responsable deberá publicar una lista completa de definiciones y términos que refleje las definiciones utilizadas en las prácticas recomendadas internacionales.[76]

En caso afirmativo, asegúrese de que se corresponden con las definiciones del glosario y las definiciones (pág. 178) para garantizar una buena traducción.

En caso negativo, sería conveniente consultar el glosario y las definiciones (pág. 178) como práctica recomendada para garantizar una buena traducción.

76. Véase, por ejemplo, las Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, ECPAT International, 2016.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

1 Capacidad institucional

D **Comité directivo nacional de seguridad infantil en Internet**

El comité directivo nacional de seguridad infantil en Internet se encargará de desarrollar e implementar políticas y actuará como punto de enlace para la cooperación a nivel regional y nacional. Desarrollará una estrategia para presentar las Herramientas para la seguridad de niñas, niños y adolescentes en Internet. El comité se ocupará de un amplio abanico de competencias que abarcan varios ámbitos normativos, entre ellos la educación, la sanidad, la justicia, la protección de los consumidores, la protección de datos, la aplicación de la ley, las TIC y los servicios sociales. Además, supervisará la aplicación y el cumplimiento de las normas. El comité se comunicará periódicamente con el ministerio responsable.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Evaluar qué ministerios y organizaciones gubernamentales pueden contribuir a la ejecución efectiva de la política de seguridad infantil en Internet y participar en reuniones periódicas.
2. Considerar qué delegados regionales o locales pueden tener un interés en la seguridad infantil en Internet.
3. Involucrar a expertos destacados para garantizar que los planes se consideren prácticas recomendadas y sean adecuados para su propósito.
4. Basarse en las evidencias de las empresas y la sociedad civil.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

E **Dialogar con las partes involucradas en la seguridad infantil en Internet**

Podría ser útil agrupar a las partes interesadas y asignarles la función de apoyar e informar al comité directivo. En ocasiones, podría ser más práctico hablar con las partes interesadas de manera informal o según sea necesario. En cualquier caso, es probable que haya un amplio grupo de «partes interesadas», incluidos padres/cuidadores, docentes y niños, y un grupo más pequeño de personas con competencias y experiencia relevantes, por ejemplo, las fuerzas de seguridad, la industria, los expertos en derechos del niño, las ONG (nacionales e internacionales), los profesionales sanitarios y los círculos académicos. Aprovechar su interés y experiencia puede ser muy beneficioso para promocionar o implementar políticas de seguridad infantil en Internet en múltiples contextos.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Elaborar una lista de partes interesadas, competencias y experiencia, que cubra los ámbitos normativos enumerados en el kit de herramientas. Para obtener indicaciones, consulte la plantilla que adjuntamos como Herramientas de apoyo 2 (pág. 49).
2. Garantizar que incluyan a niños o representantes que trabajen directamente con niños.
3. Si se trata de un grupo formal, establecer mandatos que comprometan claramente al grupo de interesados con las actividades del comité directivo.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

F **Definir roles y responsabilidades**

Debe existir un marco de trabajo corregulador que defina tanto las funciones y las responsabilidades de todas las organizaciones que desarrollen y gestionen la infraestructura, las redes y los servicios digitales como las obligaciones de los departamentos gubernamentales. Se deben establecer normas básicas para todos en la cadena de valor, incluidos tanto los responsables de la infraestructura, del hardware y de los productos y los servicios digitales como aquellos que los gestionan o los utilizan cuando interactúan con los niños. Estas normas deben centrarse en la seguridad infantil y en hacer efectivos los derechos del niño en el mundo digital. Debe garantizarse la participación de la sociedad civil en los grupos de partes interesadas.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Establecer una línea clara de responsabilidad para cada acción del plan.
2. Asignar responsabilidades a las distintas agencias, organismos gubernamentales, reguladores o designados, escuelas, organizaciones benéficas, instituciones sanitarias y empresas para garantizar que todos los aspectos queden cubiertos de forma transparente.

G **Definir indicadores y evaluaciones de rendimiento**

Cada aspecto del plan de implementación debe tener una autoridad responsable (persona, institución u organismo) y recursos humanos y financieros para completar con éxito la tarea prevista. La misma autoridad puede ser responsable de más de un área de la política o de un único ámbito de especialización. Deben introducirse indicadores clave de rendimiento (KPI), mecanismos de evaluación y estructuras claras de presentación de informes para que el comité directivo pueda supervisar y gestionar los progresos. Ya que el entorno digital evoluciona a gran velocidad, los KPI deberán revisarse constantemente.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Establecer KPI y procesos de revisión como parte del plan estratégico. Por ejemplo, los KPI establecidos en la política de protección infantil en Internet de Ruanda.[77]
2. Establecer líneas claras de responsabilidad para el comité directivo.

77. Child Online Protection in Rwanda (Política de protección infantil en Ruanda), 5Rights Foundation, 2019.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

H **Garantizar la integración de la seguridad infantil en Internet en todas las áreas de la política gubernamental**

Cualquier plan nacional relevante, como un plan nacional de banda ancha, un plan de acción nacional para abordar la violencia contra los niños, un marco de trabajo para la cultura digital, una estrategia de ciberseguridad, etc., debe incluir la política de seguridad infantil en Internet como parte de su estrategia de implementación. Los planes que se desarrollan a lo largo de varios años deberán revisarse y actualizarse cuando se alcancen objetivos importantes.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Utilizar la lista de verificación proporcionada en el documento «Herramientas de apoyo 3» para revisar las áreas de la política e identificar si se incluye la seguridad infantil en Internet (pág. 51). Podría ser útil nombrar a un experto externo para que coteje el plan estratégico con las políticas y disposiciones gubernamentales existentes.
2. Presentar cualquier anomalía al comité directivo nacional de seguridad infantil en Internet, creado en el proceso D.

Cómo encaja esto con los documentos fundacionales:

Los gobiernos deberían implementar un marco de trabajo de coordinación a nivel nacional con un mandato claro y autoridad suficiente para coordinar todas las actividades relativas a los derechos del niño, los medios digitales y las TIC a nivel intersectorial, nacional, regional y local. Los gobiernos deben incluir objetivos con plazos determinados y un proceso transparente para evaluar y supervisar los progresos, y deben facilitar los recursos humanos, técnicos y financieros necesarios para garantizar un funcionamiento óptimo de este marco de trabajo.

Los gobiernos deberían establecer una plataforma de múltiples interesados para dirigir el desarrollo, la implementación y el seguimiento de la agenda digital nacional para la infancia. Dicha plataforma debería reunir a representantes de los grupos más importantes, incluidos: niños y jóvenes; asociaciones de padres/cuidadores; sectores relevantes del gobierno; sectores de la educación, la justicia, la salud y la atención social; instituciones nacionales de derechos humanos y los organismos reguladores pertinentes; sociedad civil; industria; círculos académicos y asociaciones de profesionales relevantes.

Fuente: «Directrices sobre la protección de la infancia en línea para los encargados de formular políticas», Unión Internacional de Telecomunicaciones, 2020[78]

78. «Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas», Unión Internacional de Telecomunicaciones, 2020.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

Herramientas de apoyo:

1. Plantilla FODA para identificar el departamento o ministerio responsable más apropiado

El proceso B («Designar a un ministerio u organismo para que tome la iniciativa en el desarrollo de una política nacional de seguridad infantil en Internet») requiere que identifique cuidadosamente el organismo adecuado para que se responsabilice de la seguridad infantil en Internet. Esta herramienta está diseñada para ayudarle en este proceso.

Muchos países han adoptado distintos enfoques para elegir un organismo responsable:

- **Tanzania**: Ministerio de Salud
- **Ghana**: Ministerio de Comunicaciones
- **Etiopía**: autoridad reguladora
- **Australia**: Departamento de Infraestructura, Transporte, Desarrollo Regional y Comunicaciones
- **Reino Unido**: Departamento de Cultura, Medios de Comunicación y Deporte

Para ayudarle a seleccionar el ministerio o departamento adecuados, complete un análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas) de cada ministerio o departamento que esté considerando para identificar cuál ocupa la mejor posición para tomar la iniciativa en materia de seguridad infantil en Internet:

Puntos fuertes	Puntos débiles
Cuestiones importantes: ¿se le dan bien a este ministerio las cuestiones relacionadas con la seguridad en Internet? ¿Algunas de las áreas de acción de la política son ya competencia del ministerio? ¿Tiene los recursos necesarios para asumir responsabilidades de liderazgo? ¿Dispone de la influencia y de los contactos necesarios para hacer un buen trabajo? ¿El personal directivo está dispuesto a asumir las tareas y puede hacerlo?	**Cuestiones importantes:** ¿ha tenido algún problema este ministerio con temas de seguridad en Internet? ¿Carece de la capacidad para asumir más competencias? ¿Carece de la influencia o de las conexiones necesarias para cumplir con estas tareas intersectoriales? ¿Falta liderazgo o el equipo directivo no está interesado en la labor?
Oportunidades	**Amenazas**
Cuestiones importantes: ¿hay algún tipo de sinergia entre las cuestiones de seguridad infantil en Internet y otras políticas emergentes de este ministerio (por ejemplo, banda ancha o implementación de 5G)? ¿El ministerio está compuesto por funcionarios públicos o dirigido por políticos que posiblemente son más efectivos que otros?	**Aspectos importantes:** ¿el rendimiento del ministerio es deficiente? ¿Existe alguna amenaza inminente para el ministerio (por ejemplo, recortes presupuestarios previstos)? ¿Tiene el ministerio algún interés contradictorio que pueda presentar problemas a la hora de tomar el liderazgo (por ejemplo, financiación o acuerdos vigentes en conflicto con proveedores de telecomunicaciones o empresas de tecnología)? ¿Va a haber cambios en el personal directivo?

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

2. Plantilla para identificar a las partes interesadas

Esta plantilla le ayudará a enumerar las partes interesadas necesarias para crear un grupo de interesados, con funciones y responsabilidades relevantes, tal y como exige el proceso E («Comprender a las partes interesadas en la seguridad infantil en Internet»). Los representantes, organizaciones, funciones y responsabilidades dependerán del contacto local, y puede haber varios para cada tipo. Una vez que haya identificado el ministerio u organización responsable, también será importante incluir a las mismas partes interesadas o similares en el proceso para garantizar un equilibrio, eficiencia y resultados óptimos.

Los tipos que se enumeran a continuación reflejan los mencionados en las Directrices sobre la protección de la infancia en línea para los encargados de formular políticas de la UIT (2020) y en la Observación general núm. 25 (2021).

Representante de la parte interesada	Tipo	Organización	Función y responsabilidades
Ejemplo: Persona o representante designado con autoridad adecuada para contribuir/tomar decisiones sobre/ garantizar la asignación de recursos	Niños y jóvenes	Youth Group X	La voz del niño: ofrecer información desde el punto de vista de los niños; subrayar las preocupaciones y preguntas de los niños
	Grupo consultor de jóvenes de 5Rights		La voz del niño: ofrecer información desde el punto de vista de los niños; subrayar las preocupaciones y preguntas de los niños
	Padres, cuidadores, educadores		Garantizar que las políticas favorezcan a los adultos que se encargan de cuidar a otras personas
	Industria		Garantizar que las políticas creen obligaciones para que todos los productos y servicios estén orientados a los niños y sean seguros
	Comunidad de investigadores y ONG		Garantizar que las políticas reflejen las evidencias y conocimientos actuales

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

Representante de la parte interesada	Tipo	Organización	Función y responsabilidades
	Cumplimiento de la ley		Garantizar que las políticas se pueden aplicar y educar a las fuerzas del orden
	Servicios sociales		Garantizar que las políticas tienen en cuenta a los niños más vulnerables
	Servicios sanitarios		Incorporar asesoramiento médico y apoyo a las víctimas de Internet, o apoyo a las personas en situación de riesgo o que han sufrido daños
	Ministerios y organismos reguladores		Implicar a reguladores y ministerios especialistas que no sean el ministerio a cargo
	Operadores de banca ancha, móviles y redes wifi		Ofrecer un acceso digital seguro y asequible a los niños
	Organizaciones de los derechos del niño		Garantizar que las políticas digitales facilitan y cumplen todos los derechos del niño
	Académicos, abogados, particulares y organizaciones especializados en determinados ámbitos (por ejemplo, en derecho, auditorías algorítmicas, prácticas de moderación, etc.)		Ofrecer asesoramiento especializado en función de las necesidades, para garantizar que las políticas estén bien elaboradas pero también sean prácticas

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3. Lista de verificación para identificar qué áreas de la política abordan la seguridad infantil en Internet

Esta lista de verificación le ayudará a revisar las políticas existentes relevantes para establecer si contienen elementos sobre seguridad infantil en Internet. Esto le ayudará a lograr el proceso H («Garantizar la integración de la seguridad infantil en Internet en todas las áreas de la política gubernamental»).

Comunique al grupo de interesados de seguridad infantil en Internet las conclusiones de esta revisión.

Elemento de seguridad infantil en Internet reflejado en la política de seguridad infantil en Internet	Marque la casilla si ya está incluido	En caso negativo, identifique brechas, anomalías y los cambios recomendados, y comuníqueselos al grupo de interesados de seguridad infantil en Internet.
Plan nacional de banda ancha	☐	✎
Marcos de trabajo y hojas de ruta para implementar los Objetivos de Desarrollo Sostenible	☐	
Todos los programas de educación y formación necesarios	☐	
Marcos de trabajo de cultura digital para niños	☐	
Plan de estudios nacional para las escuelas	☐	
Plan de estudios vocacional para docentes y trabajadores sociales	☐	
Plan de estudios vocacional para la polícia y las fuerzas del orden	☐	

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

1 Capacidad institucional

Elemento de seguridad infantil en Internet reflejado en la política de seguridad infantil en Internet	Marque la casilla si ya está incluido	En caso negativo, identifique brechas, anomalías y los cambios recomendados, y comuníqueselos al grupo de interesados de seguridad infantil en Internet.
Derechos de los consumidores	☐	
Violencia contra los niños, estrategia de protección y salvaguardia de la infancia	☐	
Justicia penal	☐	
Derechos humanos	☐	
Derechos del niño	☐	
Igualdad y lucha contra la discriminación	☐	
Protección de datos	☐	
Comercio internacional	☐	
Controles de juegos de azar	☐	

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

1 Capacidad institucional

Elemento de seguridad infantil en Internet reflejado en la política de seguridad infantil en Internet	Marque la casilla si ya está incluido	En caso negativo, identifique brechas, anomalías y los cambios recomendados, y comuníqueselos al grupo de interesados de seguridad infantil en Internet.
Normas de publicidad	☐	
Delitos financieros	☐	
Educación	☐	
Salud	☐	
Cooperación internacional	☐	
Otros	☐	

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

1 Capacidad institucional

Otros recursos de referencia:

1. **El Consejo del Reino Unido para la Seguridad de los Niños en Internet (UKCIS, por sus siglas en inglés) como modelo para un grupo de interesados en la seguridad infantil en Internet**[79]

   El Consejo del Reino Unido para la Seguridad de los Niños en Internet (UKCIS) es un foro colaborativo en el que colaboran el Gobierno, la comunidad tecnológica y el sector terciario. El UKCIS forma parte del Ministerio de Cultura, Medios de Comunicación y Deporte del Reino Unido, el Ministerio de Educación y el Ministerio del Interior. A lo largo del tiempo, el UKCIS ha sido un lugar de encuentro para empresas, círculos académicos, expertos en seguridad infantil, funcionarios públicos y ministros. También ha encargado investigaciones importantes que han proporcionado una base empírica para la elaboración de las políticas. A diferencia de como recomienda el kit de herramientas, el UKCIS no se adhirió formalmente a un plan de acción para un comité directivo.

2. **Guía para la elaboración de una estrategia nacional de ciberseguridad: participación estratégica en la ciberseguridad, UIT**[80]

   Facilitado por la UIT, doce socios de los sectores público y privado, el mundo académico y la sociedad civil comparten sus experiencias y conocimientos proporcionando un conjunto de principios armonizados y agregados para el desarrollo, el establecimiento y la implementación de estrategias de ciberseguridad nacionales. El objetivo de la guía es fomentar el pensamiento estratégico y ayudar a los dirigentes nacionales y responsables de formular políticas a desarrollar, establecer e implementar estrategias nacionales de ciberseguridad en todo el mundo.

3. **Guía sobre los derechos de los niños en el entorno digital para los encargados de formular políticas, Consejo de Europa**[81]

   El objetivo de esta guía es ayudar a los Estados miembros del Consejo de Europa a implementar la Recomendación CM/Rec(2018)7 sobre las Directrices para respetar, proteger y hacer efectivos los derechos del niño en el entorno digital. Este documento incluye las primeras directrices integrales del mundo para los Estados en lo relativo a los derechos del niño en el entorno digital.

4. **Protección infantil en Internet en Ruanda**[82]

   Creada en colaboración entre 5Rights Foundation, la Universidad del Este de Londres, la Universidad de Ruanda y el Gobierno de Ruanda, la Política de protección infantil en Internet ofrece un plan de implementación de alto nivel como ejemplo para cualquier nación que quiera trabajar en el ámbito de la protección infantil en Internet.

79. Consejo del Reino Unido para la Seguridad de los Niños en Internet, Ministerio de Cultura, Medios de Comunicación y Deporte, Ministerio de Educación y Ministerio del Interior, 2021.
80. Guía para la elaboración de una estrategia nacional de ciberseguridad: participación estratégica en la ciberseguridad, Unión Internacional de Telecomunicaciones, 2018.
81. Guía sobre los derechos de los niños en el entorno digital para los encargados de formular políticas, Consejo de Europa, 2020.
82. Child Online Protection in Rwanda (Protección infantil en Internet en Ruanda), 5Rights Foundation, 2019.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

> **Los niños pueden afrontar especiales dificultades para obtener reparación cuando sus derechos han sido vulnerados en el entorno digital por empresas, en particular en el contexto de sus operaciones a escala mundial. Los Estados parte deben considerar la posibilidad de adoptar medidas para respetar, proteger y hacer efectivos los derechos del niño en el contexto de las actividades y operaciones empresariales de carácter extraterritorial, siempre que exista un vínculo razonable entre el Estado y la conducta de que se trate. Deben asegurarse de que las empresas ofrezcan mecanismos de denuncia eficaces; sin embargo, estos mecanismos no deben impedir que los niños tengan acceso a recursos estatales. También deben cerciorarse de que los organismos con competencias de supervisión que sean pertinentes para los derechos del niño, como los relacionados con la salud y la seguridad, la protección de datos y los derechos de los consumidores, la educación, y la publicidad y la comercialización, investiguen las denuncias y ofrezcan recursos adecuados para los casos de violaciones o vulneraciones de los derechos del niño en el entorno digital.**
>
> Fuente: Observación general núm. 25 (2021), párr. 48[83]

Objetivo:

Reforzar y reajustar los marcos normativos jurídicos y reglamentarios nacionales relacionados con la seguridad infantil en Internet, y reforzar la capacidad de los organismos de seguridad y reguladores en el ámbito de la seguridad infantil en Internet, incluida su capacidad para colaborar con otros sectores, en particular el de las TIC.

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

2a. Reforzar y hacer cumplir las leyes que prohíban los delitos relacionados con la seguridad infantil en Internet
Las leyes y los procedimientos penales facilitan la investigación y el enjuiciamiento de los delitos digitales que vulneran el derecho de los niños a la protección. Por lo tanto, deben reforzarse y modificarse en consonancia con las normas internacionales y con las prácticas recomendadas. Esto debería incluir la introducción de evaluaciones de riesgo obligatorias para reducir los posibles daños y la mejora de las sanciones y de los marcos de trabajo en relación a las sentencias, en caso de que sea necesario. También se debe incluir la posibilidad de emplear procedimientos de notificación y de retirada. Las leyes penales relativas a la seguridad infantil en Internet deben elaborarse teniendo en cuenta todos los derechos del niño, incluido su derecho a ser escuchados y a la participación.[84]

2b. Introducir reglamentos de protección de datos y autoridades de supervisión independientes para garantizar que los datos de los niños se tratan de forma apropiada y solo se recopilan cuando es necesario, con altos niveles de seguridad y cuidado
Dichos reglamentos generales deben incluir una categoría especial para los datos de los niños en la que se exija un mayor nivel de protección y de salvaguarda por defecto, así como la protección contra el uso comercial indebido de los datos de los niños. Cuando se solicite el consentimiento de los niños (o de los padres/cuidadores en su nombre) para recopilar y tratar datos de los niños, debe notificarse de forma clara y hacerse con una finalidad legítima. La recopilación de datos con fines de salvaguardia debe ser objetivo de una consideración especial en circunstancias excepcionales cuando se lleve a cabo en favor del interés superior del niño.

83. Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital, CDN, 2021.
84. Por ejemplo, los marcos jurídicos que no dejan claro si las imágenes sexuales autogeneradas que se intercambian de forma consensuada entre niños se considerarán material de explotación sexual de niñas, niños y adolescentes. Incluso aunque en la práctica no se procese a los niños, esta incertidumbre jurídica puede socavar los derechos a la confianza, al control y a la autonomía.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2c. Reforzar la investigación, los procesos y las condenas penales por explotación o abuso sexuales de niños en Internet[85]

Los organismos de justicia penal con competencias en los delitos relacionados con la seguridad infantil en Internet deben recibir formación en materia de seguridad infantil en Internet con el objetivo de fomentar una mayor prevención, un enjuiciamiento eficaz y unas condenas adecuadas, así como para comprender mejor cómo afectan estas situaciones a las víctimas. Las aptitudes de los equipos de investigación y respuesta pertinentes deben revisarse y reforzarse para detectar y prevenir las amenazas de ciberseguridad y reaccionar ante ellas, especialmente en el caso de las relacionadas con la seguridad infantil en Internet. Los sistemas de justicia penal deben poder garantizar un acceso oportuno a la justicia.

2d. Revisar y reforzar los sistemas de justicia de menores

Garantizar que la ley sea clara y proporcionada para reducir todo lo posible el riesgo de que los niños entren en conflicto con la ley en el contexto de la seguridad infantil en Internet. En el caso de que los niños se enfrenten a sanciones penales relacionadas con la seguridad infantil en Internet, por ejemplo, en relación con el acoso cibernético o el abuso sexual basado en imágenes, el sistema judicial deberá hacer todo lo posible para evitar que se criminalice a los niños y proporcionar el apoyo y la representación legal adecuados a aquellos niños que entren en conflicto con la ley para proteger sus derechos.

2e. Identificar y ratificar protocolos internacionales en materia de seguridad infantil en Internet

Para crear un ecosistema sostenible de seguridad infantil en Internet se requiere un enfoque de múltiples partes interesadas y una participación a escala global. Cada país debe identificar y ratificar los protocolos y los tratados internacionales y regionales pertinentes y dar los pasos necesarios para aplicar las diferentes medidas.

2f. Reforzar las capacidades de los organismos de seguridad

Se identificarán las deficiencias en los sistemas policiales y judiciales, y se adoptarán medidas para aumentar la sensibilización, la presentación de denuncias y la persecución de los delincuentes. Siempre que sea posible, se solicitará la formación y el intercambio de conocimientos a nivel internacional, y se fomentará la coordinación y colaboración entre la industria y las fuerzas del orden público.

85. La explotación sexual de niños, niñas y adolescentes (ESIA) se produce cuando se obliga a un niño a participar en actividades sexuales o se le convence para que lo haga. Esto puede implicar actividades con o sin contacto físico y puede darse tanto en el entorno digital como fuera de él.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

Hoja de ruta para hacer efectivas las políticas:

A **Reforzar y hacer cumplir las leyes que prohíban los delitos relacionados con la seguridad infantil en Internet**

Las leyes y los procedimientos penales facilitan la investigación y el enjuiciamiento de los delitos digitales que vulneran el derecho de los niños a la protección. Por lo tanto, deben reforzarse y modificarse en consonancia con las normas internacionales y con las prácticas recomendadas. Esto debería incluir la introducción de evaluaciones de riesgo obligatorias para reducir los posibles daños y la mejora de las sanciones y de los marcos de trabajo en relación a las sentencias, en caso de que sea necesario. También se debe incluir la posibilidad de emplear procedimientos de notificación y de retirada. Las leyes penales relativas a la seguridad infantil en Internet deben elaborarse teniendo en cuenta todos los derechos del niño, incluido su derecho a ser escuchados y a la participación.[86]

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar leyes relevantes. Para obtener indicaciones, consulte la lista de verificación que adjuntamos en «Herramientas de apoyo 1» (pág. 64).
2. Cotejarlas con los estándares internacionales en cada una de las áreas (justicia de menores, etc.).
3. Evaluar los riesgos de las leyes existentes.
4. Encargar análisis de deficiencias a expertos.
5. Proponer enmiendas a las leyes existentes.
6. Planificar esfuerzos de promoción para garantizar que se adopten las enmiendas y que se disponga de los recursos adecuados para su implementación.

86. Por ejemplo, los marcos jurídicos que no dejan claro si las imágenes sexuales autogeneradas que se intercambian de forma consensuada entre niños se considerarán material de explotación sexual de niñas, niños y adolescentes. Incluso aunque en la práctica no se procese a los niños, esta incertidumbre jurídica puede socavar los derechos a la confianza, al control y a la autonomía.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

B **Introducir reglamentos de protección de datos y contar con autoridades de supervisión independientes para garantizar que los datos de los niños se tratan de forma apropiada y que solo se recopilan cuando es necesario, con la máxima seguridad y el mayor de los cuidados.**

Algunas jurisdicciones disponen de normativas generales en materia de protección de datos que quizás deban mejorarse o formalizarse para garantizar que los niños reciben una protección adecuada para su edad. En los casos en los que la protección de datos es escasa o inexistente, puede ser necesario proponer una legislación de protección de datos exclusiva para niños. En ambos casos, los datos de los niños deben considerarse una categoría especial que exija un mayor nivel de protección y salvaguardias por defecto, así como protección contra el uso comercial indebido de lo datos de los niños. Cuando se solicite el consentimiento de los niños (o de los padres/cuidadores en su nombre) para recopilar y tratar datos de los niños, debe notificarse de forma clara y hacerse con una finalidad legítima. La recopilación de datos con fines de salvaguardia debe ser objeto de una consideración especial en circunstancias excepcionales cuando se lleve a cabo en favor del interés superior del niño.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Analizar las deficiencias en los marcos regulatorios existentes en materia de protección de datos.
2. Proponer nuevos reglamentos o enmiendas con recursos y evidencias para respaldarlos.
3. Establecer el cumplimiento o dotar de recursos a las autoridades de supervisión independientes existentes para que lo supervisen y garanticen.
4. Adaptar las normativas de protección de datos para niños a las prácticas internacionales existentes.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

C **Reforzar la investigación, los procesos y las condenas penales por explotación o abuso sexuales de niños en Internet**[87]

Los organismos de justicia penal con competencias en los delitos relacionados con la seguridad infantil en Internet deben recibir formación en materia de seguridad infantil en Internet con el objetivo de fomentar una mayor prevención, un enjuiciamiento eficaz y unas condenas adecuadas, así como para comprender mejor cómo afectan estas situaciones a las víctimas. Las aptitudes de los equipos de investigación y respuesta pertinentes deben revisarse y reforzarse para detectar y prevenir las amenazas de ciberseguridad y reaccionar ante ellas, especialmente en el caso de las relacionadas con la seguridad infantil en Internet. Los sistemas de justicia penal deben poder garantizar un acceso oportuno a la justicia.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Incorporar la seguridad infantil en Internet en el programa (véanse las referencias a la formación del «Área de acción de la política», pág. 144).
2. Revisar las competencias y deficiencias en materia de seguridad infantil en Internet.
3. Analizar los recursos para garantizar el acceso eficaz a la justicia orientada a los niños.

87. La explotación sexual de niños, niñas y adolescentes (ESIA) se produce cuando se obliga a un niño a participar en actividades sexuales o se le convence para que lo haga. Esto puede implicar actividades con o sin contacto físico y puede darse tanto en el entorno digital como fuera de él.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

D **Revisar y reforzar los sistemas de justicia de menores**

Garantizar que la ley sea clara y proporcionada para minimizar el riesgo de que los niños entren en conflicto con la ley en el contexto de la seguridad infantil en Internet. En el caso de que los niños se enfrenten a sanciones penales relacionadas con la seguridad infantil en Internet, por ejemplo, en relación con el acoso cibernético o el abuso sexual basado en imágenes, el sistema judicial deberá hacer todo lo posible para evitar que se criminalice a los niños y proporcionar el apoyo y la representación legal adecuados a aquellos niños que entren en conflicto con la ley para proteger sus derechos.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Revisar y analizar las deficiencias del sistema de justicia de menores.
2. Proponer enmiendas cuando sea necesario.
3. Desarrollar la capacidad de los profesionales clave y plantear estrategias de prevención y sensibilización para reducir los riesgos de criminalización.

E **Identificar y ratificar protocolos internacionales en materia de seguridad infantil en Internet**

Para crear un ecosistema sostenible de seguridad infantil en Internet se requiere un enfoque de múltiples partes interesadas y una participación a escala global. Cada país debe identificar y ratificar los protocolos y los tratados internacionales y regionales pertinentes y dar los pasos necesarios para aplicar las diferentes medidas.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Verificar los recursos en el Anexo D.
2. Enumerar los instrumentos relevantes.
3. Identificar cualquier impedimento para ratificar los protocolos.
4. Redactar propuestas de firma y ratificación.
5. Firmar y ratificar los protocolos.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

F **Reforzar las capacidades de los organismos de seguridad**

Se identificarán las deficiencias en los sistemas policiales y judiciales, y se deberán adoptar medidas para aumentar la sensibilización, la presentación de denuncias y la persecución de los delincuentes. Siempre que sea posible, se solicitará la formación y el intercambio de conocimientos a nivel internacional, y se fomentará la coordinación y colaboración entre la industria y las fuerzas del orden público.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar deficiencias de competencias
2. Identificar módulos de formación (véanse las referencias a la formación del «Área de acción de la política», pág. 144).
3. Identificar posibles socios nacionales e internacionales para el intercambio de competencias (consultar los recursos en materia de cooperación global en el «Área de acción de la política», pág. 161).

Cómo encaja esto con los documentos fundacionales:

> **«La legislación y la reglamentación son instrumentos indispensables para garantizar que las actividades y las operaciones de las empresas no incidan negativamente en los derechos del niño ni los vulneren. Los Estados deben promulgar leyes que den efecto a los derechos del niño por terceras partes y que proporcionen un entorno jurídico y reglamentario claro y previsible que permita que las empresas respeten los derechos del niño».**
>
> Fuente: Observación general núm. 16 (2013) sobre las obligaciones del Estado en relación con el impacto del sector empresarial en los derechos del niño, párr. 53[88]

> **A pesar de la existencia de mecanismos internos de reclamación, los gobiernos deberían establecer mecanismos de supervisión para la investigación y reparación de las infracciones de los derechos del niño, con miras a mejorar la rendición de cuentas de las TIC y otras empresas pertinentes, así como reforzar la responsabilidad de los organismos reguladores en la elaboración de normas relativas a los derechos del niño y las TIC. Esto es especialmente importante porque los demás recursos de los que disponen las personas perjudicadas por las acciones de las empresas —como los procedimientos civiles y otros recursos judiciales— suelen ser engorrosos y costosos.**
>
> Fuente: Directrices sobre la protección de la infancia en línea para los encargados de formular políticas (2020), UIT[89]

88. Observación general núm. 16 (2013) sobre las obligaciones del Estado en relación con el impacto del sector empresarial en los derechos del niño, CDN de las Naciones Unidas, 2013.
89. Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas, Unión Internacional de Telecomunicaciones, 2020.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

Herramientas de apoyo:

1. Lista de verificación legal: un ejemplo

Hemos diseñado esta lista para ayudarle a identificar leyes y políticas relevantes en su jurisdicción para lograr el proceso A: «Reforzar e imponer leyes que prohíban los delitos relacionados con la seguridad infantil en Internet». Incluimos ejemplos del Reino Unido a título indicativo, que deberán sustituirse por ejemplos nacionales o regionales pertinentes.

Área de la política	Ley/reglamento	Estado	¿Incluye la seguridad infantil en Internet?	Regulador/tribunal
Derechos de los consumidores	La Ley de Derechos de los Consumidores de 2015[90] Normativa sobre la seguridad de los juguetes de 2011[91] Normativa sobre la seguridad general de los productos de 2005[92]	Ley Instrumento jurídico Instrumento jurídico	Sí	Tribunal
Protección de la infancia	Ley de Niños y Trabajo Social de 2017[93] Ley de Infancia de 2004[94] Ley de Economía Digital de 2017[95]	Ley Ley Ley	Sí	Tribunal de Familia
Justicia penal	Varios delitos tipificados en la legislación penal	Ley	Sí	Tribunal
Derechos humanos, incluidos los derechos del niño	Ley de Derechos Humanos de 1998[96] Convención sobre los Derechos del Niño de las Naciones Unidas[97] Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital[98]	Ley Tratado Tratado	Sí	Tribunal Comisión de Igualdad y Derechos Humanos (y comisiones nacionales) Presentación de informes al Comité de los Derechos del Niño de las Naciones Unidas Tribunales de las Naciones Unidas

90. Ley de Derechos de los Consumidores de 2015, capítulo 3: contenido digital, Reino Unido; Ley de Derechos de los Consumidores (contenido digital). Asesoramiento para negocios, Ministerio de Negocios, Innovación y Empleo, 2015.
91. Normativa sobre la seguridad de los juguetes de 2011, Oficina de Seguridad y Estándares de Productos, 2011.
92. Normativa sobre la seguridad general de los productos de 2005, Gobierno del Reino Unido, 2017.
93. Ley de Niños y Trabajo Social de 2017, capítulo 2: proteger a los niños, Gobierno del Reino Unido, 2004.
94. Ley de Infancia de 2004, Gobierno del Reino Unido, 2004.
95. Ley de Economía Digital de 2017, Gobierno del Reino Unido, 2017.
96. Ley de Derechos Humanos de 1998, Gobierno del Reino Unido, 1998.
97. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
98. Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital, Comité de los Derechos del Niño de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

Área de la política	Ley/reglamento	Estado	¿Incluye la seguridad infantil en Internet?	Regulador/tribunal
Protección de datos	Código de diseño adecuado a la edad de 2020[99] Ley de Protección de Datos 2018[100]	Ley Ley	Sí	Oficina del Comisario de Información
Comercio internacional	Ley de Comercio de 2021[101] (incorpora una cláusula de protección infantil)	Ley	Sí	Tribunal
Juegos de azar	Ley de Juegos de Apuestas de 2005[102]	Ley	Sí	Comisión de Apuestas
Publicidad	Autoridad de Normas de Publicidad, Código CAP 2010[103] Autoridad de Normas de Publicidad, Código BCAP 2010[104]	Voluntario Voluntario	Sí	Organización de socios corregulada bajo la supervisión de Ofcom
Delitos financieros	Ley de Fraudes de 2006[105] Ley de Robo de 1968[106] Ley de Productos del Delito de 2002[107] Reglamentos sobre el blanqueo de capitales, la financiación del terrorismo y la transferencia de fondos (información del ordenante) 2017[108] Ley de Sanciones y contra el Blanqueo de Capitales de 2018[109]	Ley Ley Ley Ley Ley	No, pero hay un código de conducta voluntario de las compañías de tarjetas de crédito en materia de ESIA y pornografía	Tribunal Tribunal Tribunal Tribunal y Autoridad de Servicios Financieros Tribunal y Autoridad de Servicios Financieros
Educación	Ley de Niños y Trabajo Social de 2017[110] Convención sobre los Derechos del Niño de las Naciones Unidas[111] Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital[112]	Ley Tratado Tratado	Sí	Tribunal, Ofsted Presentación de informes al Comité de los Derechos del Niño de las Naciones Unidas

99. Código de diseño adecuado a la edad de 2020, Gobierno del Reino Unido, 2020.
100. Ley de Protección de Datos de 2018, Gobierno del Reino Unido, 2018.
101. Ley de Comercio de 2021, Gobierno del Reino Unido, 2021.
102. Véase la Ley de Juegos de Apuestas de 2005: parte 1, sección 4 (Juegos de apuestas a distancia) y parte 4 (Protección de niñas, niños y adolescentes) 2005, Gobierno del Reino Unido, 2005.
103. Véase la sección 5 (Niños) del código CAP de publicidad no transmitida de la Autoridad de Normas de Publicidad, Autoridad de Normas de Publicidad, 2010.
104. Véase la sección 5 (Niños) del código CAP de publicidad transmitida de la Autoridad de Normas de Publicidad, Autoridad de Normas de Publicidad, 2010.
105. Ley de Fraudes de 2006, Gobierno del Reino Unido, 2006.
106. Ley de Robo de 1968, Gobierno del Reino Unido, 1968.
107. Ley de Productos del Delito de 2002, Gobierno del Reino Unido, 2002.
108. Reglamentos sobre el blanqueo de capitales, la financiación del terrorismo y la transferencia de fondos (información del ordenante) de 2017, Gobierno del Reino Unido, 2017.
109. Ley de Sanciones y contra el Blanqueo de Capitales de 2018, Gobierno del Reino Unido, 2018.
110. Ley de Niños y Trabajo Social de 2017, Gobierno del Reino Unido, 2017 (especialmente el capítulo 4 sobre relaciones, sexo y habilidades para la vida).
111. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
112. Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital, Comité de los Derechos del Niño de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

Área de la política	Ley/reglamento	Estado	¿Incluye la seguridad infantil en Internet?	Regulador/tribunal
Salud	Ley de Salud y Asistencia Social de 2012[113]	Ley	No	Director médico Tribunal Tribunal de Familia
Cooperación internacional	Objetivos de Desarrollo Sostenible[114]	Acuerdo internacional	No	Tribunal
Igualdad	Ley de Igualdad de 2010[115]	Ley	No	Tribunal Comisión de Igualdad y Derechos Humanos y comisiones nacionales en las naciones descentralizadas

113. Ley de Salud y Asistencia Social de 2012, Gobierno del Reino Unido, 2012.
114. Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible, Naciones Unidas, 2021.
115. Ley de Igualdad de 2010, Gobierno del Reino Unido, 2010.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

2. Una lista de verificación legal en blanco para completar

Hemos diseñado esta lista para ayudarle a identificar leyes y políticas relevantes en su jurisdicción para lograr el proceso A: «Reforzar e imponer leyes que prohíban los delitos relacionados con la seguridad infantil en Internet».

Área de la política	Ley/reglamento	Estado	¿Incluye la seguridad infantil en Internet?	Regulador/tribunal
Derechos de los consumidores				
Protección de la infancia				
Justicia penal				
Derechos humanos, incluidos los derechos del niño				
Protección de datos				
Planes de banda ancha				
Comercio internacional				

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

2 Marcos jurídicos y reguladores

Área de la política	Ley/reglamento	Estado	¿Incluye la seguridad infantil en Internet?	Regulador/tribunal
Juegos de azar				
Publicidad				
Delitos financieros				
Educación				
Salud				
Cooperación internacional				
Igualdad				
Otro(s)				

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

Otros recursos para referencias:

1. Estudio monográfico de los mecanismos de supervisión albaneses[116]

El Consejo Nacional para los Derechos y la Protección del Niño figura en la ley como el comité nacional responsable de la gobernanza y la supervisión, y la protección contra la explotación y los abusos sexuales de los niños en Internet se incluye en las principales políticas y leyes.

2. Ley de Ciberseguridad de Ghana (Ley 1038)[117]

La Ley de Ciberseguridad de Ghana (Ley 1038) contiene disposiciones para la protección infantil en Internet. Las conductas sexuales en línea en las que participan niños están tipificadas como delitos. La ley prohíbe las imágenes y fotografías indecentes de niños, el engaño por parte de pederastas (o «grooming») para la explotación sexual, el acoso cibernético y la extorsión sexual. La ley impone a los proveedores de servicios de telecomunicaciones obligaciones para proteger a los niños en el espacio digital. Se han propuesto nuevas enmiendas a la Ley de la Infancia (Ley 560).

116. Programming for children's protection online in Albania: A Promising Practice (Programación para proteger a los niños en Internet en Albania: una práctica prometedora), UNICEF, 2020.

117. Ley de Ciberseguridad 2020, Gobierno de Ghana, Ministerio de Comunicaciones y Digitalización (Ley 1038), 2020.

«Me gustaría utilizar las tecnologías digitales para mejorar el mundo, algo que no hago ahora. Sin embargo, me gustaría hacerlo, ya que sería algo positivo para todos».

– Alemania, 16

«Participo en conversaciones en línea para debatir cuestiones importantes con los demás».

– Indonesia, 14

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

> **Los Estados parte deben adoptar medidas legislativas, administrativas y de otra índole para garantizar que la privacidad de los niños sea respetada y protegida por todas las organizaciones y en todos los entornos en que se procesen sus datos. La legislación debe incluir salvaguardias sólidas, transparencia, supervisión independiente y acceso a recursos. Los Estados parte deben exigir la integración de la privacidad desde la fase del diseño en los productos y servicios digitales que afectan a los niños. Deben revisar periódicamente la legislación sobre privacidad y protección de datos y asegurarse de que los procedimientos y las prácticas impidan toda infracción deliberada o violación accidental de la privacidad de los niños. Cuando se estime que el cifrado es un medio apropiado, los Estados parte deben considerar la adopción de medidas adecuadas que permitan detectar y denunciar la explotación y los abusos sexuales de niños o el material que muestre abusos sexuales de niños. Estas medidas deben estar estrictamente limitadas con arreglo a los principios de legalidad, necesidad y proporcionalidad.**
>
> Fuente: Observación general núm. 25 (2021), párr. 70[118]

Objetivo:

Reconocer los beneficios y responder a las amenazas actuales y emergentes en materia de privacidad, identidad y representación de los niños en el mundo digital que plantea el uso de datos, incluidos los datos personales, la biometría y la toma de decisiones automatizada.

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

3a. Establecer marcos de trabajo de protección de datos o garantizar que los existentes proporcionen protección específica para los datos de los niños

Los derechos del niño en el entorno digital están estrechamente relacionados con la forma en que se recopilan, almacenan y utilizan sus datos. Las leyes y los reglamentos de protección de datos para los niños deben ser accesibles, eficaces y capaces de adaptarse para abordar los riesgos emergentes.[119] Esto implica no solo establecer marcos jurídicos y reguladores, sino también garantizar que funcionan en la práctica y que se implementan debidamente.

3b. Establecer protocolos y limitaciones para el uso de la toma de decisiones automatizada que pueda afectar a los niños

Las normas, leyes y códigos de prácticas deben garantizar que los niños se beneficien de los sistemas automatizados y no se vean afectados negativamente por la toma de decisiones automatizada.[120] Es particularmente importante evitar el potencial de discriminación a través de la toma de decisiones automatizada. Estos protocolos y limitaciones pueden aplicarse en el contexto de la justicia penal, el bienestar social, la salud, la medicina, la educación y el sector privado, entre otros. ▶

118. Observación general núm. 25 (2021) relativa a los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
119. Reglamento General de Protección de Datos, Unión Europea, 2018.
120. World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert (El mundo va derechito a una distopía liderada por el bienestar digital, advierte un experto en derechos humanos de las Naciones Unidas), Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2019.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

3c. Garantizar las protecciones jurídicas y reglamentarias adecuadas para los datos biométricos de los niños
Los gobiernos y organismos reguladores deben establecer protocolos jurídicos y reglamentarios apropiados y limitaciones para el uso de los datos biométricos de los niños en virtud de los principios de los derechos del niño, la limitación de los fines y los requisitos de la política de seguridad infantil en Internet.

3d. Establecer directrices, leyes y reglamentos claros sobre las prácticas que pueden afectar a la voluntad de los niños
Crear marcos jurídicos que prevengan la segmentación personalizada y el seguimiento de los niños con fines comerciales en función de sus datos personales. Establecer códigos sobre el uso de sistemas de recomendación y otros procesos o tecnologías de toma de decisiones automatizadas que puedan motivar el comportamiento de los niños, alterar sus preferencias y opiniones, socavar la reputación o limitar la experimentación.[121]

3e. Establecer mecanismos efectivos de supervisión y seguimiento
Crear organismos y sistemas que puedan recopilar información relevante sobre la seguridad infantil en Internet, garantizar la transparencia y que las empresas, los gobiernos y otras organizaciones implementen de forma eficaz los derechos y protecciones de los niños.

3f. Establecer marcos para garantizar la transparencia
Un organismo regulador que disponga de los recursos y la experiencia necesarios para comprender los sistemas en la práctica y cómo afectan a los derechos del niño deberá supervisar dichos marcos de trabajo. Dicho organismo regulador deberá, además, tener acceso a investigadores y a expertos independientes.

121. Véase, por ejemplo: YouTube Data Breach Claim (Reclamación por filtración de datos de YouTube), McCann vs Google, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

Hoja de ruta para alcanzar el objetivo:

A **Establecer marcos de trabajo de protección de datos o garantizar que los existentes proporcionen protección específica para los datos de los niños**

Los derechos del niño en el entorno digital están estrechamente relacionados con la manera de recopilar, almacenar y utilizar sus datos. Las leyes y los reglamentos de protección de datos para los niños deben ser accesibles, eficaces y capaces de adaptarse para abordar los riesgos emergentes.[122] Esto implica no solo establecer marcos jurídicos y reguladores, sino también garantizar que funcionan en la práctica.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Véase el Código de diseño adecuado a la edad del Reino Unido[123], que sirve de referencia para la protección de datos de los niños (véase la «Referencia 2» en «Otros recursos»).
2. Utilizar el RGPD[124] como modelo para redactar un reglamento más generalizado o que incluya disposiciones de aplicación y definiciones clave.
3. Valorar la necesidad de códigos especializados o independientes, por ejemplo, códigos para cubrir el uso de los datos en entornos educativos y sanitarios, o datos en poder de organismos gubernamentales.
4. Garantizar que estén cubiertos por su plan, tal y como se ha desarrollado en el área de acción de la política en virtud del marco jurídico y regulatorio. Véase «Herramientas de apoyo» 1 (pág. 80).

122. Reglamento General de Protección de Datos, Unión Europea, 2018.
123. Documento de síntesis del Código de diseño adecuado a la edad de 2020, Oficina del Comisario de Información del Reino Unido, 2020.
124. Reglamento General de Protección de Datos, Unión Europea, 2018.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

B **Establecer protocolos y limitaciones para el uso de la toma de decisiones automatizada que pueda afectar a los niños**

Las normas, leyes y códigos de prácticas deben garantizar que los niños se beneficien de los sistemas automatizados y no se vean penalizados por la toma de decisiones automatizada.[125] Es particularmente importante evitar el potencial de discriminación a través de la toma de decisiones automatizada. Estos protocolos y limitaciones pueden aplicarse en el contexto de la justicia penal, el bienestar social, la salud, la medicina, la educación y el sector privado, entre otros.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente consultar la legislación, los reglamentos y las normas técnicas internacionales más recientes de diseño, auditoría y supervisión de IA en otras jurisdicciones u organizaciones regionales o internacionales (por ejemplo, la Ley de Inteligencia Artificial de la EU[126]) y adaptarlos a su país.

125. World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert (El mundo va derechito a una distopía liderada por el bienestar digital, advierte un experto en derechos humanos de las Naciones Unidas), Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2019.

126. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la unión COM/2021/206, EUR-Lex, 2021; Global Policy AI, Organización para la Cooperación y el Desarrollo Económicos, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

C **Garantizar la protección jurídica y reguladora adecuada para los datos biométricos de los niños**

Los Gobiernos y los organismos reguladores deben establecer protocolos jurídicos y reguladores apropiados y limitaciones para el uso de los datos biométricos de los niños, en virtud de los principios de los derechos del niño, la limitación de los fines y los requisitos de la política de seguridad infantil en Internet.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Comprobar si los datos biométricos están cubiertos por otras leyes o reglamentos nacionales (por ejemplo, la legislación en materia de datos). Es posible que algunas leyes que no mencionan los datos biométricos se interpreten de una forma en la que se incluyan:[127]

   A. En caso de mencionarse, garantizar una mejor protección para los niños.

   B. En caso de no mencionarse, desarrollar una provisión para datos biométricos. Debe abarcar los datos biométricos para los que se ha otorgado consentimiento (por ejemplo, desbloquear un teléfono) y para los que no se ha otorgado o su uso no es obvio (por ejemplo, reconocimiento facial para entrar a la escuela o identificación con huella digital para comer en la escuela).

127. Véase, por ejemplo: Chile: children asked for their biometrics data to obtain food rations in schools (Los niños de Chile deben mostrar sus datos biométricos para comer en la escuela), Privacy International, 2019.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

D **Establecer directrices, leyes y reglamentos claros sobre las prácticas que pueden afectar a la voluntad de los niños**

Crear marcos jurídicos que prevengan la segmentación personalizada y el seguimiento de los niños con fines comerciales en función de sus datos personales. Establecer códigos sobre el uso de sistemas de recomendación y otros procesos o tecnologías de toma de decisiones automatizadas que puedan motivar el comportamiento de los niños, alterar sus preferencias y opiniones, socavar la reputación o limitar la experimentación.[128]

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente verificar los últimos avances en las leyes de datos y si están apareciendo reglamentos en otras jurisdicciones que garanticen el uso equitativo de la elaboración de perfiles o limiten las notificaciones excesivas. Por ejemplo, el Código de diseño adecuado a la edad (Reino Unido),[129] el Reglamento General de Protección de Datos (RGPD, UE)[130] o la Ley de Servicios Digitales (UE)[131] y el Código de publicidad no transmitida, promoción de ventas y marketing directo (Código CAP, Reino Unido).[132]

128. Véase, por ejemplo: YouTube Data Breach Claim (Reclamación por filtración de datos de YouTube), McCann vs Google, 2021.
129. Código de diseño adecuado a la edad, Oficina del Comisario de Información del Reino Unido, 2020.
130. Reglamento General de Protección de Datos, Unión Europea, 2018.
131. Ley de Servicios Digitales: para un entorno online seguro y responsable, Comisión Europea, 2019.
132. Código de publicidad no transmitida, promoción de ventas y marketing directo, Código CAP, Reino Unido.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

E **Establecer mecanismos efectivos de supervisión y seguimiento**

Crear organismos y sistemas que puedan recopilar información relevante sobre la seguridad infantil en Internet, garantizar la transparencia y que las empresas, los gobiernos y otras organizaciones implementen de forma eficaz los derechos y protecciones del niño.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Asegurarse de que haya instituciones u organismos con potestad para recomendar y hacer cumplir las prácticas acordadas. Por ejemplo, las directrices del Centro Nacional para Niños Desaparecidos y Explotados.[133]
2. Aclarar esto en la estrategia desarrollada en el área de acción de la política sobre marcos jurídicos y reguladores con líneas de responsabilidades y supervisión (pág. 56).

133. Nuestro trabajo, Centro Nacional para Niños Desaparecidos y Explotados (NCMEC).

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

F **Establecer marcos de trabajo para garantizar la transparencia**

Un organismo regulador que disponga de los recursos y la experiencia necesarios para comprender los sistemas en la práctica y cómo afectan a los derechos del niño deberá supervisar dichos marcos de trabajo. Dicho organismo regulador deberá, además, tener acceso a investigadores y a expertos independientes.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente garantizar que el organismo regulador esté obligado por ley y disponga de los recursos y las competencias para gestionarlo. Por ejemplo, la Oficina del Comisario de Información (ICO).[134] La ICO es una autoridad independiente del Reino Unido creada para defender los derechos de información en aras del interés público. O la Autoridad Nacional de Protección de Datos (ANPD) que opera bajo la Ley General de Protección de Datos de Brasil.[135]

134. Oficina del Comisario de Información del Reino Unido (ICO).
135. Autoridad Nacional de Protección de Datos (ANPD), Gobierno Federal de Brasil.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

Cómo encaja esto con los documentos fundacionales:

La adopción de salvaguardias en materia de identidad digital es un factor clave para los Gobiernos y las Naciones Unidas en su afán de aprovechar plenamente su utilidad y potencial al tiempo que se fomenta la confianza en su uso. Esa labor comprende, por ejemplo, iniciativas como la descentralización del almacenamiento de datos, la identificación y la certificación, las comunicaciones cifradas y la incorporación de los principios de «privacidad desde el diseño».

Fuente: Hoja de ruta del secretario general de las Naciones Unidas para la cooperación digital, junio de 2020[136]

Cuando se solicite el consentimiento para procesar los datos de un niño, los Estados parte deben cerciorarse de que el niño o, según su edad y el grado de evolución de sus facultades, el padre o el cuidador, den su consentimiento informado, libre y previo al procesamiento de esos datos. Cuando el propio consentimiento del niño se considere insuficiente y se requiera el consentimiento de los padres para procesar los datos personales del niño, los Estados parte deben exigir que las organizaciones que procesan esos datos verifiquen que el consentimiento es informado, consecuente y dado por el padre o cuidador del niño.

Fuente: Observación general núm. 25 (2021), párr. 71[137]

Los Estados parte deben garantizar que los niños y sus padres o cuidadores puedan acceder fácilmente a los datos almacenados, rectificar los que sean inexactos u obsoletos y eliminar los datos almacenados de forma ilegal o innecesaria por autoridades públicas, particulares u otras entidades, con sujeción a limitaciones razonables y legales. Deben garantizar asimismo el derecho de los niños a retirar su consentimiento y a oponerse al procesamiento de datos personales cuando la persona encargada de procesarlos no demuestre que existen motivos legítimos e imperiosos para ello. Además, deben proporcionar información a los niños, padres y cuidadores sobre estas cuestiones, en un lenguaje adaptado a los niños y en formatos accesibles.

Fuente: Observación general núm. 25 (2021), párr. 72[138]

136. Hoja de ruta del secretario general de las Naciones Unidas para la cooperación digital, Naciones Unidas, junio de 2020.
137. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
138. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

El proceso A («Establecer marcos de trabajo de protección de datos o garantizar que los existentes proporcionen protección específica para los datos de los niños») requiere garantizar que todos los aspectos de los datos de los niños estén protegidos adecuadamente en las leyes y los reglamentos. Esta herramienta está diseñada para ayudar a los responsables de formular las políticas a considerar todas y cada una de las cuestiones que un marco de trabajo de protección de datos debe abordar para los niños.

Herramientas de apoyo:

1. Lista de verificación para garantizar una legislación integral de protección de datos para los niños

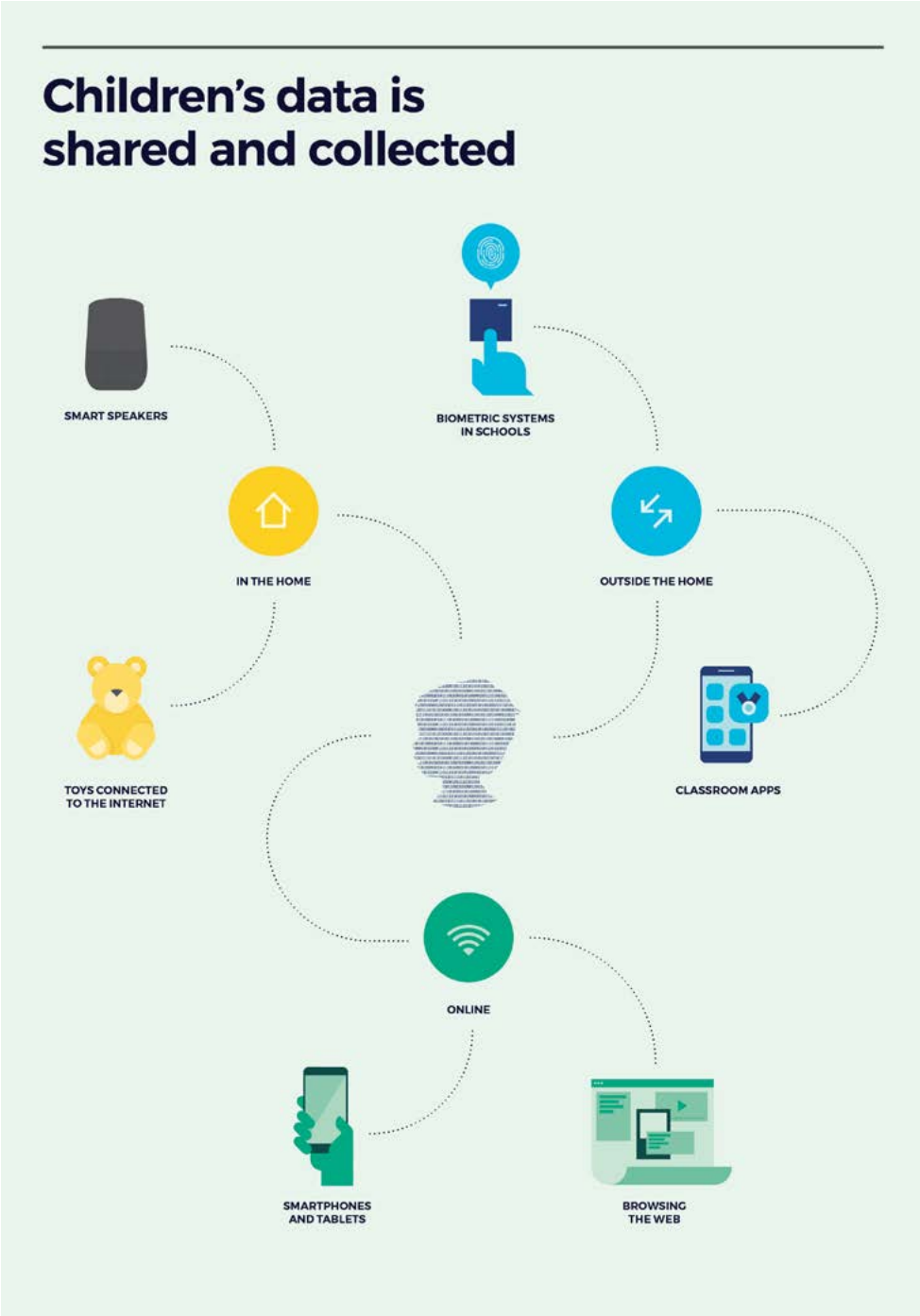
¿Dispone de marcos de trabajo de protección de datos que cubran los siguientes ámbitos?	
Recopilación	
Almacenamiento	
Uso	
Datos educativos	
Datos sanitarios	
Datos gubernamentales y administrativos	
Datos utilizados para la toma de decisiones automatizada	
Datos utilizados en otros sistemas de IA	
Datos biométricos	

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

Otros recursos de referencia:

1. Elementos visuales para comprender mejor la magnitud de los datos recopilados de los niños



Fuente: 'Who knows what about me' Infographic (Infografía «Quién sabe qué sobre mí»), Children's Commissioner[139]

139. Who knows what about me? (Quién sabe qué sobre mí), Children's Commissioner, 2018.

3 Datos personales, identidad y autonomía

Fuente: 'Who knows what about me' Infographic (Infografía «Quién sabe qué sobre mí»), Children's Commissioner[140]

2. Estudio monográfico del Código de diseño adecuado a la edad del Reino Unido[141]

El Reino Unido ha implementado una legislación innovadora que aborda la forma en que se pueden utilizar los datos de los niños: el *Código de diseño adecuado a la edad*.

> **«Este diseño aborda cómo diseñar sistemas de seguridad para la protección de datos en los servicios en línea para garantizar que sean apropiados para los niños y que cumplan con sus necesidades de desarrollo. Refleja la creciente preocupación por el lugar que ocupan los niños en la sociedad y, en concreto, en el mundo digital moderno. Existe un consenso a nivel internacional y, específicamente, en el Reino Unido, sobre la necesidad de trabajar para crear un espacio en línea seguro en el que los niños puedan aprender, explorar y divertirse. Este código logra lo anterior protegiendo a los niños en el mundo digital, no alejándolos de él».**

El código establece 15 normas de diseño adecuado a la edad que reflejan un enfoque basado en el riesgo. La atención se centra en proporcionar entornos predeterminados que garanticen que los niños puedan disfrutar del mejor acceso posible a los servicios en línea, minimizando por defecto la recopilación y el uso de datos. Los principios son:

1. El mejor interés del niño
2. Evaluaciones de impacto en la protección de datos
3. Aplicación adecuada a la edad
4. Transparencia
5. Uso perjudicial de los datos
6. Políticas y normas comunitarias
7. Ajustes por defecto
8. Minimización de los datos
9. Cesión de datos
10. Geolocalización
11. Controles parentales
12. Elaboración de perfiles
13. Técnicas «nudge»
14. Juguetes y dispositivos conectados
15. Herramientas en línea

140. Who knows what about me? (Quién sabe qué sobre mí), Children's Commissioner, 2018.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

El Código de diseño adecuado a la edad entró en vigor en Reino Unido el 2 de septiembre de 2021. Se basa principalmente en el Reglamento General de Protección de Datos (RGPD) de la UE y, por lo tanto, es probable que su contenido resulte familiar a aquellos países que cumplen con el RGPD. Se considera en general como el programa de protección de datos de los niños más avanzado del mundo. Desde su implementación, los servicios han ido anunciando un conjunto de cambios en su forma de interactuar con los niños, como los siguientes:

- En Instagram, los adultos no pueden enviar mensajes directos a menores de 18 años que no los sigan.
- SafeSearch de Google se activará de forma predeterminada para todos los menores de 18 años.
- En YouTube, la reproducción automática está desactivada para los menores de 18 años y los recordatorios para hacer pausas e ir a dormir están activados de forma predeterminada.
- Los niños menores de 16 años no pueden ofrecer retransmisiones en directo en TikTok y las notificaciones push están desactivadas a partir de las 21:00.
- Google y Facebook detendrán la publicidad conductual dirigida a los niños.

Algunos sectores o tipos específicos de información pueden estar sujetos a disposiciones adicionales, por ejemplo, los datos sanitarios, financieros y educativos. Estas pueden ser otras áreas que requieren códigos adicionales o complementos, pero todas deben cumplir con un alto nivel de privacidad y respetar el interés superior del niño.

3. Manifesto for the Better Governance of Children's Data (Manifiesto de UNICEF para una mejor gobernanza de los datos de los niños), UNICEF[142]

El grupo de trabajo de UNICEF sobre gobernanza de datos ha elaborado un informe que documenta las razones y los principios para una mejor gobernanza de los datos de los niños. Los diez puntos de acción del manifiesto se centran en utilizar los datos en el mejor interés de los niños, colaborando con los niños para entender los usos prácticos y reduciendo las brecha de conocimientos entre la tecnología y los organismos y personas que los utilizan.

4. Marco de privacidad de la OCDE[143]

El marco de privacidad de la OCDE reúne los componentes clave del marco de privacidad de la OCDE, basado en sus directrices de privacidad:

PRINCIPIOS BÁSICOS DE APLICACIÓN NACIONAL:

Principio de limitación de la recopilación
Debe haber límites para la recopilación de datos personales y dichos datos deben obtenerse por medios legales y justos y, en su caso, con el conocimiento o consentimiento de la persona interesada.

Principio de calidad de los datos
Los datos personales deben ser relevantes para los fines para los que se van a utilizar y en la medida necesaria para dichos fines. Deben ser exactos, completos y estar actualizados.

141. Código de diseño adecuado a la edad, Oficina del Comisario de Información del Reino Unido, 2020.
142. The Case for Better Governance of Children's Data: A Manifesto (Manifiesto para una mejor gobernanza de los datos de los niños), Oficina de Política y Perspectiva Global de UNICEF, 2021.
143. Recomendación del Consejo relativa a las Directrices que regulan la protección de la privacidad y flujos transfronterizos de datos personales. Organización para la Cooperación y el Desarrollo Económicos, 2013

Principio de especificación del propósito
Deben especificarse los fines para los que se recopilan los datos personales a más tardar en el momento de la recopilación de los datos y su uso posterior debe limitarse al cumplimiento de estos fines o de otros que no sean incompatibles con dichos fines y que se especifiquen en cada ocasión en que cambien los fines.

Principio de limitación del uso
Los datos personales no deben divulgarse, facilitarse o utilizarse de otro modo para fines distintos de los especificados de conformidad con el párrafo 9, excepto: a) con el consentimiento de la persona interesada; o b) si lo exige la ley.

Principio de salvaguardias de seguridad
Los datos personales deben protegerse mediante salvaguardias de seguridad razonables contra riesgos tales como la pérdida de acceso o el acceso no autorizado, la destrucción, el uso, la modificación o la divulgación de datos.

Principio de transparencia
Debe existir una política general de transparencia sobre los desarrollos, las prácticas y las políticas en materia de datos personales. Debe haber medios disponibles de inmediato para establecer la existencia y la naturaleza de los datos personales y los principales fines de su uso, así como la identidad y la residencia habitual del responsable del tratamiento.

Principio de participación individual
Las personas deben tener derecho a:

a) Recibir la confirmación del responsable del tratamiento, o de otro modo, de si dispone o no de datos relativos a su persona.

b) Que se les comuniquen los datos relacionados con su persona:

   i. en un plazo razonable;

   ii. por un precio, si lo hubiera, que no sea excesivo;

   iii. de manera razonable; y

   iv. en una forma que se puedan entender fácilmente.

c) Recibir información sobre por qué se ha rechazado una solicitud formulada en virtud de los apartados (a) y (b), y a poder impugnar dicha denegación; y a

d) Impugnar los datos relativos a su persona y, si la impugnación tiene éxito, solicitar que los datos se borren, rectifiquen, completen o modifiquen.

Principio de responsabilidad
El responsable del tratamiento se encargará de cumplir las medidas para hacer efectivos los principios expuestos anteriormente.

Principios básicos de aplicación internacional: libre circulación y restricciones legítimas

- El responsable del tratamiento seguirá siendo responsable de los datos personales bajo su control independientemente de la ubicación de los datos.
- Un Estado miembro debe abstenerse de restringir la circulación transfonteriza de los datos personales entre sí y otro país si (a) el otro país cumple en gran medida estas directrices o (b) existen salvaguardias suficientes, incluidos mecanismos eficaces de aplicación y medidas adecuadas establecidas por el responsable del tratamiento, para garantizar un nivel continuo de protección acorde con estas directrices.
- Cualquier restricción a la circulación transfronteriza de datos personales debe ser proporcional a los riesgos existentes, teniendo en cuenta la sensibilidad de los datos y la finalidad y el contexto del tratamiento.

5. **Reglamento General de Protección de Datos de la Unión Europea (texto y herramientas)**[144]
El Reglamento General de Protección de Datos (RGPD) es una ley de privacidad y seguridad autorizada por la Unión Europea. Exige que las empresas que operan dentro y fuera de los países europeos utilicen los datos personales de los ciudadanos de la UE de conformidad con la ley.

6. **La Estrategia Digital Europea (incluidas las propuestas sobre inteligencia artificial y datos)**[145]
Una guía muy útil para entender cómo perfila la Unión Europa su futuro digital. El objetivo de la Estrategia Digital Europea es desarrollar un mercado único para que todas las empresas compitan en igualdad de condiciones sin infringir los derechos de privacidad de los consumidores, y perfilar una mejor sociedad digital tanto a nivel regional como internacional.

7. **Fundamentos de la Autoridad de Protección de Datos de Irlanda para un enfoque de tratamiento de datos orientado a los niños (los Fundamentos)**[146]
Redactados por la Comisión de Protección de Datos de Irlanda (DPC, por sus siglas en inglés), los Fundamentos tienen como objetivo mejorar los estándares del tratamiento de datos. Sirven como guía para las organizaciones involucradas en el tratamiento de datos de los niños y sus principios se basan en el RGPD.

8. **Memo on Artificial Intelligence and Children's Rights (Memorando de UNICEF sobre la inteligencia artificial y los derechos del niño) de UNICEF**[147]
Este memorando de UNICEF describe los elementos clave sobre cómo influye la IA en los derechos del niño en distintos ámbitos, como en la popular plataforma de streaming YouTube, los juguetes inteligentes y la IA en la educación. También formula recomendaciones iniciales para los responsables de la formulación de políticas, las grandes empresas, los padres y los educadores.

9. **Informe de la Agencia de los Derechos Fundamentales de la UE, Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights (Bajo vigilancia: biometría, sistemas informáticos de la UE y derechos fundamentales)**[148]
Los sistemas de tecnología de la información (TI) establecidos por la UE desempeñan un papel vital en la seguridad regional, como en la gestión de la migración y la lucha contra el terrorismo y los delitos graves. Sin embargo, aún no se han estudiado los efectos de los sistemas en los derechos fundamentales. Por ejemplo, con el marco de trabajo establecido en el artículo 24 de la Convención sobre los Derechos del Niño de la OHCHR, el informe del capítulo 7 hace hincapié en que los sistemas deben dar prioridad al interés superior del niño al recopilar identificadores biométricos.

144. Reglamento General de Protección de Datos, Unión Europea, 2018.
145. Shaping Europe's digital future (Perfilando el futuro digital de Europa), Unión Europea, 2020.
146. Fundamentos para un enfoque de procesamiento de datos orientado a los niños, Autoridad de Protección de Datos de Irlanda, 2020.
147. Artificial Intelligence and Children's Rights (Inteligencia artificial y derechos del niño), Fondo de las Naciones Unidas para la Infancia, 2019.
148. Under watchful eyes: biometrics, EU IT systems and fundamental rights (Bajo vigilancia: biometría, sistemas informáticos de la UE y derechos fundamentales), Agencia de los Derechos Fundamentales de la Unión Europea, 2018.

3 Datos personales, identidad y autonomía

10. Orientación de UNICEF sobre la IA y los niños[149]

Si bien muchos países han implementado de forma generalizada los sistemas de IA, las preocupaciones sobre esta nueva tecnología también han llevado a los gobiernos, las empresas y la sociedad civil a desarrollar principios para potenciarlos por medio de la ética. Aunque los derechos humanos se han incluido en estas estrategias de IA, los derechos del niño en particular aún no se han abordado en la medida necesaria. Con esta orientación, el objetivo de UNICEF es crear conciencia sobre los derechos del niño y formular recomendaciones para las distintas partes —principalmente responsables de la formulación de políticas y dirigentes empresariales— sobre políticas y prácticas de IA relacionadas con los niños.

Asistentes de voz y chatbots con IA

Los asistentes de voz virtuales y chatbots utilizan PLN (procesamiento de lenguaje natural), reconocimiento automático de voz y aprendizaje automático para reconocer comandos verbales, identificar patrones, obtener información y generar respuestas. Si bien estos sistemas no siempre se han creado o adaptado para los niños, son sistemas que tienen una influencia emocional o conductual en millones de niños. Los partidarios de estas tecnologías han citado sus ventajas, que incluyen el apoyo a los niños con problemas visuales o movilidad limitada, y nuevas formas de aprender y despertar la curiosidad y la creatividad de los niños. Además, algunos chatbots ayudan a los niños a estudiar y a gestionar su tiempo de forma más eficaz.

Sin embargo, el uso de chatbots puede conllevar riesgos adicionales para los niños, especialmente en el ámbito de la salud mental, cuando estos bots no reconocen las peticiones de ayuda u ofrecen consejos inadecuados. Por ejemplo, una prueba que la BBC realizó en 2018 con dos chatbots de salud mental reveló que las aplicaciones no gestionaron adecuadamente las denuncias de abuso sexual de los niños, a pesar de que ambas se habían considerado aptas para niños. Según un informe de UNICEF, «cuando no se diseñan cuidadosamente, los chatbots pueden agravar el sufrimiento en lugar de aplacarlo», lo que resulta «particularmente peligroso para los usuarios más jóvenes que pueden no tener la fortaleza emocional para lidiar con una experiencia negativa o confusa con un chatbot». Además, los chatbots pueden plantear distintas amenazas de seguridad, incluidos la suplantación de identidad (hacerse pasar por otra persona), la manipulación de datos, el robo de datos y la vulnerabilidad a los ciberataques, y pueden imponer prejuicios, dado que a menudo seleccionan una respuesta predeterminada en función de las palabras clave o patrones de redacción más similares.

La privacidad y la propiedad de los datos son otras cuestiones preocupantes relativas a las tecnologías de chatbot y asistentes personales. Por ejemplo, dado que los asistentes de voz suelen almacenar grabaciones de voz para que el sistema aprenda de forma continua, los defensores de los derechos del niño han planteado cuestiones sobre la falta de transparencia en las políticas de retención de datos de las empresas y el consentimiento de los niños y de los padres.

Reconocimiento facial para la identificación biométrica

Los sistemas de reconocimiento facial emplean técnicas de visión computerizada y algoritmos de aprendizaje automático para determinar, procesar y analizar los rasgos faciales de una persona con una amplia gama de objetivos, como verificar la identidad de la persona con los registros existentes. Puede utilizarse con fines de identificación en controles de fronteras, para analizar y prevenir delitos y a modo de vigilancia escolar porque —supuestamente— mejora la seguridad. El reconocimiento facial se utiliza cada vez más como «credencial» digital para la identificación legal y funcional. Aunque no sustituye a la identificación legal, que hace que un Estado pueda reconocer a las personas y es un derecho reconocido, esta tecnología puede validar de forma más rápida o sencilla un registro de identidad existente.

149. Policy guidance on AI for children (Orientación normativa sobre IA para niños), Fondo de las Naciones Unidas para la Infancia, 2020.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3 Datos personales, identidad y autonomía

Los riesgos y limitaciones asociados a los derechos humanos y de los niños son altos. Los defensores de la privacidad ya han advertido del uso que realmente se le está dando como herramienta de investigación para las fuerzas del orden en iniciativas de vigilancia masiva del gobierno, especialmente porque se puede utilizar para perfilar, rastrear y reprimir comunidades vulnerables. En algunos casos, estos sistemas también plantean problemas de consentimiento significativo, ya que las personas pueden no saber quién está recopilando los datos biométricos o incluso si se están recopilando, cómo se están almacenando o cómo podrían aplicarse. Además, sigue habiendo imprecisiones en la detección del reconocimiento facial. En concreto, la coincidencia es menos fiable en los rostros de los niños y en otros grupos basados en el género y la etnicidad, como las mujeres de color. Como consecuencia, esto podría arraigar aún más los prejuicios sociales existentes y provocar la discriminación o una mayor marginalización de las comunidades minoritarias.

Fuente: Policy guidance on AI for children (Orientación normativa sobre IA para niños), Fondo de las Naciones Unidas para la Infancia, 2020[150]

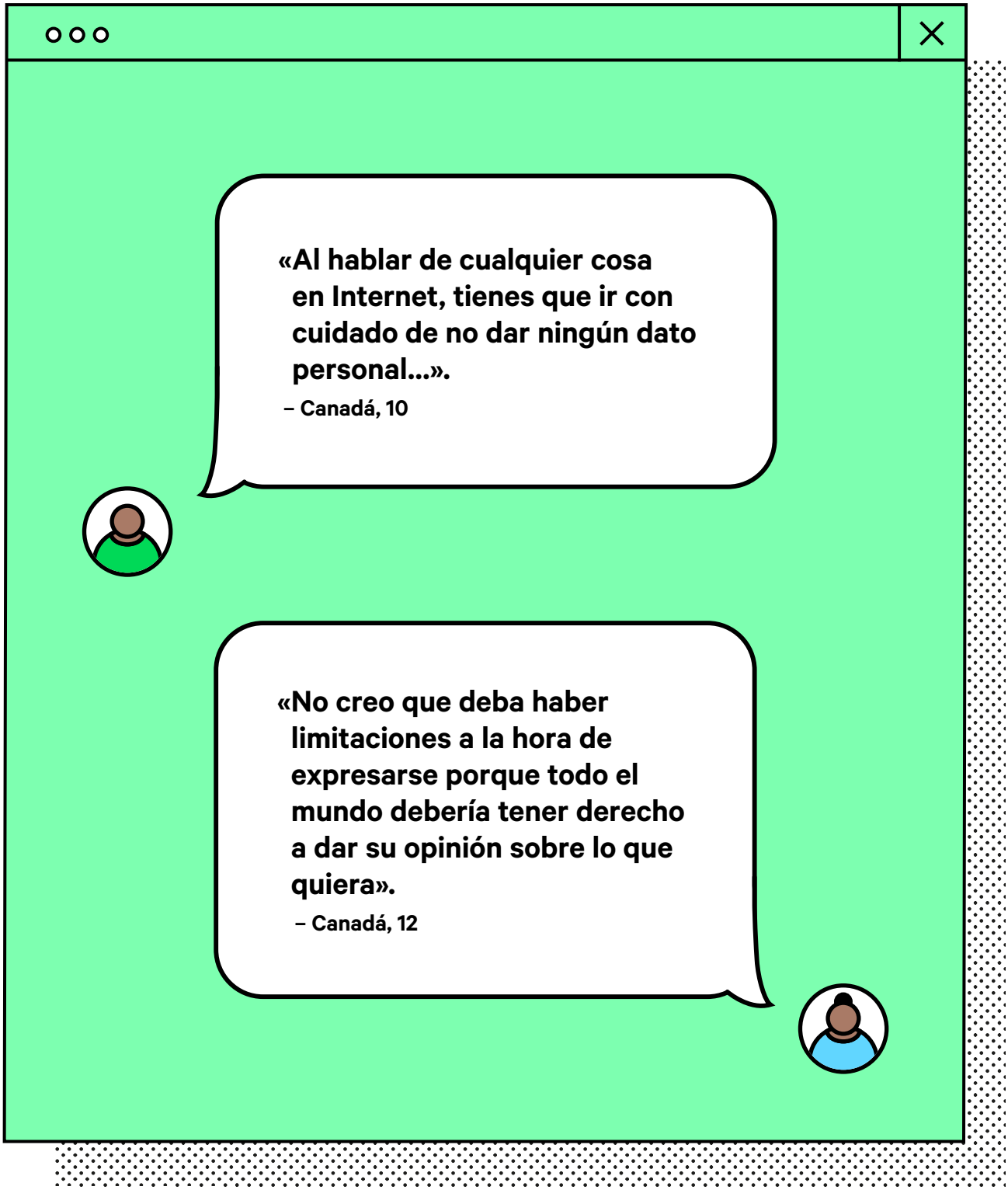
1. **Recursos adicionales del Código del niño**[151]
   En este sitio web pueden consultarse todos los recursos adicionales de la Oficina del Comisario de Información del Reino Unido sobre el Código de diseño adecuado a la edad, incluidas las Preguntas frecuentes y una Plantilla de evaluación del impacto de la protección de datos.

2. **5Rights Foundation's Demystifying the Age Appropriate Design Code (Descodificando el Código de diseño adecuado a la edad)**[152]
   Folleto para niños sobre el desarrollo del Código de diseño adecuado a la edad del Reino Unido.

150. Policy guidance on AI for children (Orientación normativa sobre IA para niños), Fondo de las Naciones Unidas para la Infancia, 2020.
151. Recursos adicionales del Código del niño, ICO 2021.
152. Demystifying the Age Appropriate Design Code (Descodificando el Código de diseño adecuado a la edad), 5Rights Foundation, 2020.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >



< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

Los Estados parte deben proporcionar a los niños información adaptada a sus necesidades y a su edad en un lenguaje apropiado para ellos sobre sus derechos y sobre los mecanismos de información y denuncia, los servicios y los recursos de que disponen en caso de violación o vulneración de sus derechos en relación con el entorno digital. Esta información también debe proporcionarse a los padres, cuidadores y profesionales que trabajan con los niños y en favor de estos.

Fuente: Observación general núm. 25 (2021), párr. 49[153]

Modelo de respuesta nacional (competencia 4): prácticas recomendadas de aplicación de la ley

En aquellos países que actualmente no dispongan de una competencia específica para aplicar la ley en el ámbito de la explotación sexual de niñas, niños y adolescentes, el organismo de seguridad nacional debe identificar esta necesidad y comprometerse a desarrollar dicha competencia.

A los países que ya dispongan de una competencia específica para aplicar la ley en dicho ámbito pero que aún necesiten desarrollar un enfoque de múltiples partes interesadas, les beneficiaría incorporar profesionales especializados en protección infantil e investigadores. Al planificar y llevar a cabo una investigación en el ámbito de la explotación sexual infantil, se deben seguir en todo momento los principios de protección de la infancia para la aplicación de la ley. De esta forma, se dará prioridad en todo momento a las necesidades y los derechos del niño. El enfoque de múltiples partes interesadas reforzará la protección y el apoyo a las víctimas y ayudará a recabar las mejores pruebas de la víctima, lo que a su vez contribuirá a un enjuiciamiento exitoso. También recomendamos que se compartan las prácticas recomendadas en toda la región.

Fuente: Modelo de respuesta nacional de la Alianza Mundial WeProtect[154]

Objetivo:

Establecer un marco de trabajo coordinado de múltiples partes interesadas para abordar los riesgos de los niños en Internet, en particular la explotación sexual de niñas, niños y adolescentes (ESIA): incluidos mecanismos jurídicos y reglamentarios para una ejecución eficaz, prevención, recursos y acceso a asesoramiento experto en materia de seguridad infantil en Internet.

153. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
154. La explotación sexual de niños, niñas y adolescentes (ESIA) se produce cuando se obliga a un niño a participar en actividades sexuales o se le convence para que lo haga. Esto puede implicar actividades con o sin contacto físico y puede darse tanto en el entorno digital como fuera de él.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

4a. Notificación y retirada
Los organismos gubernamentales colaborarán con expertos, las fuerzas el orden y la industria para establecer y supervisar protocolos eficaces de notificación y retirada de contenido ilegal y pernicioso. Entre otras cosas, será necesario diseñar protocolos (y las leyes correspondientes) que garanticen que los proveedores locales de servicios de Internet restrinjan el acceso a los sitios o a las plataformas que no retiren el contenido respecto al que se les ha notificado o que infrinjan sistemáticamente las leyes u otros requisitos legales en materia de seguridad infantil en Internet.

4b. Establecer procesos para la gestión de riesgos en relación a los delincuentes y a la explotación sexual infantil
Debería establecerse un proceso eficaz de múltiples partes interesadas para la gestión de los infractores, basado en normas internacionales de prácticas recomendadas. Se formará a las fuerzas policiales y a otros profesionales de justicia penal para que reconozcan e investiguen los comportamientos delictivos. La gestión del riesgo de los infractores es un componente esencial de la seguridad infantil en Internet, ya que una persona o un grupo de infractores pueden llegar a un gran número de víctimas infantiles a través de Internet.

4c. Proporcionar recursos adecuados para el apoyo psicosocial de las víctimas principales y secundarias y sus familias
Las organizaciones que forman a los profesionales de los ámbitos de la salud mental, la psicología y el trabajo social que trabajan con niños vulnerables deben tener un conocimiento básico de las cuestiones de seguridad infantil en Internet.[155] La seguridad infantil en Internet debe integrarse en sistemas de seguridad y protección de los niños más generalizados, como la protección en las escuelas o la violencia contra los niños (VCN).

4d. Establecer marcos de trabajo para la identificación y la protección de las víctimas
Un objetivo primordial en la prevención de los perjuicios en Internet será evaluar las necesidades de los niños vulnerables y la mejor manera de ayudarlos. Los centros de atención integral actúan como coordinadores para las víctimas de explotación y proporcionan acceso a un amplio abanico de servicios esenciales, desde la asistencia médica hasta el asesoramiento jurídico, todo desde un mismo lugar. Ofrecen un marco de trabajo para los procedimientos de salvaguarda y protección infantil, proporcionan apoyo a las víctimas y transmiten rápidamente las denuncias de delitos en Internet a las autoridades pertinentes.[156]

4e. Garantizar que los marcos de trabajo pertinentes no criminalicen a los niños
Es importante establecer marcos de trabajo adecuados para tratar con niños que puedan encontrarse en conflicto con la ley en el contexto de la seguridad infantil en Internet (por ejemplo, en casos de ciberacoso, divulgación de información maliciosa o «hackeo»). Siempre que sea posible, debe apartarse a los niños del sistema de justicia penal y barajar la posibilidad del asesoramiento o de la justicia restauradora. Sobre todo, es fundamental garantizar que se entienden todas las circunstancias del niño. Por ejemplo, la forma de actuar de un niño puede ser producto del acoso escolar, del engaño por parte de pederastas (o «grooming») u de otra forma de coacción.

155. What Works to Prevent Violence Against Women and Girls Evidence Reviews Paper 3: Response mechanisms to prevent violence (Medidas eficaces para prevenir la violencia contra las mujeres y las niñas. Revisiones de evidencias. Artículo 3: mecanismos de respuesta para prevenir la violencia), What Works, 2015. pág. 28.
156. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prevenir y abordar la explotación sexual de niñas, niños y adolescentes (ESIA): modelo de respuesta nacional), Alianza Mundial WeProtect, 2016.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

Hoja de ruta para alcanzar el objetivo:

A **Notificación y retirada**

Los organismos gubernamentales deberían colaborar con expertos, las fuerzas el orden y la industria para establecer y supervisar protocolos eficaces de notificación y retirada de contenido ilegal y pernicioso. Entre otras cosas, será necesario diseñar protocolos (y las leyes correspondientes) que garanticen que los proveedores locales de servicios de Internet restrinjan el acceso a los sitios o a las plataformas que no retiren el contenido respecto al que se les ha notificado o que infrinjan sistemáticamente las leyes u otros requisitos legales en materia de seguridad infantil en Internet.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Desarrollar e implementar planes para abordar las brechas en la provisión. Véase «Herramientas de apoyo» 1 (pág. 97).
2. Analizar los documentos fundacionales proporcionados en «Documentos clave y otros recursos», particularmente el Modelo de respuesta nacional,[157] a modo de orientación (véase «Referencia 1» en «Otros recursos»).

157. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Evitar y abordar la explotación sexual de niños, niñas y adolescentes (ESIA), Alianza Global WeProtect, 2016.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

B **Establecer procesos para la gestión de riesgos en relación a los delincuentes y a la explotación sexual infantil**

Debería establecerse un proceso eficaz de múltiples partes interesadas para la gestión de los infractores, basado en normas internacionales de prácticas recomendadas. Se formará a las fuerzas policiales y a otros profesionales de justicia penal para que reconozcan e investiguen los comportamientos delictivos. La gestión del riesgo de los infractores es un componente esencial de la seguridad infantil en Internet, ya que una persona o un grupo de infractores pueden llegar a un gran número de víctimas infantiles en Internet.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Reunir la experiencia disponible para crear una gran base de conocimientos, por ejemplo, la Agencia Nacional contra el Crimen[158] y Europol.[159]
2. En caso de ser necesario, contactar con expertos internacionales o regionales para obtener asesoramiento, como el Centro Nacional de Niños Desaparecidos y Explotados,[160] la Internet Watch Foundation,[161] la INTERPOL[162] y ECPAT.[163]

158. Acerca de nosotros, Agencia Nacional contra el Crimen.
159. Acerca de Europol, Europol.
160. Nuestro trabajo, Centro Nacional para Niños Desaparecidos y Explotados.
161. Acerca de nosotros, Internet Watch Foundation (IWF).
162. Quiénes somos, INTERPOL.
163. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminología universal: orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales), ECPAT International, 2016.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

C **Proporcionar recursos adecuados para el apoyo psicosocial de las víctimas principales y secundarias y sus familias**

Las organizaciones que forman a los profesionales de los ámbitos de la salud mental, la psicología y el trabajo social que trabajan con niños vulnerables deben tener un conocimiento básico de las cuestiones de seguridad infantil en Internet.[164] La seguridad infantil en Internet debería integrarse en sistemas de seguridad y protección de los niños más generalizados.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Establecer un desarrollo de competencias a largo plazo en el ámbito de la explotación sexual, como parte de su plan continuo. Véase «Herramientas de apoyo 1» en la sección «Área de acción de la política» de «Formación» para recibir ayuda con el fin de identificar las necesidades de formación para aumentar la capacidad (pág. 119).
2. En caso de ser necesario, contactar con expertos internacionales o regionales para obtener asesoramiento, como el Centro Nacional de Niños Desaparecidos y Explotados, [165] la Internet Watch Foundation,[166] la INTERPOL[167] y ECPAT.[168]

164. La explotación sexual de niños, niñas y adolescentes (ESIA) se produce cuando se obliga o convence a un niño a participar en actividades sexuales. Esto puede implicar actividades con o sin contacto físico y puede ocurrir tanto en el entorno digital como fuera de él.
165. Nuestro trabajo. Centro Nacional para Niños Desaparecidos y Explotados.
166. Acerca de nosotros. Internet Watch Foundation (IWF).
167. Quiénes somos. INTERPOL.
168. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminología universal: orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales). ECPAT International, 2016.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

D **Establecer marcos de trabajo para la identificación y la protección de las víctimas**

Un objetivo primordial en la prevención de los perjuicios en Internet será evaluar las necesidades de los niños vulnerables y la mejor manera de ayudarlos. Se reforzarán la competencias de los centros de atención integral para garantizar que siguen procedimientos de protección infantil, proporcionan apoyo a las víctimas y transmiten rápidamente las denuncias de delitos en Internet a las autoridades relevantes.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Analizar los centros de atención integral existentes (como el Modelo de respuesta nacional[169] en «Referencia 1» de «Otros recursos»). Por ejemplo, la Policía de Escocia.[170]
2. En caso de ser necesario, buscar expertos internacionales o regionales para reunir la red de competencias necesarias, como el Centro Nacional de Niños Desaparecidos y Explotados,[171] la Internet Watch Foundation,[172] la INTERPOL[173] y ECPAT.[174]

169. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Prevenir y abordar la explotación sexual de niñas, niños y adolescentes (ESIA): modelo de respuesta nacional), WeProtect, 2016.
170. Internet Safety (Seguridad en Internet), Policía de Escocia.
171. Nuestro trabajo, Centro Nacional para Niños Desaparecidos y Explotados (NCMEC).
172. Acerca de nosotros, Internet Watch Foundation (IWF).
173. Quiénes somos, INTERPOL.
174. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, ECPAT International), ECPAT International, 2016.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

E **Garantizar que los marcos de trabajo pertinentes no criminalicen a los niños**

Es importante establecer marcos de trabajo adecuados para tratar con niños que puedan encontrarse en conflicto con la ley en el contexto de la seguridad infantil en Internet (por ejemplo, en casos de ciberacoso, divulgación de información maliciosa o «hackeo»). Siempre que sea posible, los niños deben apartarse del sistema de justicia penal y se debe dar preferencia a oportunidades de asesoramiento o justicia restaurativa. Sobre todo, es fundamental garantizar que se entienden todas las circunstancias del niño. La forma de actuar de un niño puede ser producto del acoso escolar, el engaño por parte de pederastas (o «grooming») u otra forma de coacción.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Involucrar a su Ministerio de Justicia para la formulación de las leyes existentes.
2. Consultar a las principales partes interesadas, incluidos los niños, los jóvenes y los padres/cuidadores, para modificar o actualizar las normas y las orientaciones normativas cuando sea necesario.
3. Recabar la experiencia de los derechos del niño para garantizar que se pueda rehabilitar y proteger a los menores, en lugar de castigarlos (excepto en los casos más graves).

Cómo encaja esto con los documentos fundacionales:

En aquellos países que actualmente no dispongan de una competencia específica para aplicar la ley en el ámbito de la explotación sexual de niñas, niños y adolescentes, el organismo de seguridad nacional debería identificar esta necesidad y comprometerse a desarrollar dicha competencia: esto incluye la identificación de funcionarios específicos que permanecerán en el puesto durante un período minimo (recomendamos un mínimo de 2 años); la asignación de un lugar apropiado para acomodar dichos recursos; la adquisición de equipamiento esencial; la provisión de formación y técnicas especializadas en materia de explotación sexual de niñas, niños y adolescentes; el apoyo a la salud mental y al bienestar para funcionarios; y el desarrollo y la impartición de formación que ayude a sensibilizar sobre la explotación sexual infantil para las fuerzas de orden público de todo el país. A los países que ya dispongan de una competencia específica para aplicar la ley en dicho ámbito pero que aún necesiten desarrollar un enfoque de múltiples partes interesadas, les beneficiaría incorporar profesionales especializados en protección infantil e investigadores. Al planificar y llevar a cabo una investigación en el ámbito de la explotación sexual infantil, se deben seguir en todo momento los principios de protección de la infancia para la aplicación de la ley. De esta forma, se dará prioridad en todo momento a las necesidades y los derechos del niño. El enfoque de múltiples partes interesadas reforzará la protección y el apoyo a las víctimas y ayudará a recabar las mejores pruebas de la víctima, lo que a su vez contribuirá a un enjuiciamiento exitoso. También recomendamos que se compartan las prácticas recomendadas en toda la región.

Fuente: Modelo de respuesta nacional de la Alianza Mundial WeProtect[175]

175. Prevenir y abordar la explotación sexual de niñas, niños y adolescentes (ESIA): modelo de respuesta nacional, Alianza Mundial WeProtect, 2016.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

Herramientas de apoyo:

1. Lista de verificación para desarrollar procedimientos adecuados de notificación y retirada

El proceso A («Notificación y retirada») comienza identificando las brechas en los sistemas de notificación y retirada. Esta lista de verificación está diseñada para ayudar a los responsables de la formulación de políticas a identificar los pasos y requisitos necesarios para garantizar que el contenido ilegal y pernicioso pueda eliminarse rápidamente una vez identificado.

	Definición jurídica de contenido ilegal articulada	**Requisitos jurídicos para eliminar el contenido ilegal articulados**	**Proceso rápido para eliminar el contenido ilegal requerido («notificaciones de retirada»)**	**Definición jurídica de contenido dañino pero no ilegal articulada**	**Requisitos jurídicos para eliminar el contenido dañino articulados**	**Proceso rápido para eliminar el contenido dañino requerido («notificaciones de retirada»)**
Proveedores de servicios de Internet						
Plataformas de redes sociales						
Plataformas de streaming						
Nube y otros servicios de alojamiento						
Otro(s)						

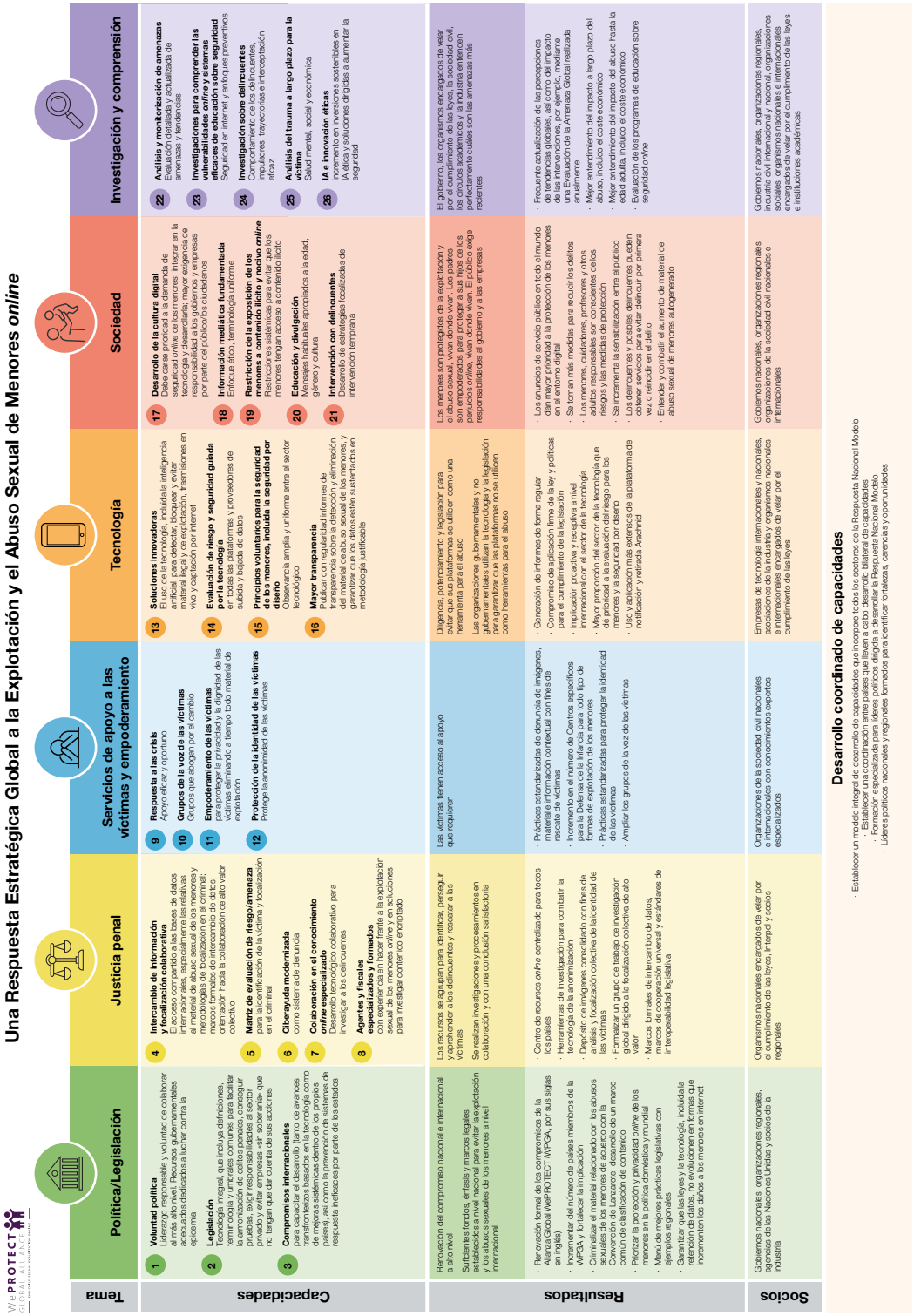
< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

4 Sistemas de respuesta y de apoyo

Otros recursos de referencia:

1. Ejemplos de trabajo del Modelo de respuesta nacional de la Alianza Mundial WeProtect[176]



176. Ejemplos de trabajo de competencias e implementación del Modelo de respuesta nacional de la Alianza Mundial, WeProtect, 2018.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

2. Proyecto de ley de Australia de Seguridad en Internet[177]

La Ley de Seguridad en Internet de Australia incluye:

- Actualizaciones sobre leyes australianas anteriores que funcionan bien (específicamente, la *Ley de Mejora de la Seguridad en línea 2015* y su esquema de explotación sexual basado en imágenes).
- Un conjunto de expectativas básicas de seguridad en Internet para los servicios de redes sociales, los servicios electrónicos relevantes y los servicios de Internet designados, que indique claramente las expectativas de la comunidad y describa los requisitos obligatorios para la presentación de informes.
- Un plan optimizado de ciberacoso para que los niños australianos disfruten de una amplia gama de servicios en línea, no solo de plataformas de redes sociales.
- Un nuevo esquema de ciberacoso para adultos australianos, para facilitar la eliminación de contenido abusivo y hostil en Internet.
- Un sistema modernizado de contenido en Internet que sustituirá a los programa de los Anexos 5 y 7 de la Ley de Servicios de Radiodifusión de 1992 (BSA). El proyecto de ley creará nuevas clases de contenido dañino en Internet y reavivará los códigos obsoletos de la industria para abordar dicho contenido.
- Nuevos acuerdos para bloquear material detestable/violento que permite al Comisario de Seguridad Electrónica responder rápidamente a un evento crítico en Internet, como los atentados terroristas de Christchurch, solicitando a los proveedores de servicios de Internet que bloqueen el acceso a sitios que incluyan contenido gravemente perjudicial.
- Requisitos de retirada consistentes para el acoso sexual basado en imágenes, el ciberabuso, el ciberacoso y el contenido dañino en Internet, que exijan a los proveedores de servicios de Internet eliminar dicho material en un plazo de 24 horas tras recibir una notificación del Comisario de Seguridad Electrónica.

3. Herramientas de EndOCSEA@Europe[178]

EndOCSEA se concibió para garantizar la protección de los derechos de los niños mediante una cooperación multinacional, interdisciplinaria e intersectorial eficaz y medidas favorables para los niños para prevenir y combatir la explotación sexual infantil facilitadas por las TIC (OCSEA) a nivel paneuropeo.

El proyecto incluye tres componentes que se refuerzan entre sí, cada uno de ellos con el objetivo de:

- Crear entornos propicios para la colaboración intersectorial y multidisciplinaria a nivel nacional y regional, reforzando las estructuras nacionales de gobernanza y llevando a cabo análisis de situación de riesgos y respuestas de OCSEA en contextos nacionales y paneuropeos.
- Apoyar las reformas legislativas y procesales, la formación y la mejora de las competencias de los agentes de la ley, el poder judicial y los fiscales, y promover la cooperación interinstitucional multidisciplinaria para el apoyo integral a las víctimas.
- Abordar las competencias de la sociedad, haciendo hincapié en la sensibilización, la educación de los grupos objetivo clave y el empoderamiento de los niños.

177. Consulta sobre un proyecto de ley para una nueva Ley de Seguridad en Internet, Ministerio de Infraestructura, Transporte, Desarrollo Regional y Comunicaciones, 2020.
178. Poner Fin a la Violencia contra los Niños en Internet, Consejo de Europa, 2020.

4. **Convenio sobre delitos cibernéticos del Consejo de Europa (Convenio de Budapest)**[179]
   El convenio es un tratado de la UE sobre delitos cometidos a través de Internet y de otras redes informáticas que trata en particular de las infracciones de los derechos de autor, el fraude informático, el material de explotación sexual de niñas, niños y adolescentes y las infracciones de seguridad de las redes. También incluye una serie de facultades y procedimientos, como la búsqueda de redes informatizadas y la intercepción.

5. **Directrices de la línea de asistencia de INHOPE**[180]
   La misión de INHOPE es apoyar la red de líneas de asistencia que combaten el material de explotación sexual de niñas, niños y adolescentes (MESNNA) en Internet. INHOPE se compone de múltiples líneas de asistencia por todo el mundo, que operan en todos los Estados miembros de la UE, Rusia, Sudáfrica, América del Norte y del Sur, Asia, Australia y Nueva Zelanda. INHOPE apoya a las líneas de asistencia y a sus organizaciones asociadas a través de la formación, las prácticas recomendadas, el control de calidad y el bienestar de los empleados.

6. **Recursos de notificación y retirada de UNICEF y GSMA**[181]
   Se trata de una guía para proveedores de servicios de Internet sobre las políticas y procedimientos de notificación y retirada, con el fin de evitar el uso indebido de sus servicios para compartir material de explotación sexual de niñas, niños y adolescentes.

7. **Servicio de prevención del suicidio R;pple**[182]
   El servicio de prevención del suicidio R;pple es una herramienta de supervisión en línea diseñada para mostrar una página visual en el dispositivo de un usuario tan pronto como se identifique que está buscando una palabra clave o frase dañina que figure en la configuración de la herramienta de monitorización de R;pple. Dichas palabras clave y frases incluyen palabras o términos que están relacionados con contenido potencialmente dañino en Internet.

8. **Estudio monográfico del enfoque de Albania para apoyar a los supervivientes**[183]
   El concepto de soporte integral está bien establecido en este estudio monográfico. Se pone en marcha de inmediato un proceso de asesoramiento psicosocial para los niños que denuncian la presencia de violencia en Internet a la Línea Nacional de Ayuda a la Infancia de Albania, ALO 116 111, y existe un procedimiento para comunicar la denuncia a las autoridades pertinentes. En 2019, todos los niños que presentaron una denuncia y lo solicitaron se derivaron a los organismos pertinentes. En el marco de la importante inversión en el desarrollo de competencias de los trabajadores sociales, se ha introducido un programa revisado para el trabajo social, en el que la denuncia y la respuesta a la violencia infantil en Internet se integran en el programa de formación continua de la Escuela de Administración Pública de Albania.

9. **Plan de Acción Nacional de Camboya para Prevenir y Responder a la Explotación Sexual Infantil en Internet 2021-2025**[184]
   Plan elaborado por el Grupo de Trabajo Técnico contra la Explotación Sexual Infantil en Internet, integrado por 11 ministerios gubernamentales, UNICEF y varias ONG. Este plan de acción reconoce el nexo entre la explotación sexual infantil y el acoso dentro y fuera del entorno digital y se engloba en el marco de trabajo del Plan de Acción para Prevenir y Responder a la Violencia contra los Niños 2017-2021, así como la próxima ronda que comenzará en 2022.

179. Convenio de Budapest, Consejo de Europa, 2021.
180. Nuestra historia, INHOPE, 2021.
181. Políticas y prácticas de empresas para eliminar el material de explotación sexual de niñas, niños y adolescentes de Internet, Fondo de las Naciones Unidas para la Infancia y GSMA, 2016.
182. Servicio de prevención del suicidio R;pple, R;pple, 2021.
183. Programming for children's protection online in Albania: A Promising Practice (Programación para proteger a los niños en Internet en Albania: una práctica prometedora), Fondo de las Naciones Unidas para la Infancia, 2020.
184. Lanzamiento oficial del Plan de Acción Nacional de Camboya para Prevenir y Responder a la Explotación Sexual Infantil en Internet 2021-2025.

10. Internet Watch Foundation (IWF)[185]
La IWF busca, detiene, elimina y previene las imágenes de explotación sexual infantil en Internet. Utiliza sus datos únicos y de confianza para investigar las nuevas tendencias, tácticas y métodos que emplean los autores de delitos en Internet. Canalizan esa experiencia para desarrollar servicios de vanguardia con el objetivo de ayudar a la comunidad tecnológica a prevenir, interrumpir y eliminar imágenes de explotación sexual infantil en Internet a nivel internacional.

11. Unidad de Delitos contra Menores de la INTERPOL[186]
La INTERPOL trabaja para abordar los delitos de alcance internacional contra los niños. Para ayudar a localizar a los niños desaparecidos, emiten notificaciones amarillas, mientras que sus expertos en trata de personas colaboran con los países miembros para rescatar a los niños víctimas de la trata y el trabajo forzoso. La unidad también bloquea el acceso a material de explotación sexual de niñas, niños y adolescentes.

185. Acerca de nosotros, Internet Watch Foundation.
186. Quiénes somos, INTERPOL.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

«Sí, mis padres me apoyan para que exprese mi opinión en Internet de forma respetuosa y con los pies en el suelo».

– Líbano, 16

«Poder expresarme en Internet es una parte importante de tener una identidad».

– Nueva Zelanda, 17

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5 Responsabilidad corporativa

El sector empresarial, incluidas las organizaciones sin fines de lucro, incide en los derechos del niño, tanto directa como indirectamente, al prestar servicios y ofrecer productos relacionados con el entorno digital. Las empresas deben respetar los derechos del niño e impedir y reparar toda vulneración de sus derechos en relación con el entorno digital. Los Estados parte tienen la obligación de garantizar que las empresas cumplen esas obligaciones.

Los Estados parte deben adoptar medidas mediante, entre otras cosas, la elaboración, vigilancia, aplicación y evaluación de leyes, reglamentos y políticas, para cerciorarse de que las empresas cumplan sus obligaciones consistentes en impedir que sus redes o servicios en línea se utilicen de forma que causen o propicien violaciones o vulneraciones de los derechos del niño, incluidos sus derechos a la privacidad y a la protección, así como en facilitar recursos rápidos y eficaces a los niños, padres y cuidadores. Deben también alentar a las empresas a proporcionar información pública y asesoramiento accesible y oportuno para apoyar la participación de los niños en actividades digitales seguras y provechosas.

Los Estados parte tienen la obligación de proteger a los niños frente a cualquier conculcación de sus derechos por parte de empresas comerciales, lo que incluye al derecho a gozar de protección contra todas las formas de violencia en el entorno digital. Aunque las empresas no estén directamente involucradas en la comisión de actos perjudiciales, pueden causar o propiciar violaciones del derecho de los niños a vivir libres de violencia, por ejemplo como resultado del diseño y el funcionamiento de sus servicios digitales. Los Estados parte deben promulgar, supervisar y hacer cumplir leyes y reglamentos destinados a prevenir las violaciones del derecho a la protección contra la violencia, así como leyes y reglamentos destinados a investigar, juzgar y reparar las violaciones que se produzcan en relación con el entorno digital.

Los Estados parte deben exigir al sector empresarial que actúe con la debida diligencia en relación con los derechos de los niños. En concreto, deben realizar evaluaciones de los efectos sobre los derechos de los niños y hacerlas públicas, con especial atención a los efectos diferenciados, y a veces graves, del entorno digital en los niños. Deben dar los pasos pertinentes para prevenir, vigilar, investigar y castigar los abusos respecto a los derechos de los niños por parte de las empresas.

Además de elaborar leyes y políticas, los Estados parte deben exigir a todas las empresas cuya labor pudiera afectar a los derechos de los niños en relación con el entorno digital que apliquen marcos de trabajo, códigos industriales y términos de servicio que cumplan con las normas más estrictas de ética, privacidad y seguridad en relación con el diseño, la ingeniería, el desarrollo, el funcionamiento, la distribución y la comercialización de sus productos y sus servicios. Esto incluye a las empresas cuyo público objetivo o cuyos usuarios finales son sobre todo niños o que realicen actividades que pudieran afectar de una forma u otra a niños. Deben exigir a dichas empresas que mantengan unos niveles altos de transparencia y de rendición de cuentas y alentarlas a que adopten medidas innovadoras que antepongan el interés superior del niño. También deben exigir que se faciliten a los niños, o a los padres o cuidadores de los niños muy pequeños, versiones de sus términos de servicio adaptadas a las edades de los niños.

Fuente: Observación general núm. 25 (2021), párrs. 35-39[187]

187. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5 Responsabilidad corporativa

Objetivo:

Promover los diseños centrados en niños, niñas y adolescentes, unas normas básicas, los acuerdos de la industria, la adopción de prácticas recomendadas y la conciencia cultural y el suministro de recursos para la seguridad infantil en Internet a través de las regulaciones y de los marcos de trabajo relacionados con la responsabilidad corporativa.

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

5a. Implementar la seguridad, los derechos y la ética desde el diseño

Deben elaborarse normas y códigos de prácticas que exijan que los diseñadores de productos, los fabricantes y los proveedores de servicios protejan los derechos de los niños y contribuyan a la seguridad infantil en Internet. Los términos y las condiciones deben reflejar el interés superior del niño. Entre otras cosas, las normas y los códigos de prácticas tendrán por objeto evitar que se ofrezca a los niños contenidos o contactos dañinos o inapropiados; proteger la privacidad de los niños en Internet, a nivel de sistemas o dispositivos; y abordar las preocupaciones de seguridad planteadas por el «internet de las cosas» (juguetes y servicios conectados con una función de transmisión de flujo continuo) para garantizar que las empresas privadas hayan tenido en cuenta, a partir de una evaluación de impacto infantil, un proceso de mitigación y prevención de riesgos de cara a ofrecer a los niños un servicio apropiado para su edad.

5b. Introducir normas básicas[188]

La industria tiene la responsabilidad de garantizar que los niños estén protegidos en Internet. Esto implica la creación de un espacio en Internet seguro y accesible para los niños. No se trata solo de impedir su acceso a contenidos dañinos. Se exigirá a las empresas que expongan qué procedimientos y qué consideraciones especiales han adoptado para garantizar la seguridad de los niños y el respeto de sus derechos, en el marco 4C de la gestión de riesgos[189], a medida que desarrollen y establezcan sus servicios en Internet.[190] El ministerio o el organismo pertinentes deben crear un código bajo la supervisión del Comité Directivo. Estas normas serán obligatorias y se exigirá su cumplimiento.

5c. Aplicación de la clasificación por edades

La aplicación de una clasificación coherente y por edades para los contenidos comerciales, los medios de comunicación de servicio público y los juegos y las actividades en Internet propicia un enfoque transparente y eficaz de la gestión de aquellos contenidos y servicios que afectan a los niños. Esto puede ser necesario para artículos y servicios a los que se les deba aplicar dicha clasificación y para los contenidos que estén pensados para diferentes rangos de edad. Se requerirá la verificación de la edad o la creación de espacios solo para adultos si se trata de contenidos prohibidos o de actividades que no sean adecuadas para niños. Para esto, quizá se deban proporcionar filtros de contenido que bloqueen los contenidos no deseados.[191]

5d. Introducir sistemas de moderación y de presentación de informes

Se requerirán mecanismos para identificar los contenidos perturbadores o inadecuados de los proveedores de servicios. Además, deben establecerse sistemas de supervisión transparentes y sólidos para todos los servicios de Internet, incluida implantación de mecanismos de retirada de contenidos. Habrá una línea directa pública y gratuita para ofrecer tanto información como ayuda o asesoramiento por parte de expertos. Los niños deben poder acceder con facilidad a los mecanismos de denuncia de contenidos. Los sistemas para señalar la existencia de contenidos inadecuados deben considerarse una herramienta adicional. ▶

188. Véase, por ejemplo, «Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse», GOV.UK, 2020.
189. Véase la sección sobre «Mitigación de riesgos y daños».
190. Derechos de los niños en evaluaciones de impacto, Fondo de las Naciones Unidas para la Infancia, 2013.
191. But how do they know it is a child? (Pero, ¿cómo saben que es un niño?), 5Rights Foundation, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5 Responsabilidad corporativa

5e. Garantizar la protección de los niños contra la presión comercial
Las medidas destinadas a proteger a los niños de la presión comercial incluirán: fomentar diseños apropiados para su edad, inhabilitar la publicidad dirigida y el intercambio con terceros y concienciar sobre el contexto en el que los niños crecen. Los productos y los servicios que pongan énfasis en los derechos y la seguridad infantil en Internet podrán contar con un certificado. Asimismo, se podrá actuar contra los desarrolladores de productos y de servicios que violen dichos valores.

5f. Garantizar que se apliquen los principios del diseño centrado en niñas, niños y adolescentes para minimizar los posibles riesgos para la seguridad infantil en Internet
Esto incluye, por ejemplo, la posibilidad de que adultos desconocidos puedan entrar en contacto con los niños, la publicidad dirigida sobre juegos de azar o la recomendación de contenidos dañinos. La seguridad infantil en Internet debe integrarse en la fase de diseño para evitar que surjan problemas más adelante.

Hoja de ruta para alcanzar el objetivo:

A **Implementar la seguridad, los derechos y la ética desde el diseño**

Se elaborarán normas y códigos de prácticas que exijan que los diseñadores de productos, los fabricantes y los proveedores de servicios protejan los derechos de los niños y contribuyan a la seguridad infantil en Internet. Los términos y las condiciones deben reflejar el interés superior del niño. Entre otras cosas, las normas y los códigos de prácticas tendrán por objeto evitar que se ofrezca a los niños contenidos o contactos dañinos o inapropiados; proteger la privacidad de los niños en Internet, a nivel de sistemas o dispositivos; y abordar las preocupaciones de seguridad planteadas por el «internet de las cosas» (juguetes y servicios conectados con una función de transmisión de flujo continuo) para garantizar que las empresas privadas hayan tenido en cuenta, a partir de una evaluación de impacto infantil, un proceso de mitigación y prevención de riesgos de cara a ofrecer a los niños un servicio apropiado para su edad.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar las oportunidades regulatorias o legales de albergar un código de conducta para la seguridad por diseño.
2. Identificar una autoridad u organismo regulador con los recursos y la experiencia suficientes para fomentar el cumplimiento de las normas o, en caso de ser necesario, hacerlas cumplir.
3. Desarrollar un marco de trabajo de seguridad/derechos por diseño. Pueden encontrarse muchos ejemplos de esto, como por ejemplo «Safety by Design»,[192] que se pueden reproducir o en los cuales inspirarse.
4. Garantizar que todas las partes interesadas conozcan los procesos necesarios —tanto tecnológicos como de gobernanza— a la hora de establecer el marco de trabajo.
5. Llevar a cabo un estudio periódico de la situación general para determinar las amenazas emergentes y la eficacia de los marcos de trabajo, para garantizar que estos no queden obsoletos respecto a las innovaciones y a las prácticas comerciales.

192. «Safety by Design», eSafety Commissioner, 2018.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5 Responsabilidad corporativa

B **Introducir normas básicas**[193]

La industria tiene la responsabilidad de garantizar que los niños estén protegidos en Internet. Esto implica la creación de un espacio en Internet seguro y accesible para los niños. No se trata solo de impedir su acceso a contenidos dañinos. Se exigirá a las empresas que expongan qué procedimientos y qué consideraciones especiales han adoptado para garantizar la seguridad de los niños y el respeto de sus derechos, en el marco 4C de la gestión de riesgos[194], a medida que desarrollen y establezcan sus servicios en Internet.[195]El ministerio o el organismo pertinentes deben crear un código bajo la supervisión del Comité Directivo. Estas normas serán obligatorias y se exigirá su cumplimiento.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Introducir normas básicas en las áreas que abarca el marco de trabajo mencionado anteriormente. Identificar los modelos oportunos[196] de otros países o regiones.
2. Comprobar que las normas básicas cubran las siguientes áreas: verificación de la edad, moderación, términos o reglas de la comunidad, toma de decisiones automatizada y publicidad. Véase «Supportive tool 1» (página 109).

193. Véase, por ejemplo, «Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse», GOV.UK, 2020.
194. Consultar la sección sobre «Riesgos y daños».
195. «Los derechos del niño en evaluaciones de impacto», Fondo de las Naciones Unidas para la Infancia, 2013.
196. Véase, por ejemplo, «Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse», GOV.UK, 2020.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5 Responsabilidad corporativa

C Aplicación de la clasificación por edades

La aplicación de una clasificación coherente y por edades para los contenidos comerciales, los medios de comunicación de servicio público y los juegos y las actividades en Internet propicia un enfoque transparente y eficaz de la gestión de aquellos contenidos y servicios que afectan a los niños. Esto puede ser necesario para artículos y servicios a los que se les deba aplicar dicha clasificación y para los contenidos que estén pensados para diferentes rangos de edad. Se requerirá la verificación de la edad o la creación de espacios solo para adultos si se trata de contenidos prohibidos o de actividades que no sean adecuadas para niños. Para esto, quizá se deban proporcionar filtros de contenido que bloqueen los contenidos no deseados.[197]

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Encontrar un servicio de clasificación por edades adecuado. En muchos países ya hay una clasificación por edades para las películas comerciales[198] o los juguetes, por lo que se pueden utilizar esos mismos criterios y aplicarlos al material y a las actividades de Internet.
2. Ampliar a los espacios digitales, incluidas las aplicaciones, la obligación de clasificar por edades los contenidos y las actividades.
3. Garantizar que un órgano pertinente supervise las disputas y el incumplimiento de las normas.

D Introducir sistemas de moderación y de presentación de denuncias

Se requerirán mecanismos para identificar los contenidos perturbadores o inadecuados de los proveedores de servicios. Además, deben establecerse sistemas de supervisión transparentes y sólidos para todos los servicios de Internet, incluida implantación de mecanismos de retirada de contenidos. Habrá una línea directa pública y gratuita para ofrecer tanto información como ayuda o asesoramiento por parte de expertos. Los niños deben poder acceder con facilidad a los mecanismos de denuncia de contenidos. Los sistemas para señalar la existencia de contenidos inadecuados deben considerarse una herramienta adicional.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Establecer unas normas básicas, como se expone en el proceso A.
2. Determinar qué agencia estará al cargo de una línea directa pública.
3. Consultar con expertos para garantizar que los niños tengan acceso a los diferentes mecanismos.

197. But how do they know it is a child? (Pero, ¿cómo saben que es un niño?) 5Rights Foundation, 2021.
198. Véase, por ejemplo, el British Board of Film Classification.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5 Responsabilidad corporativa

E **Garantizar la protección de los niños contra la presión comercial**

Las medidas destinadas a proteger a los niños de la presión comercial incluirán: fomentar diseños apropiados para su edad, inhabilitar la publicidad dirigida y el intercambio con terceros y concienciar sobre el contexto en el que los niños crecen. Los productos y los servicios que pongan énfasis en los derechos y la seguridad infantil en Internet podrán contar con un certificado. Asimismo, se podrá actuar contra los proveedores de productos y de servicios que violen dichos valores.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar las leyes y regulaciones existentes referentes a las relaciones comerciales con los niños: tanto las que tienen que ve con la protección y los derechos de los niños como con los consumidores, cuentan con restricciones respecto a las relaciones comerciales con los niños o respecto a sectores como la sanidad o la educación.
2. Armonizar las directrices para garantizar que abarquen los productos y los servicios digitales.

F **Garantizar que se apliquen los principios del diseño centrado en niñas, niños y adolescentes para minimizar los posibles riesgos para la seguridad infantil en Internet**

Esto incluye, por ejemplo, la posibilidad de que adultos desconocidos puedan entrar en contacto con los niños, la publicidad dirigida sobre juegos de azar o la recomendación de contenidos dañinos. La seguridad infantil en Internet debe integrarse en la fase de diseño para evitar que surjan problemas más adelante.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

Evaluar las normas de la seguridad por diseño[199] para áreas específicas que puedan afectar a los niños indirectamente, como es el caso de los juegos de azar y las apuestas, los servicios financieros, la pornografía u otros ámbitos de Internet a los que no deberían acceder los niños.

199. But how do they know it is a child? (Pero, ¿cómo saben que es un niño?) 5Rights Foundation, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5 Responsabilidad corporativa

Cómo encaja esto con los documentos fundacionales:

Funciones reglamentarias y normativas de los Estados

Para cumplir con sus obligaciones de protección, los Estados deben:

a) hacer cumplir las leyes que tengan por objeto o por efecto obligar a las empresas a respetar los derechos humanos, evaluar de forma periódica la idoneidad de dichas leyes y remediar posibles vacíos jurídicos;

b) garantizar que otras leyes y normas que rigen la creación y las actividades de las empresas, como el derecho mercantil, no restrinjan el respeto de los derechos humanos por parte de las empresas, sino que lo fomenten;

c) asesorar de manera eficaz a las empresas sobre cómo respetar los derechos humanos en sus actividades;

d) promover que las empresas expliquen cómo determinan el impacto de sus actividades sobre los derechos humanos (y, si es preciso, exigírselo).

Fuente: «Principios rectores sobre las empresas y los derechos humanos de las Naciones Unidas», 2011, sección3[200]

Los Estados Parte deben hacer del interés superior del niño una cuestión primordial al regular la publicidad y las comunicaciones comerciales dirigidas a los niños y a las que puedan tener acceso. Los patrocinios, el posicionamiento de productos y todas las demás formas de contenido comercial deben distinguirse claramente del resto de contenidos y no deben perpetuar los estereotipos raciales o de género.

Observación general núm. 25 (2021), párr. 41[201]

Los Estados parte deben prohibir por ley la elaboración de perfiles, o la selección de niños de cualquier edad con fines comerciales, sobre la base de un registro digital con sus características (reales o inferidas), lo cual incluye los datos de grupos o colectivos y la elaboración de perfiles por asociación o afinidad. También debe prohibirse el contacto directo o indirecto con los niños en el caso de las prácticas que se basan en el neuromarketing, el análisis emocional, la publicidad inmersiva y la publicidad en entornos de realidad virtual y aumentada para promover productos, aplicaciones y servicios.

Fuente: Observación general núm. 25 (2021), párr. 42[202]

Herramientas de apoyo:

1. Pasos para diseñar productos y servicios digitales teniendo en cuenta los derechos de los niños

La 5Rights Foundation y el Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) han creado una norma con pasos prácticos que las empresas pueden seguir para diseñar productos y servicios digitales que sean apropiados para cada edad. Introduce una serie de procesos que las empresas pueden aplicar para que las necesidades de los jóvenes sean la piedra angular del diseño.

200. «Principios rectores sobre las empresas y los derechos humanos», Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2011.
201. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.
202. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

5 Responsabilidad corporativa

Otros recursos de referencia:

1. Un ejemplo de las reflexiones de los jóvenes sobre la responsabilidad corporativa

A los jóvenes con los que habló 5Rights les gustaría que las empresas tomasen las siguientes medidas:

- Reglas comunitarias coherentes en todas las plataformas
- Plazos claros para las denuncias
- Poder informar a las víctimas de lo que se ha hecho con su acosador
- Contenidos mejor etiquetados
- Poder retirar los contenidos con facilidad
- Prohibir la difusión de los abusos
- Ventanas emergentes en las que se hable de buenas conductas y que fomenten la configuración de niveles altos de privacidad
- Resolver de forma clara las reclamaciones
- Políticas redactadas en un lenguaje sencillo

2. Directrices de «Derechos del niño y principios empresariales de la ONU» sobre la rendición de cuentas del sector privado[203]

El sector privado también tiene responsabilidades respecto a la seguridad infantil en Internet, lo cual debería quedar claro en las esferas políticas pertinentes. Algunas áreas, como el acoso cibernético, la explotación sexual de menores o el fraude financiero, cuentan con marcos específicos para respaldar la seguridad infantil en Internet; pero existen, además, marcos de trabajo generales para la responsabilidad corporativa.

Los derechos de los niños y los principios empresariales necesitan que las empresas hagan lo siguiente:

- ☐ Asumir su responsabilidad de respetar los derechos de los niños comprometerse a respaldar los derechos humanos de los niños.
- ☐ Contribuir a la abolición del trabajo infantil, lo cual incluye las actividades y las relaciones comerciales.
- ☐ Ofrecer trabajos dignos tanto a los empleados jóvenes como a los padres o a los cuidadores.
- ☐ Garantizar la protección y la seguridad de los niños en todas las actividades y en todas las instalaciones de la empresa.
- ☐ Garantizar que los productos y los servicios sean seguros e intentar respaldar a través de ellos los derechos de los niños.
- ☐ Emplear estrategias de marketing y publicidad que respeten y respalden los derechos de los niños.
- ☐ Respetar y respaldar los derechos de los niños en relación con el medioambiente y con la adquisición y el uso de la tierra.
- ☐ Respetar y respaldar los derechos de los niños en lo tocante a las medidas de seguridad.
- ☐ Ayudar a proteger a los niños afectados por emergencias.
- ☐ Reafirmar las medidas de la comunidad y del Gobierno para proteger y hacer efectivos los derechos de los niños.

203. «Obligaciones y medidas en relación con los derechos de los niños y las empresas», Comisión Internacional de Juristas y Fondo de las Naciones Unidas para la Infancia, 2015.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

3. **Observación general núm. 16 (2013) sobre las obligaciones del Estado en relación con el impacto del sector empresarial en los derechos del niño**[204]
   Esta es la guía del Comité de los Derechos del Niño de la ONU sobre las obligaciones que tienen los Estados con respecto al impacto que tienen las actividades y las operaciones comerciales en los derechos de los niños.

4. **Las empresas y los derechos de los niños**[205] **(versión explicada)**
   Esta es una versión de fácil lectura de la «Observación general núm. 16» (2013) del Comité de los Derechos del Niño sobre las obligaciones del Estado con respecto al impacto del sector empresarial en los derechos de los niños.

5. **Principios rectores de los derechos de los niños y las empresas**[206]
   Desarrollado por UNICEF, el Pacto Mundial de las Naciones Unidas y Save the Children, se trata de un conjunto integral de principios para orientar a las empresas sobre todas las medidas que pueden tomar en el lugar de trabajo, en los mercados y en las comunidades para respaldar y apoyar los derechos de los niños.

6. **Obligaciones y medidas en relación con los derechos del niño y las empresas**[207]
   Esta es una guía práctica para los Estados sobre cómo aplicar la «Observación general núm. 16» (2013) del Comité de los Derechos del Niño de las Naciones Unidas.

7. **Norma IEEE 2089-2021 para el marco de trabajo de servicios digitales apropiados para cada edad**[208]
   La 5Rights Foundation y el Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) han creado una norma con pasos prácticos que las empresas pueden seguir para diseñar productos y servicios digitales que sean apropiados para cada edad.

8. **Guía de UNICEF para el uso de la herramienta de evaluación de la seguridad en Internet de los niños: Fomento de un entorno seguro en Internet para los niños por parte de las empresas tecnológicas**[209]
   Esta es la guía de UNICEF sobre el uso de su herramienta de evaluación de la seguridad infantil en Internet, que sirve de ayuda a las empresas para prepararse y completar una evaluación de su impacto sobre los niños. Describe el propósito, el contexto y las funciones de la herramienta de evaluación de la seguridad infantil en Internet y ofrece instrucciones y consejos detallados sobre el uso de la herramienta.

9. **Child Safety Online – A Practical Guide for Providers of Social Media and Interactive Services**[210]
   Esta es la guía del Gobierno del Reino Unido para que los proveedores de redes sociales hagan que sus plataformas sean más seguras para los usuarios. Está basada en el marco de seguridad de la ICT Coalition for Children Online, una iniciativa de la industria europea.

204. Observación general núm. 16 (2013) sobre las obligaciones de los Estados en relación con el impacto del sector empresarial en los derechos de los niños, Convención de las Naciones Unidas sobre los Derechos del Niño, 2013.
205. «Las empresas y los derechos de los niños» (versión explicada), Fondo de las Naciones Unidas para la Infancia y Save the Children, 2015.
206. «Derechos de los niños y principios empresariales», Fondo de las Naciones Unidas para la Infancia, Pacto Mundial de las Naciones Unidas y Save the Children, 2013.
207. «Obligaciones y medidas en relación a los derechos de los niños y las empresas», Comisión Internacional de Juristas y Fondo de las Naciones Unidas para la Infancia, 2015.
208. «Norma IEEE 2089-2021 para el marco de trabajo de servicios digitales apropiados para cada edad», IEEE SA, 2021.
209. Guía de UNICEF para el uso de la herramienta de evaluación de la seguridad en Internet de los niños, Fondo de las Naciones Unidas para la Infancia, 2016.
210. Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services, Departamento de Tecnología, Cultura, Medios de Comunicación y Deporte del Reino Unido, 2016.

10. **Informe de la 5Rights Foundation: «But How Do They Know It Is a Child»**[211]
    Este informe de la 5Rights Foundation aborda el debate sobre la verificación y la estimación de la edad.

11. **Código italiano sobre ciberacoso**[212]
    Este es el código formal del Gobierno italiano sobre ciberacoso (en italiano).

12. **Coalición Financiera contra la Pornografía Infantil**[213]
    Este informe describe los métodos utilizados por algunos miembros de la Coalición Financiera contra la Pornografía Infantil en sus procesos de solicitud y verificación, así como para detectar el material relacionado con la explotación sexual de los niños e impedir la creación o el mantenimiento de cuentas comerciales relacionadas con la distribución y la venta comercial de esa clase de material.

13. **Explotación sexual de los niños en Internet con fines comerciales, 2015**[214]
    Este informe de la Coalición Financiera Europea contra la Explotación Sexual de los Niños en Internet con Fines Comerciales es una actualización de la «Evaluación estratégica de la explotación sexual de los niños en Internet con fines comerciales» publicada en octubre de 2013, en el marco de trabajo de la Coalición Financiera Europea. Además de presentar los datos y las cifras de 2013, analiza otros factores fundamentales de este ámbito.

14. **Declaración Universal de Seguridad Infantil en Línea**[215]
    Esta es la declaración de la Comisión de la Banda Ancha, que tiene como objetivo alinear a todas las partes interesadas pertinentes en la misión común de defender la causa de la protección de los niños en Internet.

15. **Trilogy of Promising Practice, UNICEF Albania**[216]
    Este es un estudio de caso de Albania. Cuatro de las cinco principales empresas de Internet y telecomunicaciones han colaborado en un proceso participativo para redactar las directrices de la industria que han sido publicadas por la Autoridad Nacional de Certificación Electrónica y Ciberseguridad.

16. **Directrices de la OCDE para proveedores de servicios digitales**[217]
    Estas directrices pretenden complementar la «Recomendación del Consejo sobre la infancia en el entorno digital» [NOTA A PIE DE PÁGINA 2] y ofrecer asistencia a los proveedores de servicios digitales cuando toman medidas que pueden afectar directa o indirectamente a los niños en el entorno digital. El objetivo final es determinar la mejor manera de proteger y de respetar los derechos, la seguridad y los intereses de los niños.

211. But how do they know it is a child? (Pero, ¿cómo saben que es un niño?), 5Rights Foundation, 2021.
212. Disposiciones respecto a la protección de los menores para prevenir y contrastar el fenómeno del ciberacoso, Gazzetta Ufficiale, 2017.
213. Internet Merchant Acquisition and Monitoring Sound Practices to Help Reduce the Proliferation of Commercial Child Pornography (Adquisición comercial de Internet y control de prácticas eficaces para ayudar a reducir la proliferación de pornografía infantil), Centro Internacional para Niños Desaparecidos y Explotados, 2016.
214. Commercial Sexual Exploitation of Children Online (Explotación sexual comercial del niño en línea), Europol, 2015.
215. Declaración Universal de Seguridad Infantil en Línea, Comisión de Banda Ancha, 2019.
216. Programming for Children's Protection Online in Albania (Programación para la protección del niño en línea en Albania), Fondo de las Naciones Unidas para la Infancia, 2020.
217. Directrices de la OCDE para proveedores de servicios digitales, OCDE, 2021.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

«Debemos reformar las redes sociales para que puedan usarlas los niños que tienen alguna discapacidad. Hay que simplificar [...] el uso de internet en el lenguaje de signos para que los sordos podamos usar las plataformas digitales».

– Tanzania, 15

«Me gustaría que los niños [de las zonas rurales] pudieran disfrutar como todos los demás de las ventajas de Internet».

– Malasia, 13

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

6 Formación

> **Los profesionales que trabajan para (y con) los niños, y las empresas, incluidas las del sector tecnológico, deben recibir una formación que ofrezca, entre otras cosas, información sobre cómo el entorno digital afecta en múltiples contextos a los derechos de los niños, sobre cómo los niños ejercen sus derechos en el entorno digital y sobre cómo acceden a la tecnología y la utilizan. También deben recibir formación respecto a la aplicación en el entorno digital de las normas internacionales de derechos humanos. Los Estados parte deben velar por que se imparta formación previa al servicio y durante el servicio, en relación con el entorno digital, a los profesionales que trabajan en todos los niveles educativos, a fin de respaldar el desarrollo de sus conocimientos, aptitudes y prácticas.**
>
> Fuente: Observación general núm. 25 (2021), párr. 33[218]

Objetivo:

Garantizar que todos los involucrados en los servicios relacionados con los niños, incluidos el Gobierno, las fuerzas del orden, la justicia, la sanidad y el bienestar, los políticos y los funcionarios públicos, así como los que diseñan tecnologías, tengan una buena comprensión de la seguridad infantil en Internet y del interés superior de los niños.

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

6a. Facilitar formación, desarrollo de habilidades y orientación a todos los involucrados en la seguridad infantil en Internet

Desde los que ofrecen contenidos o servicios hasta los jueces, todos los que forman parte de la cadena de aplicación de la ley y los profesionales que trabajan con niños en otros entornos como la educación o la sanidad, deben estar familiarizados con la seguridad infantil en Internet. Se les debe facilitar una formación completa, en concreto sobre cómo su función particular se relaciona con la seguridad infantil en Internet, cómo reconocer los comportamientos delictivos y cómo proporcionar a las víctimas acceso a la asistencia necesaria.

6b. Facilitar formación especializada sobre la asistencia psicosocial y la identificación de todas aquellas señales que alerten de problemas respecto a la seguridad infantil en Internet

Para ser eficaces, los profesionales pertinentes deben recibir formación sobre la seguridad de los niños en internet, sobre políticas de salvaguarda y protección de la infancia y sobre asesoramiento infantil y familiar. La concienciación sobre la seguridad infantil en Internet debe incorporarse a los marcos de trabajo existentes relacionados con la protección de los niños. Los profesionales que trabajan con niños en la educación, la sanidad, la comunidad y en otros entornos deben estar capacitados para reconocer las señales y los síntomas que alerten de problemas respecto a la seguridad infantil en Internet.

6c. Crear planes de educación terciaria

Las sesiones sobre seguridad infantil en Internet deben ser parte obligatoria en los campos de la enseñanza, el trabajo social, el trabajo sanitario, la psicología y de otros programas lectivos relevantes, tanto en universidades públicas o privadas como en el resto de instituciones educativas. Es necesario revisar con periodicidad la eficacia de estos conocimientos a la luz de los avances en la formación sobre seguridad infantil en Internet y de las cuestiones emergentes. Los planes de estudio deben abarcar todos los aspectos de la seguridad infantil en Internet, como se establece en esta política. ▶

218. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

6 Formación

6d. Fomentar el desarrollo profesional

Se establecerán, se revisarán y se actualizarán periódicamente programas de educación continua sobre la seguridad y la protección de los niños en Internet destinados a los profesionales que trabajan en las esferas pertinentes, a fin de mantenerse al día respecto a los avances tecnológicos y de abordar nuevos obstáculos y preocupaciones a medida que vayan surgiendo.

Hoja de ruta para alcanzar el objetivo:

A **Facilitar formación, desarrollo de habilidades y orientación a todos los involucrados en la seguridad infantil en Internet**

Desde los que ofrecen contenidos o servicios hasta los jueces, todos los que forman parte de la cadena de aplicación de la ley y los profesionales que trabajan con niños en otros entornos como la educación o la sanidad, deben estar familiarizados con la seguridad infantil en Internet. Se les debe facilitar una formación completa, en concreto sobre cómo su función particular se relaciona con la seguridad infantil en Internet, cómo reconocer los comportamientos delictivos y cómo proporcionar a las víctimas acceso a la asistencia necesaria.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar las profesiones y los contactos necesarios que puedan necesitar formación sobre seguridad infantil en Internet. La «Herramienta de apoyo 1» que se puede encontrar más adelante resulta útil a este respecto (consultar la página 119).
2. Revisar los programas de formación existentes y determinar en qué momento y con qué nivel de detalle se requiere formación respecto a la seguridad infantil en Internet (consultar los recursos a continuación).
3. Encargar la formación sobre seguridad infantil en Internet (o actualizarla, si ya existe) que sea aplicable al ámbito en cuestión. Este tipo de material puede compartirse entre diferentes disciplinas para garantizar una formación de alta calidad.
4. Garantizar que la cualificación en cualquiera de los campos esté sujeta a completar con éxito la formación.
5. Garantizar que los materiales de formación se actualicen con periodicidad y cubran todos los aspectos de la vida de un niño en Internet: contenidos, contactos, conductas y riesgos comerciales.
6. Estudiar cómo incorporar la voz y la opinión de los niños y de los jóvenes a la formación.[219]

219. Véase, por ejemplo, «Modelo Lundy sobre participación infantil», Comisión Europea, 2007.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

6 Formación

B **Facilitar formación especializada sobre la asistencia psicosocial y la identificación de todas aquellas señales que alerten de problemas respecto a la seguridad infantil en Internet**

Para ser eficaces, los profesionales pertinentes deben recibir formación sobre la seguridad de los niños en internet, sobre políticas de salvaguarda y protección de la infancia y sobre asesoramiento infantil y familiar. La concienciación sobre la seguridad infantil en Internet debe incorporarse a los marcos de trabajo existentes relacionados con la protección de los niños. Los profesionales que trabajan con niños en la educación, la sanidad, la comunidad y en otros entornos deben estar capacitados para reconocer las señales y los síntomas que alerten de problemas respecto a la seguridad infantil en Internet, comprender en qué consisten las conductas ofensivas y proporcionar información sobre el acceso de las víctimas a la asistencia.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar a aquellos que necesitan formación para el apoyo psicosocial y respecto a la explotación sexual de menores.
2. Identificar aquellos tipos de formación que han demostrado resultados, ya sea a nivel internacional o nacional (consultar «Otros recursos» para la referencia 1-4 a continuación).
3. Garantizar que los recursos económicos y el tiempo sean una prioridad para la formación en relación con la explotación sexual de menores.
4. Identificar cuándo y cómo se impartirá, se revisará y se actualizará la formación.
5. Estudiar cómo incorporar la voz y la opinión de los niños y de los jóvenes a la formación.[220]
6. Crear identificadores clave de rendimiento (KPI) para la formación de los empleados. Dichos identificadores se evaluarán y se expondrán regularmente.

220. Véase, por ejemplo, «Modelo Lundy sobre participación infantil», Comisión Europea, 2007.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

6 Formación

C **Crear planes de educación terciaria**

Las sesiones sobre seguridad infantil en Internet deben ser parte obligatoria en los campos de la enseñanza, el trabajo social, el trabajo sanitario, la psicología y de otros programas lectivos relevantes, tanto en universidades públicas o privadas como en el resto de instituciones educativas. Es necesario revisar con periodicidad la eficacia de estos conocimientos a la luz de los avances en la formación sobre seguridad infantil en Internet y de las cuestiones emergentes. Los planes de estudio deben abarcar todos los aspectos de la seguridad infantil en Internet, como se establece en esta política.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente consultar «Otros recursos» para la referencia 1, a modo de ejemplos.

D **Fomentar el desarrollo profesional**

Se establecerán, se revisarán y se actualizarán periódicamente programas de educación continua sobre la seguridad y la protección de los niños en Internet destinados a los profesionales que trabajan en las esferas pertinentes, a fin de mantenerse al día respecto a los avances tecnológicos y de abordar nuevos obstáculos y preocupaciones a medida que vayan surgiendo.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Garantizar que la formación esté disponible durante toda la carrera profesional de los interesados y reaccionar de manera efectiva ante los cambios tanto en el mundo digital como en las funciones de los profesionales.
2. Identificar oportunidades de formación adicional.
3. Crear planes de estudios para formación que respalden un aprendizaje más detallado o «complementario» (consultar «Otros recursos»para la referencia 1-4 a continuación).
4. Estudiar cómo incorporar a la formación la voz y la opinión de los jóvenes.[221]

221. Véase, por ejemplo, «Modelo Lundy sobre participación infantil», Comisión Europea, 2007.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

6 Formación

Cómo encaja esto con los documentos fundacionales:

> **Los Estados parte deben analizar cómo los diferentes usos de las tecnologías digitales pueden facilitar u obstaculizar la investigación y el enjuiciamiento de los delitos contra los niños y adoptar todas las medidas preventivas, coercitivas y correctivas disponibles, lo que incluye trabajar de forma conjunta con colaboradores internacionales. Deben impartir formación especializada a los funcionarios encargados de hacer cumplir la ley, a los fiscales y a los jueces sobre las violaciones de los derechos de los niños relacionadas con el entorno digital, lo que incluye cooperar internacionalmente.**
>
> Fuente: Observación general núm. 25 (2021), párr. 47[222]

222. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

6 Formación

Herramientas de apoyo:

1. Una lista de las profesiones que pueden beneficiarse de una formación específica y temas por abordar

Esto se ha diseñado para que se pueda determinar si la formación existente es apropiada y relevante para los profesionales en la jurisdicción pertinente y para identificar las posibles carencias. Esto forma parte de los pasos a seguir para completar el proceso A («Proporcionar formación, desarrollo de habilidades y orientación a todos los involucrados en la seguridad de los niños en Internet»).

Profesión	Formación sobre todos los problemas de seguridad infantil en Internet y las «4C» relacionadas con los riesgos	Formación sobre salvaguarda y políticas de salvaguarda	Identificar los problemas de seguridad infantil en Internet	Entender las conductas de los delincuentes y la rehabilitación	Asesora-miento	Apoyo a las víctimas
Jueces	*[identificar la formación existente o sus carencias]*					
Cumplimiento de la ley						
Trabajadores sociales						
Trabajadores sanitarios						
Profesores						
Trabajadores en entornos comunitarios						
Psicólogos						
Otros						

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

6 Formación

Otros recursos de referencia:

En Internet hay disponibles muchos ejemplos de módulos de formación para los diferentes grupos de profesionales. Debe impartirse formación inicial, terciaria y continua a un amplio abanico de profesionales, incluidos profesores/educadores, policías, trabajadores del sector de la Justicia, trabajadores sociales y aquellos que trabajen con jóvenes, profesionales de la salud, parlamentarios, funcionarios públicos, tecnólogos (incluidos programadores informáticos, diseñadores de experiencia de usuario y responsables de la gobernanza) y reguladores de los ámbitos pertinentes.

1. **Recursos para profesores, trabajadores sociales y para quienes trabajan con jóvenes**
   Consultar la formación sobre seguridad en Internet de la NSPCC. Quienes trabajan con niños y jóvenes deben saber qué hacer si un niño acude a ellos para hablarles de algo que le preocupa o que haya visto en Internet. Esta formación se ha diseñado para ayudar a los profesionales a confiar en su capacidad para brindar seguridad a los niños en Internet.[223]

2. **Recursos para profesionales de la salud**
   La formación en línea de eIntegrity sobre protección infantil para profesionales de la salud («Safeguarding Children and Young People») abarca las competencias y los conocimientos necesarios para los profesionales de la salud y la asistencia social de cara a salvaguardar el bienestar de los niños. En su desarrollo ha participado un consorcio de asociaciones profesionales, con el Royal College of Paediatrics and Child Health a la cabeza.[224]

   Este curso de protección en línea está conectado con el marco de trabajo del Reino Unido referente a la formación sobre esta área: el documento interuniversitario «Safeguarding Children and Young People: Roles and Competencies for Health Care Staff» (2019).[225] Sin embargo, los temas son extrapolables a los profesionales de la salud y de la asistencia social de todo el mundo.[226]

3. **Recursos para la aplicación de la ley**[227]
   El ICMEC ofrece una variedad de oportunidades de formación y cursos, tales como:

   - ☐ Claves de los delitos contra los niños que la tecnología facilita
   - ☐ Investigaciones avanzadas de explotación en Internet
   - ☐ Tecnologías avanzadas
   - ☐ Fundamentos para actuar respecto a niños desaparecidos.

223. Introduction to safeguarding and child protection training (Introducción a la salvaguardia y protección infantil), National Society for the Prevention of Cruelty to Children.
224. Online child protection training for healthcare professionals (Formación en línea sobre protección infantil para profesionales de la salud), eIntegrity.
225. Safeguarding children and young people – roles and competencies (Salvaguardia de niños y jóvenes; roles y competencias), Royal College of Paediatrics and Child Health, 2019.
226. Online child protection training for healthcare professionals (Formación en línea sobre protección infantil para profesionales de la salud), eIntegrity.
227. Building global capacity to keep children safer from harm (Generación de capacitación global para evitar perjuicios al niño), International Centre for Missing & Exploited Children, 2015 y recursos del ICMEC, International Centre for Missing & Exploited Children.

4. **Violencia de género en Namibia: una evaluación exploratoria y mapeo de los servicios de respuesta a la violencia de género en Windhoek, 2016**[228]
   La Unidad de Protección (GBVPU) contra la Violencia de Género (GBC) y los programas de Formación de Testigos para Menores imparten formación en Namibia a investigadores, fiscales, magistrados y trabajadores sociales de la Policía (personal de protección de la infancia) para garantizar una mejor asistencia integral a las víctimas. La GBVPU es accesible para discapacitados, cuenta con una sala de entrevistas en vídeo adaptada para niños y se rige por los procedimientos operativos estándar de la GBV/VAC.

5. **Recursos para el sector de la Justicia**[229]
   El proyecto EndOCSEA del Consejo de Europa facilita formación sobre la explotación sexual de menores a jueces y fiscales.

6. **Recursos generales**
   La Family and Child Commission de Queensland ha elaborado un módulo sobre la protección de los niños en Internet.[230]

228. Gender-based Violence in Namibia: An exploratory assessment and mapping of GBV response services in Windhoek (Violencia de género en Namibia: una evaluación exploratoria y mapeo de los servicios de respuesta a la violencia de género en Windhoek), Victims 2 Survivors y UNAIDS, 2016.
229. End Online Child Sexual Exploitation and Abuse (Poner fin a la explotación y abuso sexuales del niño), Consejo de Europa, 2021.
230. Módulo sobre la protección de los niños en Internet, Family & Child Commission de Queensland, 2022.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

7 Educación

> **Los Estados parte deben facilitar y apoyar la creación de contenidos digitales apropiados para cada edad y que sean positivos para los niños, siempre en consonancia con la evolución de sus capacidades, y velar por que los niños tengan acceso a diferentes tipos de información —incluida la información con la que cuentan los organismos públicos— sobre cultura, deporte, artes, salud, asuntos civiles y políticos y sobre los derechos del niño.**
>
> **Los Estados parte deben fomentar la producción y la difusión de dicho contenido en múltiples formatos y a partir de una pluralidad de fuentes nacionales e internacionales, incluidos los medios de comunicación, las emisoras de radio y televisión, los museos, las bibliotecas y las organizaciones educativas, científicas y culturales. Sobre todo, deben poner especial énfasis en mejorar la divulgación de contenidos diversos, accesibles y beneficiosos para niños con discapacidad y para niños pertenecientes a grupos étnicos, lingüísticos e indígenas minoritarios o a otros grupos similares. La posibilidad de acceder a información de relevancia en los idiomas que los niños entiendan puede tener un impacto positivo y significativo en términos de igualdad.**
>
> Fuente: Observación general núm. 25 (2021), párrs. 51 y 52[231]

Objetivo:

Promover un uso sano de la tecnología digital como fuente de entretenimiento, de información y de aprendizaje para los niños en un entorno seguro.

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

7a. Designar orientadores de protección infantil

Cada colegio debe designar un orientador de protección infantil.[232] Cada orientador debe recibir formación sobre procedimientos de protección infantil y formación específica sobre la seguridad infantil en Internet. Los orientadores tendrán la responsabilidad de garantizar que se adopten, se promulguen y se hagan cumplir en los colegios las políticas de seguridad infantil en Internet (incluidos los procedimientos de salvaguardia y los sistemas de denuncia anónima). El orientador de protección infantil será la persona de contacto en relación a las cuestiones relacionadas con la protección infantil y la seguridad infantil en Internet. Asimismo, comunicará a las autoridades pertinentes los perjuicios que se denuncien. Los orientadores deben facilitar, además, los planes de intervención para proteger a los niños contra cualquier posible perjuicio.

7b. Promover una educación digital accesible

Promover contenidos —incluidos los programas entre pares— de probada eficacia que ayuden a los niños a desarrollar habilidades digitales y los empoderen de cara a construir comunidades respetuosas que fomenten la seguridad infantil en Internet. La educación digital debe ser holística y abarcar los datos y la alfabetización mediática, junto con las cuestiones de salvaguardia (sobre todo, cuestiones como la sexualidad y el consentimiento). La educación debe hacerse extensiva a los padres/cuidadores para respaldar el papel de estos en el fomento de la seguridad infantil en Internet. ▶

231. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, Comité de los Derechos del Niño de las Naciones Unidas, 2021.
232. Podría tratarse de alguien de una junta de seguridad escolar, un educador o alguien de un comité de protección infantil de la aldea o de la comunidad en el que estén representados los colegios.

7 Educación

7c. Promover contenidos educativos
A medida que se generalice la adopción digital, se proporcionarán a los alumnos y a los profesores los conocimientos necesarios para interactuar con los sistemas digitales y para beneficiarse plenamente de los contenidos del plan de estudios, tanto en idiomas locales como internacionales.

7d. Promover la alfabetización de datos
Se introducirá un programa de alfabetización de datos en todo el plan de estudios. El programa educará a los niños sobre la forma en que se pueden utilizar sus datos y proporcionará una comprensión básica de la economía de los datos. Se enfatizará y se fomentará el uso positivo, autónomo y creativo de las tecnologías digitales por parte de los niños; se definirán claramente los riesgos, las ventajas y los beneficios sociales del uso de la tecnología; y se tendrá como objetivo garantizar que las medidas de protección y de prevención se difundan, se comprendan y se apliquen en profundidad. En la alfabetización de datos debe quedar claro quiénes son los responsables de la seguridad en Internet.

7e. Promover el pensamiento crítico
La educación de los niños y los de los padres/cuidadores respecto al pensamiento crítico y a los riesgos de la desinformación en Internet deben incorporarse a la educación sobre cultura digital. Lo anterior debe incluir una educación más amplia que promueva la comprensión y el conocimiento de los derechos humanos —en particular de los derechos del niño— y de sus mecanismos dentro y fuera de Internet.[233]

7f. Introducir en los colegios procedimientos formales para la seguridad infantil en Internet
La formación en materia de seguridad infantil en Internet debe ser obligatoria en las titulaciones relacionadas con la enseñanza, tanto para primaria como para secundaria, y dicha formación deberá continuar durante la carrera profesional. Todos los profesores deben completar la formación obligatoria sobre la seguridad infantil en Internet, conocer la política escolar en relación con la seguridad infantil en Internet e impartir conocimientos sobre la seguridad infantil en Internet a sus alumnos. Todos los colegios deben designar a un orientador en materia de seguridad infantil en Internet que defienda las normas de seguridad infantil en Internet y se haga cargo de hacer cumplir la política escolar sobre seguridad infantil en Internet.

233. Véase el artículo 29 de la Convención sobre los Derechos del Niño y las secciones pertinentes de la observación general.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

7 Educación

Hoja de ruta para alcanzar el objetivo:

A **Designar orientadores de protección infantil**

Cada colegio debe designar un orientador de protección infantil.[234] Cada orientador debe recibir formación sobre procedimientos de protección infantil y formación específica sobre la seguridad infantil en Internet. Los orientadores tendrán la responsabilidad de promulgar y hacer que se cumplan en los colegios las políticas de seguridad infantil en Internet (incluidos los procedimientos de salvaguardia y los sistemas de denuncia anónima). Esta figura será la persona de contacto en relación a las cuestiones relacionadas con la protección infantil y la seguridad infantil en Internet. Asimismo, comunicará a las autoridades pertinentes los perjuicios que se denuncien. Los orientadores deben facilitar, además, los planes de intervención para proteger a los niños contra cualquier posible perjuicio.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar las políticas y las normas de protección y de salvaguardia infantil que existan en el colegio y asegurarse de que incluyan módulos sobre la seguridad infantil en Internet. Si no existieran dichas normas o políticas, se deben emplear las prácticas recomendadas. En «Otros recursos» 1-6 se pueden encontrar algunos ejemplos.
2. En cualquier caso, hay que garantizar que la preparación de cada año escolar incluya medidas actualizadas de protección y de salvaguardia infantil y que se facilite a todos los profesores una panorámica general de los problemas de seguridad infantil. En «Otros recursos» 2 hay información sobre los cursos en línea disponibles para los profesionales que están en primera línea.

234. Podría tratarse de alguien de una junta de seguridad escolar, un educador o alguien de un comité de protección infantil de la aldea o de la comunidad en el que estén representados los colegios.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

7 Educación

B **Promover una educación digital accesible**

Promover contenidos —incluidos los programas entre pares— de probada eficacia que ayuden a los niños a desarrollar habilidades digitales y los empoderen de cara a construir comunidades respetuosas que fomenten la seguridad infantil en Internet. La educación digital debe ser holística y abarcar los datos y la alfabetización mediática, junto con cuestiones como la sexualidad y el consentimiento. La educación en materia de protección y salvaguardia infantil debe hacerse extensiva a los padres/cuidadores para respaldar el papel de estos en el fomento de la seguridad infantil en Internet.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Garantizar que la cultura digital incluya todo el abanico de experiencias en Internet y no solo los problemas de seguridad, ya que muchos niños a los que no les interesa la seguridad electrónica están muy abiertos a una comprensión más amplia de las oportunidades y los riesgos. Véase el modelo de DQ (consultar «Otros recursos» 3) de las áreas que deben abarcarse (véase «Recursos» a continuación). Se debe garantizar que cualquier área que relacionada con los riesgos abarque las «4C» (véase la sección «Identificación de riesgos y mitigación de daños»).
2. Garantizar que la educación sexual, la sexualidad y el consentimiento se expliquen en el contexto del mundo digital para garantizar que los niños tengan la máxima capacidad de acción posible sobre los problemas relacionados con esas cuestiones que puedan surgir en Internet.
3. Identificar programas de cultura digital en el idioma pertinente o que estén disponibles para su traducción, de ser necesario.[235]
4. Garantizar que la cultura digital de los padres/cuidadores esté totalmente alineada con la cultura digital de los niños. Los recursos para los padres deben estar enfocados de una manera positiva y ser exhaustivos, de forma que no generen miedos innecesarios respecto al mundo digital ni fomenten medidas drásticas contra los niños.[236]
5. Buscar empresas tecnológicas que ofrezcan programas gratuitos de cultura digital tanto para niños como para adultos. Dichos programas suelen estar muy bien diseñados y son muy efectivos, aunque no identifican los riesgos y los perjuicios comerciales de la propia tecnología. Si se opta por estos programas, conviene comprobar que cubren todos los aspectos relacionados con los riesgos, incluidos los que generan los propios programas.

235. Véase, por ejemplo, «Digital Literacy», Unión Internacional de Telecomunicaciones.
236. Véase, por ejemplo, «Media and Digital Literacy: Resources for Parents», The George Lucas Educational Foundation, 2012.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

7 Educación

C **Promover los contenidos educativos**

A medida que se generalice la adopción digital, se proporcionarán a los alumnos y a los profesores los conocimientosnecesarios para interactuar con los sistemas digitales y para beneficiarse plenamente de los contenidos del plan de estudios, tanto en idiomas locales como internacionales.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar buenos contenidos educativos que estén en línea con el plan de estudios o con las actividades extracurriculares del colegio.
2. Garantizar que los términos de uso sean apropiados para la privacidad y la seguridad de los alumnos.
3. Garantizar que todos los alumnos, independientemente de su género, sus posibles discapacidades o su nivel socioeconómico, puedan acceder a los recursos. Para esto puede hacer falta valorar la conectividad, la asequibilidad —incluidos los datos— y el acceso a los dispositivos adecuados.
4. Buscar recursos de instituciones reputadas —por ejemplo, universidades, colegios, ONG— y que ofrezcan una buena variedad de temas y recursos. Para ciertos temas puede ser más conveniente utilizar material que ya exista, o traducirlo, en vez de crear el material desde cero. En otros casos, puede ser una buena inversión identificar o encargar material en idiomas locales y que incorpore la cultura o la historia locales.
5. Se debe valorar el hecho de que la gran variedad de materiales disponibles en Internet puede complementar los conocimientos especializados disponibles a nivel local. No obstante, los profesores cualificados ofrecen una experiencia cualitativamente diferente al aprendizaje en línea.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

7 Educación

D **Promover la alfabetización de datos**

Se introducirá un programa de alfabetización de datos en todo el plan de estudios. El programa educará a los niños sobre la forma en que se pueden utilizar sus datos y proporcionará una comprensión básica de la economía de los datos. Se enfatizará y se fomentará el uso positivo, autónomo y creativo de las tecnologías digitales por parte de los niños; se definirán claramente los riesgos, las ventajas y los beneficios sociales del uso de la tecnología; y se tendrá como objetivo garantizar que las medidas de protección y de prevención se difundan, se comprendan y se apliquen en profundidad. En la educación sobre alfabetización de datos debe quedar claro quiénes son los responsables de la seguridad en Internet.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente tener en cuenta los recursos y las medidas que se exponen en los puntos A-C anteriores.

E **Promover el pensamiento crítico**

La educación de los niños y los de los padres/cuidadores respecto al pensamiento crítico y a los riesgos de la desinformación en Internet deben incorporarse a la educación sobre cultura digital. Lo anterior debe incluir una educación más amplia que promueva la comprensión y el conocimiento de los derechos humanos —en particular de los derechos del niño— y de sus mecanismos dentro y fuera de Internet.[237]

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente tener en cuenta los recursos y las medidas que se exponen en los puntos A-C anteriores.

237. Consultar el artículo 29 de la Convención sobre los Derechos del Niño y las secciones pertinentes de la observación general.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

7 Educación

F **Introducir en los colegios procedimientos formales para la seguridad infantil en Internet**

La formación en materia de seguridad infantil en Internet debe ser obligatoria en las titulaciones relacionadas con la enseñanza, tanto para primaria como para secundaria, y dicha formación deberá continuar durante la carrera profesional. Todos los profesores deben completar la formación obligatoria sobre la seguridad infantil en Internet, conocer la política escolar en relación con la seguridad infantil en Internete impartir conocimientos sobre la seguridad infantil en Internet a sus alumnos. Todos los colegios deben designar a un orientador en materia de seguridad infantil en Internet que defienda las normas de seguridad infantil en Internet y se haga cargo de hacer cumplir la política escolar sobre seguridad infantil en Internet.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente tener en cuenta los recursos y las medidas que se exponen en los puntos A-C anteriores.

Cómo encaja esto con los documentos fundacionales:

Educar a los niños en relación a la cultura digital como parte de una estrategia para garantizar que puedan beneficiarse de la tecnología sin consecuencias negativas. Esto permitirá a los niños desarrollar habilidades de pensamiento crítico que les ayudarán a identificar y a comprender los aspectos buenos y malos de su comportamiento en el espacio digital. Si bien es importante ilustrar a los niños respecto a los peligros de Internet, esto solo será efectivo si forma parte de un programa más amplio de cultura digital apropiado para cada edad y centrado en las habilidades y las competencias. Es importante incluir conceptos de aprendizaje social y emocional dentro de la educación sobre seguridad en Internet, ya que así los alumnos comprenderán y gestionarán las emociones y podrán establecer relaciones sanas y respetuosas dentro y fuera de Internet.

Fuente: «Directrices sobre la protección de la infancia en línea para los encargados de formular políticas», Unión Internacional de Telecomunicaciones, 2020[238]

Garantizar una educación de calidad inclusiva y equitativa y promover oportunidades de aprendizaje a lo largo de la vida para todos.

Fuente: Objetivo de desarrollo sostenible 4[239]

238. «Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas», Unión Internacional de Telecomunicaciones, 2020.
239. Objetivo 4: Garantizar una educación inclusiva y equitativa de calidad y promover oportunidades de aprendizaje a lo largo de la vida para todos, Naciones Unidas, 2017.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

7 Educación

Herramientas de apoyo:

1. Una lista de verificación para garantizar los procedimientos formales de seguridad infantil en Internet en los colegios

El objetivo de esto es identificar en los colegios carencias respecto a los procedimientos de seguridad infantil en Internet. Se realizará un seguimiento de los avances en relación con el proceso F («Introducir procedimientos formales de seguridad infantil en Internet en los colegios»).

Pregunta	Respuesta
¿La seguridad infantil en Internet forma parte de los cursos de formación del profesorado?	
¿Todas las escuelas primarias y secundarias cuentan con un orientador sobre seguridad infantil en Internet?	
¿Todas las escuelas primarias y secundarias cuentan con una política de seguridad infantil en Internet?	
¿Todas las escuelas primarias imparten a los alumnos cursos sobre la seguridad infantil en Internet? a. Designar orientadores de protección infantil b. Promover una educación digital accesible c. Promover los contenidos educativos d. Promover la alfabetización de datos e. Promover el pensamiento crítico f. Introducir en los colegios procedimientos formales para la seguridad infantil en Internet	
¿Todas las escuelas secundarias imparten a los alumnos cursos sobre la seguridad infantil en Internet?	

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

7 Educación

Otros recursos de referencia:

1. **Kit de capacitación digital para niños de DQ: Child Digital Readiness Kit: Curso en línea de 8 días para niños (de entre 8 y 12 años) y padres**[240]
   Un programa de aprendizaje en línea de 8 días en el que los niños aprenden las «8 habilidades para la ciudadanía digital», con una supervisión mínima de padres o profesores. A medida que los niños completen cada «habilidad de ciudadanía digital», DQ enviará a los padres por correo electrónico un informe en el que se detallarán el progreso de sus hijos y la exposición a los riesgos cibernéticos. Los padres recibirán, además, una copia del «Parenting Handbook» (manual de paternidad) de DQ para ayudarlos a mejorar el coeficiente de desarrollo de toda la familia.

2. **Seguridad de los niños en Internet en Sudáfrica**[241]
   Este sitio web proporciona orientación interactiva para educadores y cuidadores sobre la seguridad infantil en Internet. Se anima a los cuidadores y a los educadores a compartir en la plataforma sus estrategias o sus políticas escolares.

3. **Asociación Nacional de Psicólogos Escolares: un marco de trabajo para que las escuelas sean seguras y ofrezcan una enseñanza de calidad**[242]
   Este marco de trabajo ofrece recomendaciones sobre cómo mejorar la seguridad física y mental de los niños y los jóvenes a partir de una estrategia de seguridad y de apoyo para las escuelas.

4. **International Task Force on Child Protection (Grupo internacional de estudio sobre la protección de la infancia): normas y expectativas internacionales de protección de la infancia**[243]
   Este informe, preparado por el Comité de Evaluación Escolar, proporciona requisitos de evaluación de protección infantil a las agencias de acreditación e inspección.

5. **Council of International Schools**[244]
   Este sitio web proporciona orientación y herramientas útiles para los cuidadores y los educadores en relación a la seguridad de los niños y los jóvenes. Ofrece ejemplos de talleres de protección infantil, talleres de salud mental y de bienestar, normas de reclutamiento seguro, etc.

6. **Formación sobre seguridad en Internet de la NSPCC (en inglés)**[245]
   Este curso en línea ofrece a los cuidadores formación en materia de seguridad; es decir, cómo y qué deben tener en cuenta con respecto a la seguridad infantil en Internet. Incluye áreas temáticas importantes relativas a Internet, como la radicalización y el extremismo, el acoso escolar o el abuso sexual. ▶

240. Global Digital Citizenship Movement for 8-12 Year-Olds (Movimiento mundial de ciudadanía digital para niños de 8 a 12 años), DQ Institute.
241. Child Online Safety (Seguridad del niño en línea), Thutong Education Portal.
242. A Framework for Safe and Successful Schools (Un marco de trabajo para escuelas seguras y exitosas), National Association of School Psychologists, 2013.
243. Updated Standards for Child Protection Adopted by School Evaluation Agencies (Estándares actualizados para la protección del niño adoptados por las agencias de evaluación escolar), International Centre for Missing & Exploited Children, 2021.
244. Recursos, Council of International Schools.
245. Introduction to safeguarding and child protection training (Introducción a la salvaguardia y protección infantil), National Society for the Prevention of Cruelty to Children.

7. Ejemplos de recursos educativos que respaldan la seguridad de los niños en Internet

A. Ejemplo de plan de estudios: Plan de estudios «Young and eSafe» de la Oficina Australiana del Comisionado de Seguridad Electrónica[246]
Este sitio web proporciona recursos a modo de vídeos cortos y contenidos educativos para ayudar a los jóvenes a familiarizarse con conductas positivas en Internet.

B. Lecciones gratuitas de ciudadanía digital de Common Sense Education para niños de todas las edades[247]
Este sitio web ofrece lecciones gratuitas para ayudar a niños y a los jóvenes aprender habilidades de ciudadanía digital. Las lecciones incluyen cuestiones como por ejemplo el ciberacoso o la privacidad en Internet.

C. Unión Internacional de Telecomunicaciones: «Libro de ejercicios sobre seguridad en línea»[248]
Este libro de actividades de seguridad en línea ofrece una introducción a la Convención sobre los Derechos delNiño y algunos ejercicios sobre cómo interactuar de forma segura con otras personas en Internet.

D. Unión Internacional de Telecomunicaciones: «Teacher's Guide»[249]
Este manual contiene instrucciones y recursos para completar ejercicios de seguridad en Internet en clase, con niños de 9 a 12 años. El objetivo de las actividades es fomentar el diálogo entre alumnos y profesores respecto a temas de seguridad en Internet y sobre cómo gestionarlos.

E. «Digiworld» de la UIT: un ejemplo de aplicación práctica de las directrices de la UIT sobre la protección de la infancia en línea,[250]
Este documento explica cómo se pueden utilizar, en la práctica, las directrices de la UIT para desarrollar las medidas para la seguridad de los niños en Internet.

F. Kit de herramientas educativas de Childnet International[251]
¡Da un paso adelante! ¡No te calles! El kit de herramientas educativas es un recurso práctico e interactivo que aborda, a partir de diferentes escenarios, el problema del acoso sexual en Internet para jóvenes de entre 13 y 17 años. Este kit de herramientas consta de cuatro grupos de lecciones con vídeos ilustrativos, historias en audio, talleres y una presentación a modo de asamblea.

G. Directrices del Reino Unido: Cómo enseñar seguridad en Internet en los colegios[252]
En esta guía se ofrece ayuda a los colegios para enseñar a sus alumnos a navegar seguros por Internet, tanto en las materias nuevas y como en las ya existentes.

H. Libro y vídeo «Kiko and the Manymes», EndOCSEA, Consejo de Europa[253]
Un libro de cuentos —con vídeo incluido— publicado por el Consejo de Europa y que proporciona orientación tanto a los cuidadores como a los niños pequeños sobre cómo usar Internet de manera segura.

246. Young and eSafe, Oficina Australiana del Comisionado de Seguridad Electrónica.
247. Everything You Need to Teach Digital Citizenship, Common Sense Education.
248. Libro de ejercicios sobre seguridad en línea: Trabaja con Sango, Unión Internacional de Telecomunicaciones.
249. Libro de ejercicios sobre seguridad en línea: Guía del profesor, Unión Internacional de Telecomunicaciones.
250. «Digiworld» de la UIT: Un ejemplo de aplicación práctica de las directrices de la UIT sobre la protección de la infancia en línea, Unión Internacional de Telecomunicaciones, 2020.
251. Teaching Toolkit, Childnet.
252. Teaching online safety in school (Enseñar seguridad en línea en la escuela), Department for Education, 2019.
253. Actividades de EndOCSEA@Europe: «Kiko's exciting adventures continue in the digital age», Consejo de Europa, 2020.

8. **Campaña «WebFighter», Sri Lanka**[254]
   Este sitio web ofrece orientación y herramientas útiles para cuidadores y educadores en relación con la seguridad de de niños y jóvenes. Ofrece ejemplos de talleres de protección infantil, talleres de salud mental y de bienestar, normas de reclutamiento seguro, etc.

9. **Programa «Swipe Safe»**[255]
   El programa «Swipe Safe» ayuda a los jóvenes a navegar por Internet de forma segura. Los educa sobre los riesgos potenciales, como las estafas cibernéticas, el acoso escolar o el abuso sexual, y les ofrece estrategias para protegerse. Organizaciones no gubernamentales de Vietnam, Laos y Myanmar han adaptado el plan de estudios. «Swipe Safe» interpela a padres, jóvenes, colegios y al sector privado para que desempeñen un papel activo respecto a la seguridad infantil en Internet. El programa ofrece formación a propietarios y gerentes de cibercafés para que identifiquen y aborden los riesgos y las posibles situaciones adversas que puedan afectar a los niños dentro y fuera de Internet. También brinda apoyo a los colegios para diseñar políticas y directrices sobre la seguridad en Internet adaptadas a los niños.

10. **Paquete de cultura digital (DLP)**[256]
    El «Paquete de cultura digital» de Ghana, auspiciado por UNICEF, se ha desarrollado para enseñar a los niños habilidades de cultura digital y garantizar su seguridad y su resiliencia en Internet. También contiene material dirigido a los padres/cuidadores para que puedan ayudar a los alumnos a navegar con seguridad por Internet, especialmente en tiempos del COVID-19, ya que la educación a distancia se ha convertido en algo habitual.

254. Goethe Institut.
255. «Swipe Safe» de ChildFund, ChildFund Alliance, 2019.
256. Paquete de cultura digital (DLP), UNICEF, 2021.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

> **Los Estados parte deben difundir información y llevar a cabo campañas de sensibilización en relación a los derechos de los niños en el entorno digital. Sobre todo, deben centrarse en aquello que tenga un impacto directo o indirecto en los niños. Deben facilitar programas educativos para niños, padres y cuidadores, para el público en general y para los responsables de la formulación de políticas, a fin de ampliar los conocimientos de todos respecto a los derechos del niño y en relación a las oportunidades y los riesgos asociados con los productos y los servicios digitales. Dichos programas deben incluir información sobre cómo los niños pueden beneficiarse de los productos y de los servicios digitales, cómo desarrollar su cultura y sus habilidades digitales, cómo proteger la privacidad de los niños y prevenir la victimización y cómo identificar a aquellos niños que son víctima de abusos dentro o fuera de Internet (y reaccionar de una manera adecuada). Esos programas deben basarse en investigaciones y en consultas con los niños, los padres y los cuidadores.**
>
> Fuente: Observación general núm. 25 (2021), párr. 32[257]

Objetivo:

Concienciar sobre todos los problemas relativos a la seguridad infantil en Internet, en todos los sectores de la comunidad, con el fin de prevenir posibles perjuicios y para promover un uso positivo de Internet. Esta información tendrá toda la difusión posible y habrá programas específicos para diferentes públicos.

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

8a. Crear un programa de concientización pública

Las estrategias de sensibilización ayudarán a la gente a comprender y a abordar la cuestión de la seguridad infantil en Internet para que puedan seguir disfrutando de las ventajas del espacio digital. El material que se diseñe debe dejar claros los principios de la seguridad infantil en Internet y las medidas que se pueden tomar para comprender los riesgos, mitigar los daños, denunciar los delitos y corregir/reparar, de ser necesario. Esta información se facilitará en los sitios web oficiales y en términos sencillos. El material y los mensajes específicos deben desarrollarse previa consulta con los niños, los jóvenes y los padres/cuidadores. Se deben tener en cuenta las necesidades específicas de los padres/cuidadores y de los niños, con especial atención para los niños más pequeños y vulnerables, incluidos los que tienen dificultades de aprendizaje o los que no cuentan con orientación parental. La educación entre pares es una estrategia valiosa para que los niños de todas las edades conozcan sus derechos y sus responsabilidades en Internet. Este programa de mensajes públicos puede ayudar a los niños y a los adultos a comprender los problemas y a tomar decisiones acertadas en sus interacciones en Internet, pero no sustituye la educación formal, la formación profesional, la seguridad por diseño ni la responsabilidad corporativa. Dicha información debe abarcar todo el abanico de problemas de la seguridad infantil en Internet, tal y como se establece en esta política.

257. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

Las cinco cuestiones transversales

1. Identificar riesgos y mitigar daños
2. Promover el acceso, la accesibilidad y la inclusión
3. Crear una cadena de responsabilidad y de colaboración
4. Integrar un diseño orientado a los niños
5. Garantizar la eficacia

Las diez áreas de acción de la política

1. Capacidad institucional
2. Marcos jurídicos y reguladores
3. Datos personales, identidad y autonomía
4. Sistemas de respuesta y de apoyo
5. Responsabilidad corporativa
6. Formación
7. Educación
8. Sensibilización del público y comunicación
9. Investigación y desarrollo
10. Cooperación global

8b. Proporcionar información y materiales educativos accesibles

La educación sobre seguridad en Internet comenzará en la primera infancia y se desarrollará de acuerdo con las necesidades cambiantes de los niños a medida que crecen. Se creará material específico para guiar y apoyar a los niños de todas las edades, así como a sus familias y cuidadores. El material de información promoverá el uso positivo de la tecnología digital y tocará cuestiones como la sexualidad y el consentimiento. Asimismo, se tendrán en cuenta las necesidades de todos los niños, independientemente de su género, su edad, su nivel económico o su contexto sociocultural. La información que se proporcione a través de terceros reflejará los derechos y los principios de los niños y tendrá como objetivo ayudar a los niños de todas las edades a conocer los riesgos que corren y sus derechos en Internet. El material debe dejar claro que los niños y los usuarios no son responsables cuando les suceden cosas malas.
Los grupos comunitarios, los clubes juveniles, las familias, las instituciones religiosas y las plataformas digitales desempeñarán un papel decisivo en la sensibilización sobre la seguridad infantil en Internet y en la educación informal a nivel comunitario.

8c. Sensibilizar sobre la seguridad infantil en Internet a través de los medios de comunicación

Debe facilitarse información adaptada para los niños que complemente la cobertura mediática de los problemas de seguridad infantil en Internet. Las empresas de comunicación y de entretenimiento deben estar familiarizadas con la cuestión de la seguridad infantil en Internet y se les debe alentar a apoyar campañas de sensibilización pública, cuando proceda, de una manera equilibrada, responsable e informativa. Debe darse cobertura a todo el abanico de cuestiones relacionadas con la seguridad infantil en Internet, no solo a los titulares más sensacionalistas.

8d. Involucrar a padres/cuidadores y a niños en diálogos sobre la seguridad infantil en Internet

Los padres/cuidadores y las familias deben estar capacitados para comprender lo que implica la seguridad infantil en Internet y para tomar medidas al respecto en casa. Es necesario hablar con las familias y con los niños para identificar los problemas, las soluciones y la manera de concienciar de manera efectiva respecto a la seguridad infantil en Internet en sus comunidades.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

Hoja de ruta para hacer efectivas las políticas:

A **Crear un programa de concientización pública**

Las estrategias de sensibilización ayudarán a la gente a comprender y a abordar la cuestión de la seguridad infantil en Internet para que puedan seguir disfrutando de las ventajas del espacio digital. El material que se diseñe debe dejar claros los principios de la seguridad infantil en Internet y las medidas que se pueden tomar para comprender los riesgos, mitigar los daños, denunciar los delitos y corregir/reparar, de ser necesario. Esta información se facilitará en los sitios web oficiales y en términos sencillos.

El material y los mensajes específicos deben desarrollarse previa consulta con los niños, los jóvenes y los padres/cuidadores y tendrán en cuenta las necesidades específicas de los padres/cuidadores y de los niños, con especial atención a los niños más pequeños y vulnerables, incluidos aquellos con dificultades de aprendizaje o que no cuenten con orientación parental. La educación entre pares es una estrategia valiosa para que los niños de todas las edades conozcan sus derechos y sus responsabilidades en Internet. Este programa de mensajes públicos puede ayudar a los niños y a los adultos a comprender los problemas y a tomar decisiones acertadas en sus interacciones en Internet, pero no sustituye la educación formal, la formación profesional, la seguridad por diseño ni la responsabilidad corporativa. Dicha información debe abarcar todo el abanico de problemas de la seguridad infantil en Internet, tal y como se establece en esta política.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar al público relevante y consultarle respecto a sus percepciones y sus dudas.
2. Identificar los mensajes más importantes que se pretenden transmitir a cada público. Véase «Herramienta de apoyo» 1.
3. Valorar cómo puede el mensaje fomentar la seguridad en el uso de los recursos digitales, en lugar de simplemente generar inquietud o crear ansiedad.
4. Garantizar que el mensaje no sea discriminatorio. Por ejemplo, no hay que sugerir que las niñas no deberían estar en Internet o que tener amistad en Internet con personas de otros entornos socioculturales es peligroso.
5. Trabajar con niños y padres/cuidadores para desarrollar los mensajes y probar su eficacia.
6. Valorar ejemplos de cómo públicos diferentes requieren mensajes diferentes.[258]

258. Véase, por ejemplo, la «Política de protección infantil en Ruanda», 5Rights Foundation, 2019.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

B **Proporcionar información y materiales educativos accesibles**

La educación sobre seguridad en Internet comenzará en la primera infancia y se desarrollará de acuerdo con las necesidades cambiantes de los niños a medida que crecen. Se creará material específico para guiar y apoyar a los niños de todas las edades, así como a sus familias y cuidadores. El material de información promoverá el uso positivo de la tecnología digital. Asimismo, se tendrán en cuenta las necesidades de todos los niños, independientemente de su género, su edad, su nivel económico o su contexto sociocultural. La información que se proporcione a través de terceros reflejará los derechos y los principios de los niños y tendrá como objetivo ayudar a los niños de todas las edades a conocer sus derechos en Internet. El material debe dejar claro que los niños y los usuarios no son responsables cuando les suceden cosas malas. Los grupos comunitarios, los clubes juveniles, las familias, las instituciones religiosas y las plataformas digitales desempeñarán un papel decisivo en la sensibilización sobre la seguridad infantil en Internet y en la educación informal a nivel comunitario.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar al público relevante.
2. Identificar los mensajes más importantes que se pretenden transmitir a cada público.
3. Valorar cómo puede el mensaje fomentar la seguridad en el uso de los recursos digitales, en lugar de simplemente generar inquietud o crear ansiedad.
4. Garantizar que el mensaje no sea discriminatorio. Por ejemplo, no hay que sugerir que las niñas no deberían estar en Internet o que tener amistad en Internet con personas de otros entornos socioculturales es peligroso.
5. Buscar ejemplos de diferentes audiencias y mensajes.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

C **Sensibilizar sobre la seguridad infantil en Internet a través de los medios de comunicación**

Debe facilitarse información adaptada para los niños que complemente la cobertura mediática de los problemas de seguridad infantil en Internet. Las empresas de comunicación y de entretenimiento deben estar familiarizadas con la cuestión de la seguridad infantil en Internet y se les debe alentar a apoyar campañas de sensibilización pública, cuando proceda, de una manera equilibrada, responsable e informativa. Debe darse cobertura a todo el abanico de cuestiones relacionadas con la seguridad infantil en Internet, no solo a los titulares más sensacionalistas.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Garantizar que el ministerio pertinente y el comité directivo diseñen mensajes relevantes e indicadores clave de rendimiento basados en el «Kit de herramientas para la seguridad de niñas, niños y adolescentes en Internet».
2. Hacer que los medios de comunicación tomen conciencia de estas cuestiones y las comprendan y aplicar la comprensión y la sensibilidad al lenguaje. Cuando los recursos lo permitan, sería conveniente realizar un trabajo de formación de los medios de comunicación.
3. Garantizar que estos mensajes se compartan tanto con los medios de comunicación convencionales como con los especializados, fomentar la aceptación por parte del público y garantizar la transparencia de la hoja de ruta, incluidos tanto los éxitos como cualquier retraso o complicación.
4. Conseguir que las partes interesadas relevantes y los líderes políticos estén dispuestos a promover todo lo que abarca la hoja de ruta de seguridad infantil en Internet y a comprometerse con ella.[259]

259. Política de protección infantil en Ruanda, 5Rights Foundation, 2019.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

D **Involucrar a padres/cuidadores y a niños en diálogos sobre la seguridad infantil en Internet**

Los padres/cuidadores y las familias deben estar capacitados para comprender lo que implica la seguridad infantil en Internet y para tomar medidas al respecto en casa. Es necesario hablar con las familias y con los niños para identificar los problemas y la manera de concienciar de manera efectiva respecto a la seguridad infantil en Internet en sus comunidades.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar los departamentos gubernamentales, las ONG y a los profesionales que trabajan o hablan directamente con los niños, las familias y los cuidadores.
2. Propiciar que se comprometan con la hoja de ruta y que comprendan todo lo que abarca y las posibilidades que ofrece.
3. Incorporar el sentir de los niños y los padres/cuidadores en las informaciones o el material de la política.
4. Ofrecer mensajes relevantes dirigidos a las familias y a los cuidadores que apelen a sus inquietudes pero que, además, amplíen sus conocimientos de la esfera digital. Contar con el sentir de los niños a la hora de dirigirse directamente a los padres/cuidadores.[260]

260. Nuestros derechos en un mundo digital, 5Rights Foundation, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

Cómo encaja esto con los documentos fundacionales:

> **La variedad de los objetivos de los ataques cibernéticos está aumentando con rapidez. Los nuevos usuarios de Internet no suelen estar muy al tanto en cuanto a «higiene digital» se refiere. Hoy por hoy, más de la mitad de los ataques se dirigen a «cosas» del «Internet de las cosas», que lo conecta todo: televisores inteligentes, monitores de bebé, termostatos, etc. Las redes 5G de alta velocidad integrarán aún más Internet en las infraestructuras físicas, lo cual provocará nuevas vulnerabilidades.**
>
> Fuente: The Age of Digital Interdependence: Report of the UN Secretary-General 's High-Level Panel on Digital Cooperation 2019 (Informe del Panel de Alto Nivel sobre Cooperación Digital del secretario general de las Naciones Unidas, 2019)[261]

> **Los Estados parte deben velar por que la cultura digital se imparta en los colegios como parte de los programas de enseñanza básica, desde el nivel de preescolar hasta el resto de cursos. Asimismo, dichas pedagogías deben evaluarse sobre la base de sus resultados. Los planes de estudio deben incluir las aptitudes y los conocimientos necesarios para manejar con seguridad una amplia gama de herramientas y de recursos digitales, incluidos los relacionados con los contenidos, la creación, la colaboración, la participación, la socialización y la participación ciudadana. Los planes de estudio también deben incluir la comprensión crítica, la orientación sobre cómo encontrar fuentes de información fiables e identificar las informaciones erróneas u otras formas de contenido sesgado o falso, incluidas cuestiones de salud sexual y reproductiva, derechos humanos —incluidos los derechos del niño en el entorno digital— y sobre las medidas de apoyo y reparación disponibles. Deben promover la concienciación entre los niños respecto a las posibles consecuencias adversas de la exposición a riesgos relacionados con los contenidos, el contacto con otras personas, la conducta y los contratos —incluidos el abuso y la explotación sexual, la ciberagresión, la trata y otras formas de violencia—, así como estrategias para hacer frente a los posibles perjuicios y estrategias para proteger sus datos personales y los de los demás y para desarrollar las habilidades sociales y emocionales y la resiliencia de los niños.**
>
> Fuente: Observación general núm. 25 (2021), párr. 104[262]

261. The Age of Digital Interdependence, Panel de Alto Nivel sobre Cooperación Digital del secretario general de las Naciones Unidas, 2019.
262. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

Herramientas de apoyo:

1. Lista de verificación para garantizar que el programa de concientización sea integral

El proceso A («Generar un programa de sensibilización pública») requiere el desarrollo de un programa de sensibilización general que pueda dirigirse a públicos muy específicos. Esta herramienta se ha diseñado para ayudarle a garantizar que se cumplan estos requisitos.

Grupo/público	Mensaje principal para llegar a ellos
Niños menores de 12 años	
Niños y jóvenes de 12 a 18 años	
Niños vulnerables: - En acogida - Con necesidades especiales - Con barreras lingüísticas - Involucrados en asuntos penales - Los que están al margen del sistema educativo convencional	
Familias con problemas de accesibilidad	
Familias rurales y o que viven en zonas aisladas	

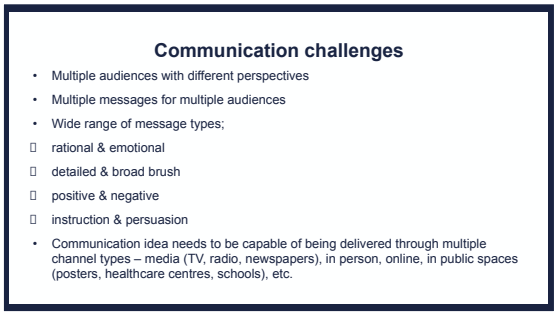
< SECCIÓN ANTERIOR

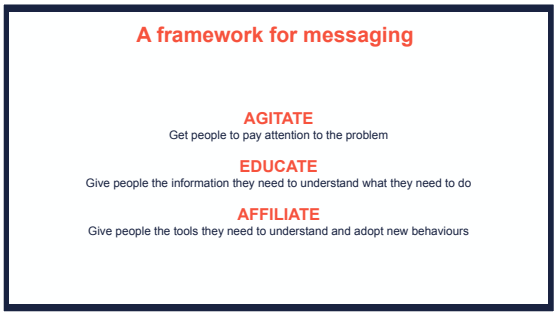
SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

Otros recursos de referencia:

1. **Protección infantil en Internet en Ruanda: Comunicaciones sobre la protección de los niños en Internet**[263]
   En nombre del Gobierno de Rwanda, la 5Rights Foundation preparó algunos contenidos de comunicación como parte de la aplicación de su política de seguridad infantil en Internet.



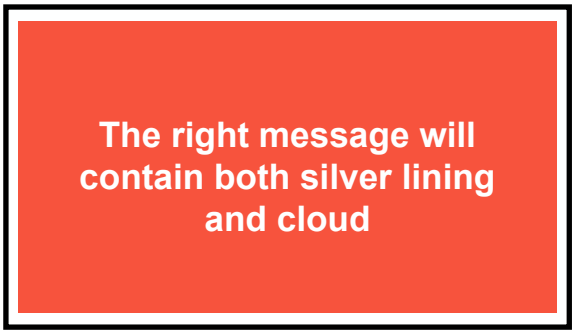


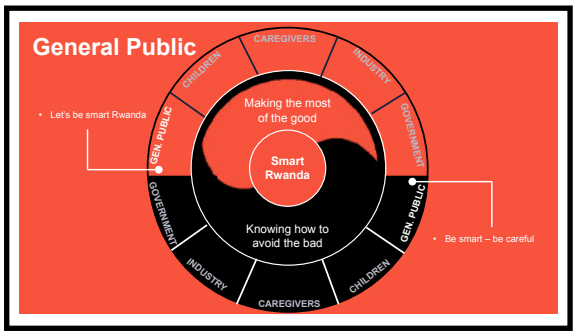
263. Child Online Protection in Rwanda, 5Rights Foundation, 2019.

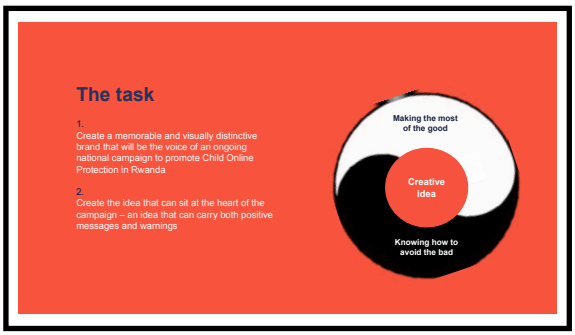
< SECCIÓN ANTERIOR

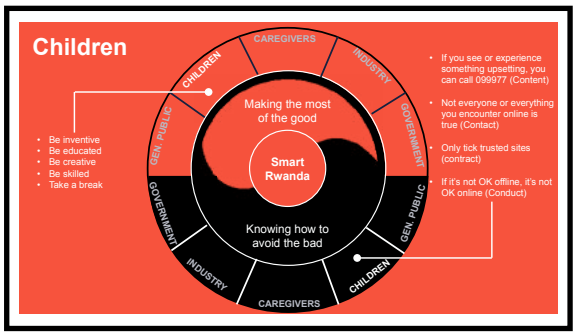
SIGUIENTE SECCIÓN >

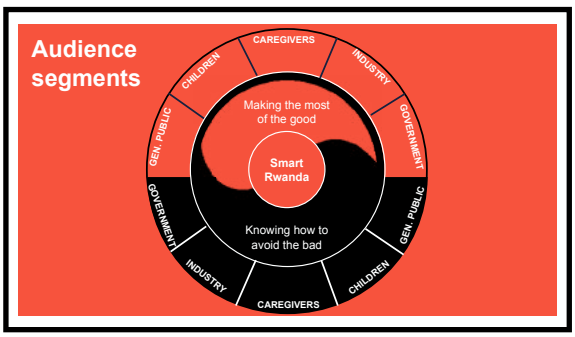
8 Sensibilización del público y comunicación

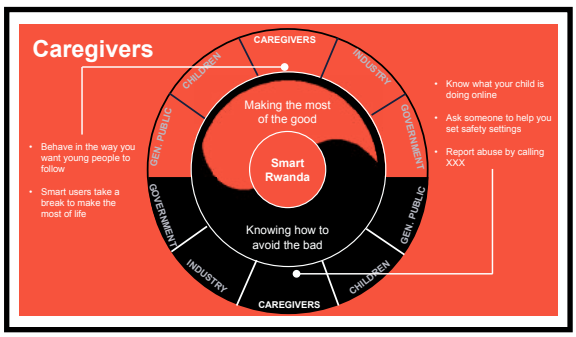








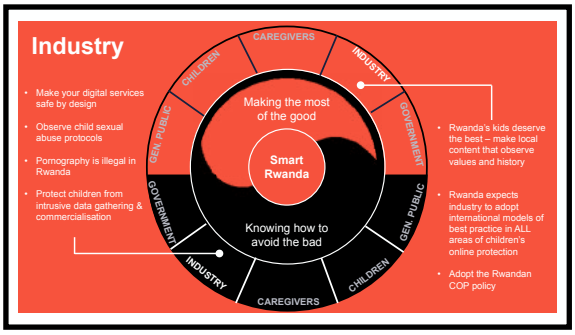


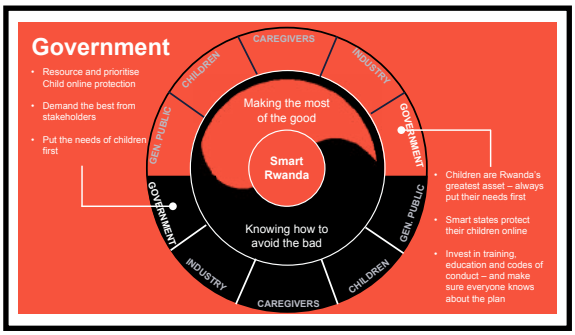


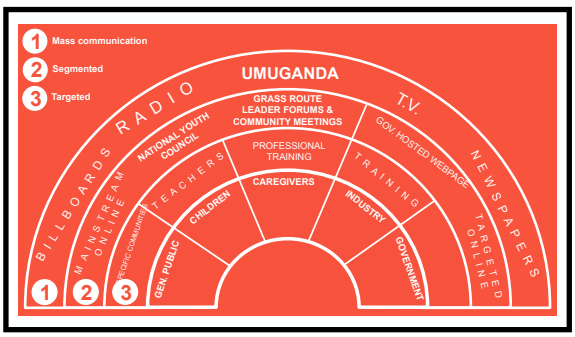
< SECCIÓN ANTERIOR

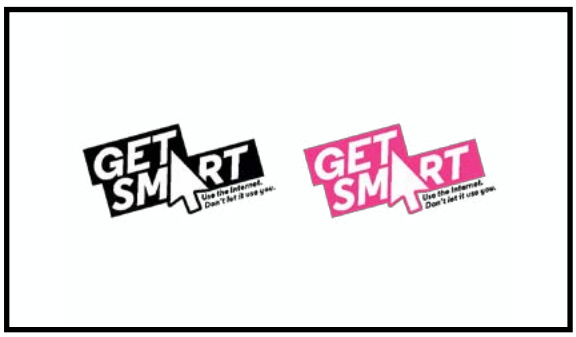
SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

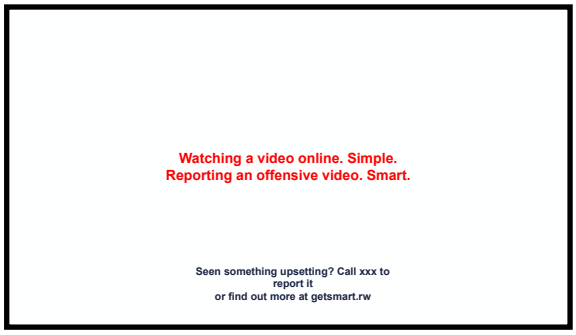








8 Sensibilización del público y comunicación



2. **Campaña «Twisted Toys» de la 5Rights Foundation**[264]
   Con esta campaña, lanzada por la 5Rights Foundation, se pretendía sensibilizar sobre cualquier tipo de vigilancia y sobre el peligro que los niños podrían correr al explorar el mundo digital.

3. **Semana Mundial de la Alfabetización Mediática e Informacional de la UNESCO**[265]
   La Semana Mundial de la Alfabetización Mediática e Informacional es un evento anual en el que se evalúa el progreso en términos de alfabetización mediática e informativa para el público.

4. **Herramientas globales para padres del comisionado australiano de Seguridad Electrónica**[266]
   Este documento, preparado por la Oficina del Comisionado de Seguridad Digital de Australia, proporciona orientación a los cuidadores y a los padres para ayudarles a proteger a los niños en Internet.

5. **Manual de paternidad digital del Consejo de Europa**[267]
   Este manual, preparado por el Consejo de Europa, proporciona orientación a los cuidadores y a los padres para garantizar la seguridad infantil en Internet, y en concreto para protegerlos de la explotación y el abuso sexuales.

6. **Objetivos para el Día de «Internet más seguro» en África, 2021, con la mascota Sango**[268]
   Con la idea de crear un mundo en el que los niños puedan conectarse a Internet y beneficiarse plenamente de las oportunidades de un entorno digital de confianza y seguro, la UIT ha esbozado los siguientes objetivos para África:

   - ☐ Promover la educación y la sensibilización en toda África sobre la importancia de la seguridad infantil en Internet.
   - ☐ Sensibilizar a los Gobiernos, la industria, los educadores, los niños y los padres para garantizar que los niños africanos estén seguros y protegidos cuando navegan por Internet.
   - ☐ Diseñar estrategias para empoderar y apoyar el desarrollo de la resiliencia de los niños africanos.
   - ☐ Desarrollar, compartir o contextualizar los recursos disponibles para apoyar el aprendizaje y la educación de los niños.

264. Twisted Toys, 5Rights Foundation, 2021.
265. Semana Mundial de la Alfabetización Mediática e Informacional, Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2021.
266. Global Online Safety Advice for Parents and Carers (Asesoramiento global de seguridad digital para padres y cuidadores) , Comisionado de Seguridad Electrónica de Australia, 2020.
267. Parenting in the Digital Age (Paternidad en la era digital), Consejo de Europa, 2017.
268. Positioning and Partnering for Child Online Protection (Posicionamiento y asociación para la protección digital infantil), Oficina Regional para África de la Unión Internacional de Telecomunicaciones (UIT), 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

8 Sensibilización del público y comunicación

7. **Estudio de caso: Ministerio de Tecnologías de la Información y Comunicaciones de Colombia**[269]
El Ministerio de Tecnologías de la Información y Comunicaciones de Colombia promueve el desarrollo de habilidades digitales para enfrentar con confianza los riesgos asociados al uso de Internet y de las TIC.

   Público objetivo:

   - ☐ De 6 a 18 años
   - ☐ Ámbito académico, 11 a 28 años
   - ☐ Adultos mayores de 28 años

   Cuentan con un sitio web que proporciona enlaces a «preguntas frecuentes», recursos educativos y de formación e información accesible sobre el mundo digital.

8. **Curso de aprendizaje electrónico: Medidas para poner fin a la explotación y al abuso sexuales de los niños**[270]
«Medidas para poner fin a la explotación y al abuso sexuales de los niños» es un curso de aprendizaje electrónico diseñado para ganar en sensibilización y en conocimientos respecto sobre la explotación y el abuso sexuales de los niños —incluidos los abusos que propician las tecnologías— y promover estrategias y acciones a partir de evidencias para la prevención y la respuesta. El curso abarca políticas, promoción y un amplio abanico de aspectos programáticos. La revisión y el curso de aprendizaje electrónico se han preparado con el apoyo financiero del End Violence Fund.

9. **WeProtect Global Alliance: Cómo hablar sobre el abuso sexual infantil en el mundo digital**[271]
Este informe estratégico describe los desafíos a la hora de hablar en los medios sobre la explotación y el abuso sexual infantil en Internet. Ofrece recomendaciones preliminares para los comunicadores.

269. En TIC confío+, Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, 2021.
270. Action to End Child Sexual Exploitation and Abuse (Acciones para acabar con la explotación y el abuso sexual infantil), UNICEF, 2022.
271. How to talk about child sexual abuse in the digital world (Cómo hablar sobre abuso sexual infantil en el mundo digital), Alianza Mundial WeProtect, 2021.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

> **Es fundamental actualizar los datos y las investigaciones de forma periódica para entender las repercusiones del entorno digital en la vida de los niños y para evaluar el impacto en sus derechos y la eficacia de las intervenciones del Estado. Los Estados parte deben velar por que se recopilen datos sólidos y exhaustivos que cuenten con recursos suficientes y que estén desglosados por edad, sexo, tipo de discapacidad, ubicación geográfica, origen étnico y nacional y contexto socioeconómico. Esos datos y esas investigaciones —incluidas las realizadas con y por niños— deben servir de base para la legislación, las políticas y la práctica y deben ser de dominio público. La recopilación de datos y la investigación relacionada con la vida digital de los niños deben respetar su privacidad y cumplir con los más altos estándares éticos.**
>
> Fuente: Observación general núm. 25 (2021), párr. 30[272]

Objetivo:

Para garantizar un enfoque holístico y actualizado de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

Texto del modelo de política:

Establecer y financiar marcos de trabajo nacionales y regionales para la investigación y el desarrollo de la seguridad infantil en Internet que sean eficaces y de acceso público para así apoyar el desarrollo y la implementación de políticas de seguridad infantil en Internet.

9a. Establecer marcos de trabajo para la investigación de la seguridad infantil en Internet
Los países deben establecer un fondo central de investigación para desarrollar un programa de investigación con términos de referencia y objetivos claramente definidos que no queden obsoletos, a fin de facilitar las investigaciones en curso sobre la seguridad infantil en Internet en relación con diversas cuestiones de relevancia. Siempre que sea posible, los países deben ponerse en contacto y cooperar entre sí en la investigación y el desarrollo de la seguridad infantil en Internet. El análisis de las carencias debería ayudar a garantizar que se dé prioridad a los recursos de las áreas con mayores necesidades y a evitar duplicaciones innecesarias. La investigación debe ponerse a disposición de los colaboradores regionales o internacionales, en particular los que cuentan con menos recursos.

9b. Innovación continua
Las evidencias que se extraigan de las investigaciones servirán de referencia para el desarrollo de productos y servicios que incorporen la seguridad por diseño. Asimismo, facilitarán la evaluación de las prácticas de seguridad infantil en Internet y proporcionarán una comprensión de las experiencias y de las soluciones relativas al uso de Internet por parte de los niños en el contexto nacional.

9c. Establecer centros de excelencia en investigación y desarrollo de la seguridad infantil en Internet
Los países deben desarrollar centros de excelencia dentro de las instituciones existentes —universidades, centros sanitarios, centros de innovación— que puedan trabajar juntos en el desarrollo de herramientas, servicios y habilidades relacionadas con la seguridad infantil en Internet a través de la participación nacional, regional e internacional. ▶

272. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

9d. Establecer marcos de trabajo éticos y sólidos para la investigación y el desarrollo en materia de seguridad infantil en Internet[273]
Los países deben desarrollar directrices para los investigadores que trabajan en el ámbito de la seguridad infantil en Internet, lo que incluye tener en cuenta los derechos de los niños de una manera efectiva como parte del proceso de investigación. Debe incluirse una orientación clara sobre la recopilación de datos y las implicaciones éticas, y respecto a los derechos, del procesamiento de los datos de los niños. Los intereses del niño deben ser la consideración principal de los marcos de trabajo éticos para la investigación y el desarrollo sobre la seguridad infantil en Internet, incluidos los escenarios en los que el acceso sea una cuestión de interés público.

9e. Establecer marcos de trabajo para la recopilación de información
Los reguladores que trabajan en el ámbito de la seguridad infantil en Internet deben establecer marcos de trabajo para la recopilación de información que les permitan supervisar y evaluar la efectividad de la seguridad infantil en Internet en diferentes contextos y el impacto que tiene en diferentes grupos de niños. La supervisión y la evaluación de las medidas relacionadas con la seguridad infantil en Internet deben formar parte del proceso de investigación y desarrollo.

9f. Permitir el acceso a los datos de las empresas privadas por el bien del interés general
Se deben crear marcos de trabajo en los que las redes sociales y otras empresas estén obligadas a compartir sus datos para respaldar las investigaciones que se realizan en el interés superior del niño.

9g. Garantizar que los datos y las estadísticas se ajusten al contexto
Los modelos estadísticos deben reflejar el panorama local, para propiciar una mejora en la comprensión de las cuestiones locales y en la respuesta a las mismas. Deben facilitar, además, el seguimiento de los efectos transfronterizos.

273. Children and the Data Cycle: Rights and Ethics in a Big Data World (Niños y el ciclo de los datos: derechos y ética en el mundo del Big Data), Fondo de las Naciones Unidas para la Infancia, 2017.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

Hoja de ruta para hacer efectivas las políticas:

A **Establecer marcos de trabajo para la investigación de la seguridad infantil en Internet**

Los países deben establecer un fondo central de investigación para desarrollar un programa de investigación con términos de referencia y objetivos claramente definidos que no queden obsoletos, a fin de facilitar las investigaciones en curso sobre la seguridad infantil en Internet en relación con diversas cuestiones de relevancia. Siempre que sea posible, los países deben ponerse en contacto y cooperar entre sí en la investigación y el desarrollo de la seguridad infantil en Internet. El análisis de las carencias debería ayudar a garantizar que se dé prioridad a los recursos de las áreas con mayores necesidades y a evitar duplicaciones innecesarias. La investigación debe ponerse a disposición de los colaboradores regionales o internacionales, en particular los que cuentan con menos recursos.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar los fondos o instituciones de investigación existentes que podrían albergar o financiar la investigación sobre la seguridad infantil en Internet.
2. Identificar el área de investigación necesaria.
3. Establecer criterios estrictos para garantizar que la investigación contribuya a los conocimientos, la seguridad y el bienestar de los niños.
4. Garantizar que los investigadores conozcan todos los aspectos de la hoja de ruta de la política y que no se concentren en un solo ámbito.
5. Propiciar que toda la financiación de la investigación dependa del amplio intercambio de resultados, incluida la retención de los resultados de la investigación en un repositorio central y la disposición de fondos para la difusión y la adopción de políticas.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

B **Innovación continua**

Las evidencias que se extraigan de las investigaciones servirán de referencia para el desarrollo de productos y servicios que incorporen la seguridad por diseño. Asimismo, facilitarán la evaluación de las prácticas de seguridad infantil en Internet y proporcionarán una comprensión de las experiencias relativas al uso de Internet por parte de los niños en el contexto nacional.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Realizar un seguimiento de los cambios —a nivel mundial— en los productos y en los servicios y compartirlos de forma amplia para garantizar que los avances realizados en materia de seguridad infantil en Internet en un sitio concreto estén disponibles en otras partes del mundo.
2. Señalar dónde se han logrado avances e involucrar a las ONG internacionales o a grupos de expertos en su difusión.
3. Aprovechar los acuerdos con organizaciones intergubernamentales, empresas privadas y ONG para difundir las prácticas recomendadas. Por ejemplo, condicionar una donación de hardware informático a la incorporación por defecto de características de seguridad y privacidad.

C **Establecer centros de excelencia en investigación y desarrollo de la seguridad infantil en Internet**[274]

Los países deben desarrollar centros de seguridad infantil en Internet que puedan trabajar conjuntamente en el desarrollo de habilidades, herramientas y servicios relacionados con la seguridad infantil en Internet a través de la participación nacional, regional e internacional.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Albergar centros de seguridad infantil en Internet en los departamentos gubernamentales o en las instituciones académicas existentes.
2. Valorar la posibilidad de establecer centros de seguridad infantil en Internet en todas las regiones con requisitos culturales y organizativos similares de cara a compartir las prácticas recomendadas.

274. La seguridad de los niños en línea: retos y estrategias, Fondo de las Naciones Unidas para la Infancia, 2011.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

D **Establecer marcos de trabajo éticos y sólidos para la investigación y el desarrollo en materia de seguridad infantil en Internet**[275]

Los países deben desarrollar directrices para los investigadores que trabajan en el ámbito de la seguridad infantil en Internet, lo que incluye tener en cuenta los derechos de los niños de una manera efectiva como parte del proceso de investigación. Debe incluirse una orientación clara sobre la recopilación de datos y las implicaciones éticas, y respecto a los derechos, del procesamiento de los datos de los niños. Los intereses del niño deben ser la consideración principal de los marcos de trabajo éticos para la investigación y el desarrollo sobre la seguridad infantil en Internet, incluso en los escenarios en los que el acceso sea una cuestión de interés público.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Establecer normas básicas para una investigación responsable (véase «Recursos» a continuación; por ejemplo, «Directrices de ECPAT»).
2. Garantizar que las normas se incorporen a la financiación o a la aceptación de los resultados de la investigación. Véase «Herramientas de apoyo» 1 (página 156).
3. Garantizar que sea obligatoria para los investigadores la formación en materia de seguridad infantil en Internet (véanse las referencias a la formación del «Área de acción de la política», página 144).

E **Establecer marcos de trabajo para la recopilación de información**

Los reguladores que trabajan en el ámbito de la seguridad infantil en Internet deben establecer marcos de trabajo para la recopilación de información que les permitan supervisar y evaluar la efectividad de la seguridad infantil en Internet en diferentes contextos y el impacto que tiene en diferentes grupos de niños. La supervisión y la evaluación de las medidas relacionadas con la seguridad infantil en Internet deben formar parte del proceso de investigación y desarrollo.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente garantizar que se les exijan a los reguladores marcos de trabajo de recopilación de información para una mejor comprensión de los datos utilizados, los métodos y los resultados. Cualquier requisito legal o reglamentario debe conllevar la presentación de informes, la transparencia y los poderes de recopilación de información. Ejemplos de ello son el GDPR[276] y el proyecto de ley de seguridad en línea del Reino Unido.[277]

275. Children and the Data Cycle: Rights and Ethics in a Big Data World (Niños y el ciclo de los datos: derechos y ética en el mundo del Big Data), Fondo de las Naciones Unidas para la Infancia, 2017.
276. Reglamento General de Protección de Datos, Unión Europea, 2018.
277. Proyecto de ley de seguridad en línea, Departamento de Tecnología, Cultura, Medios de Comunicación y Deporte, 2021.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

F **Permitir el acceso a los datos de las empresas privadas por el bien del interés general**

Se deben crear marcos de trabajo en los que las redes sociales y otras empresas estén obligadas a compartir sus datos para respaldar las investigaciones que se realizan en el interés superior del niño.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Llevar a cabo actividades de divulgación para empresas de redes sociales en el territorio pertinente y solicitando el acceso a conjuntos de datos cuando corresponda.
2. Participar en diálogos a nivel regional, nacional o mundial y realizar solicitudes similares.

G **Garantizar que los datos y las estadísticas se ajusten al contexto**

Los reguladores que trabajan en el ámbito de la seguridad infantil en Internet deben establecer marcos de trabajo para la recopilación de información que les permitan supervisar y evaluar la efectividad de la seguridad infantil en Internet en diferentes contextos y el impacto que tiene en diferentes grupos de niños. La supervisión y la evaluación de las medidas relacionadas con la seguridad infantil en Internet deben formar parte del proceso de investigación y desarrollo.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Buscar estadísticas que provengan de agencias bien documentadas y fiables.
2. Contactar con las partes interesadas de estas agencias para validar y confirmar sus estadísticas.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

Cómo encaja esto con los documentos fundacionales:

Modelo de respuesta nacional (competencia 2): Investigación, análisis y supervisión de las prácticas recomendadas para la aplicación de la ley:

Como mínimo, un análisis debe: evaluar la amenaza actual de explotación y abuso sexual de niños, cómo se manifiestan y quién corre mayor peligro; evaluar la vulnerabilidad del país a esta amenaza; evaluar la actual respuesta institucional; revisar y evaluar la aplicación de la legislación y de las políticas pertinentes para valorar el cumplimiento de las normas internacionales y de las prácticas recomendadas; revisar la respuesta actual del ecosistema de las TIC, incluidos los mecanismos de denuncia de la línea directa y la participación de la industria; y examinar la actividad de otras partes interesadas involucradas en este tema.

Para fundamentar un análisis, debe facilitarse el acceso a una amplia variedad de datos y de información relevante respecto a la explotación y el abuso sexual de niños que posean las organizaciones representadas en el organismo nacional o cualquier otra parte interesada pertinente. Además, los datos primarios deben recopilarse de diversas fuentes: niños, padres, educadores, fuerzas del orden, proveedores de servicios, etc.

Fuente: modelo de respuesta nacional (MNR) de la Alianza Mundial WeProtect, páginas 5-6[278]

278. Modelo de respuesta nacional, Alianza Mundial WeProtect, 2016.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

Herramientas de apoyo:

1. Lista de verificación de las consideraciones éticas de la investigación

El proceso D («Establecer marcos de trabajo éticos y sólidos para la investigación y el desarrollo en materia de seguridad infantil en Internet») expone la necesidad de aplicar un enfoque holístico a la ética de la investigación en la metodología, la financiación y la recopilación de datos. Esta lista de verificación está diseñada para ayudar a garantizar que los marcos de trabajo de la ética de la investigación aborden estas áreas.

¿La selección de la investigación para la financiación gubernamental tiene en cuenta la seguridad infantil en Internet?

En caso afirmativo, facilite más información:

En caso negativo, ¿cómo se abordará esta cuestión?

¿La financiación para la investigación incluye una evaluación de impacto en los niños o una revisión ética?

En caso afirmativo, facilite más información:

En caso negativo, ¿cómo se abordará esta cuestión?

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

¿Existe un marco de trabajo ético para los investigadores y los desarrolladores que incluya la perspectiva de los derechos de los niños?

En caso afirmativo, facilite más información:

En caso negativo, ¿cómo se abordará esta cuestión?

¿Los investigadores, los desarrolladores y los responsables de la toma de decisiones en relación a la financiación han recibido formación en seguridad infantil en Internet y en derechos de los niños?

En caso afirmativo, facilite más información:

En caso negativo, ¿cómo se abordará esta cuestión?

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

¿Se aplica a la investigación y el desarrollo el principio de cautela?

En caso afirmativo, facilite más información:

En caso negativo, ¿cómo se abordará esta cuestión?

¿Hay datos de código abierto disponibles para respaldar la investigación de la seguridad infantil en Internet?

En caso afirmativo, facilite más información:

En caso negativo, ¿cómo se abordará esta cuestión?

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

9 Investigación y desarrollo

Otros recursos de referencia:

1. **«Marco para una investigación y una innovación responsables en las TIC», Universidad de Oxford**[279]
   Financiado por el Consejo de Investigación de Ingeniería y Ciencias Físicas (EPSRC), este marco de trabajo explora cuestiones éticas relacionadas con la investigación de las TIC. Desarrollado por el Observatorio de la Investigación e Innovación Responsables en TIC (ORBIT), ofrece instrucciones claras sobre cómo llevar a cabo la investigación práctica y ética.

2. **Proyecto Disrupting Harm de End Violence**[280]
   En asociación con EPCAT International, la INTERPOL y la Oficina de Investigación de UNICEF, y con la financiación de End Violence, Disrupting Harm es un proyecto de investigación que expone cómo la tecnología digital propicia la explotación y el abuso sexuales de los niños en 13 países de África oriental y meridional y de Asia sudoriental.

3. **Directrices de la ECPAT para una investigación ética sobre la explotación sexual de los niños**[281]
   Una guía para los investigadores que pretenden realizar investigaciones sobre cuestiones relacionadas con la explotación y el abuso sexual de los niños, lo que plantea ciertas cuestiones y dilemas éticos. Estas directrices ayudan a los investigadores a dar forma a su proyecto de investigación de manera que se minimicen los perjuicios a los niños.

4. **Dictamen de la Agencia de Derechos Fundamentales de la UE**[282]
   Dictamen de la Agencia de Derechos Fundamentales, 9: Siempre que financien actividades de investigación y desarrollo, la UE y sus Estados miembros deben exigir a los contratistas la participación de expertos en protección de datos personales y otros derechos fundamentales. Los investigadores científicos y la industria deben prestar atención al efecto de las características fenotípicas, así como a la edad y el género, en la composición de los grupos de prueba para eliminar cualquier riesgo de resultados discriminatorios en las conclusiones de la prueba.

5. **«Enfoque de datos basados en derechos humanos», Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos**[283]
   Esta guía ofrece recomendaciones y principios para que las partes interesadas en relación con los datos y los responsables de la formulación de políticas mejoren su uso de los datos y las estadísticas. Garantiza el respeto, la protección y el cumplimiento de los derechos humanos sobre la base de la Agenda 2030, que se está adoptando al recopilar o desglosar datos.

279. A Framework for Responsible Research and Innovation in ICT (Un marco de trabajo para la investigación y la innovación responsables en TCI), Universidad de Oxford, 2014.
280. Disrupting Harm, End Violence Partnership, 2019.
281. Guidelines for ethical research on sexual exploitation involving children (Directrices para una investigación ética de la explotación sexual infantil), ECPAT International, 2019.
282. Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights (Bajo una mirada vigilante: biometría, sistemas TI de la UE y derechos fundamentales), Agencia de los Derechos Fundamentales de la Unión Europea, 2018.
283. Enfoque de datos basados en derechos humanos, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2018.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

10 Cooperación global

El carácter transfronterizo y transnacional del entorno digital exige una estrecha cooperación internacional y regional para garantizar que todas las partes interesadas, incluidos los Estados, las empresas y otros actores, respeten, protejan y hagan efectivos los derechos de los niños en relación con el entorno digital. Por consiguiente, es fundamental que los Estados parte cooperen bilateral y multilateralmente con las organizaciones no gubernamentales nacionales e internacionales, con los organismos de las Naciones Unidas, con las empresas y con las organizaciones especializadas en la protección de los niños y los derechos humanos en relación con el entorno digital.

Los Estados parte deben promover y colaborar en el intercambio internacional y regional de conocimientos especializados y de prácticas recomendadas y establecer y promover tanto el desarrollo de capacidades como los recursos, las normas, los reglamentos y la protección a través de las fronteras nacionales que permitan la comprensión de los derechos del niño en el entorno digital por parte de todos los Estados. Deben fomentar la formulación de una definición común de lo que constituye un delito en el entorno digital, la asistencia judicial recíproca y la recopilación conjunta y el intercambio de pruebas.

Fuente: Observación general núm. 25 (2021), párrs. 123 y 124[284]

Objetivo:

Colaborar con organizaciones y actores nacionales, regionales y globales para compartir las prácticas recomendadas.

Texto del modelo de política:

Para garantizar un enfoque holístico de la seguridad infantil en Internet, son necesarios cada uno de los siguientes pasos.

10a. Establecer marcos de trabajo formales de relación —por ejemplo, un «Memorando de entendimiento» (MOU)— con las comunidades regionales y globales de seguridad infantil en Internet
El fortalecimiento de la cooperación internacional a lo largo y ancho del planeta en la mejora de la seguridad infantil en Internet es fundamental para garantizar la seguridad a nivel global. Los países deben formalizar colaboraciones para inversiones conjuntas de asociaciones público-privadas en áreas relacionadas con, entre otras cuestiones, la ciberseguridad, el desarrollo de capacidades de seguridad infantil en Internet, la innovación, la aplicación de la ley, el sistema judicial y la educación.

10b. Adscribirse a los instrumentos jurídicos regionales e internacionales que promueven la cooperación en materia de seguridad infantil en Internet
Los países deben identificar instrumentos clave a nivel regional e internacional que les permitan cooperar con otros países en materia de seguridad infantil en Internet. Esto debería incluir, entre otras cosas, acuerdos internacionales sobre cooperación respecto a la aplicación de la ley, prácticas recomendadas a nivel internacional, programas internacionales que proporcionen recursos para la cooperación en materia de seguridad infantil en Internet y acceso a aquellas normas relacionadas con los derechos humanos, o similares, que faciliten la cooperación entre los países. ▶

284. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, CDN de las Naciones Unidas, 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

10 Cooperación global

10c. Identificar organizaciones y países colaboradores que puedan proporcionar los modelos y el apoyo adecuados para el desarrollo de la seguridad infantil en Internet
Puede que no haga falta desarrollar las políticas desde cero. Los países deben buscar ejemplos oportunos de marcos de trabajo y de herramientas de seguridad infantil en Internet que puedan utilizar y adaptar a su propio contexto. El intercambio de información sobre los desafíos y los problemas que se detecten en materia de seguridad infantil en Internet puede ser muy valioso para la planificación, el desarrollo y la aplicación de políticas de seguridad infantil en Internet.

10d. Apoyar a otros países en el desarrollo de políticas de seguridad infantil en Internet
Cuando corresponda, convendría compartir modelos de leyes y marcos regulatorios, así como los conocimientos fruto de la experiencia u otros materiales que puedan utilizar otros países para desarrollar sus marcos de trabajo y sus políticas de seguridad infantil en Internet.[285]

Hoja de ruta para hacer efectivas las políticas:

A **Establecer marcos de trabajo formales de relación —por ejemplo, un «Memorando de entendimiento» (MOU)— con las comunidades regionales y globales de seguridad infantil en Internet**

El fortalecimiento de la cooperación internacional a lo largo y ancho del planeta en la mejora de la seguridad de los niños en Internet es fundamental para garantizar la seguridad a nivel global. Los países deben formalizar colaboraciones para inversiones conjuntas de asociaciones público-privadas en áreas relacionadas con, entre otras cuestiones, la ciberseguridad, el desarrollo de capacidades de seguridad infantil en Internet, la innovación, la aplicación de la ley, el sistema judicial y la educación.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar los acuerdos y los tratados regionales y globales oportunos relativos a la seguridad infantil en Internet (consultar «Documentos clave»).
2. Añadir los pasos necesarios a la hoja de ruta de seguridad en línea en Internet y tomar las medidas pertinentes para adscribirse a ella.
3. Verificar que se incluyen, como mínimo, las acciones requeridas por:

- ☐ Los Objetivos de Desarrollo Sostenible.[286]
- ☐ La Convención sobre los Derechos del Niño y sus «Protocolos facultativos».[287]
- ☐ La «Observación general núm. 25» (2021) sobre los derechos del niño en relación con el entorno digital.[288]
- ☐ El Modelo de Respuesta Nacional.[289] Véase la «Herramienta de apoyo» 1 (página 166).

285. Véase, por ejemplo, International Leadership and Collaboration Materials (Liderazgo internacional y materiales de colaboración) del Comisionado de Seguridad Digital de Australia, 2021.
286. Transformar nuestro mundo: Agenda 2030 para el Desarrollo Sostenible, Naciones Unidas, 2021.
287. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
288. Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital, Comité de los Derechos del Niño de las Naciones Unidas, 2021.
289. Modelo de respuesta nacional, WeProtect, 2016.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

10 Cooperación global

B **Adscribirse a los instrumentos jurídicos regionales e internacionales que promueven la cooperación en materia de seguridad infantil en Internet**

Los países deben identificar instrumentos clave a nivel regional e internacional que les permitan cooperar con otros países en materia de seguridad infantil en Internet. Esto debería incluir, entre otras cosas, acuerdos internacionales sobre cooperación respecto a la aplicación de la ley, prácticas recomendadas a nivel internacional, programas internacionales que proporcionen recursos para la cooperación en materia de seguridad infantil en Internet y acceso a aquellas normas relacionadas con los derechos humanos, o similares, que faciliten la cooperación entre los países.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Consultar con organismos internacionales encargados de hacer cumplir la ley, como INTERPOL[290] y Europol.[291]
2. Consultar las prácticas recomendadas de organizaciones globales como el Centro Nacional para Niños Desaparecidos y Explotados[292] o la Internet Watch Foundation.[293]

290. Quiénes somos, INTERPOL.
291. Acerca de Europol, Europol.
292. Nuestro trabajo, Centro Nacional para Niños Desaparecidos y Explotados (NCMEC).
293. Acerca de nosotros, Internet Watch Foundation (IWF).

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

10 Cooperación global

C **Identificar organizaciones y países colaboradores que puedan proporcionar los modelos y el apoyo adecuados para el desarrollo de la seguridad infantil en Internet**

Puede que no haga falta desarrollar las políticas desde cero. Los países deben buscar ejemplos oportunos de marcos de trabajo y de herramientas de seguridad infantil en Internet que puedan utilizar y adaptar a su propio contexto. El intercambio de información sobre los desafíos y los problemas que se detecten en materia de seguridad infantil en Internet puede ser muy valioso para la planificación, el desarrollo y la aplicación de políticas de seguridad infantil en Internet.

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente contactar con organismos regionales, como la Coalición de Derechos del Niño de Asia,[294] con organizaciones líderes de los diferentes países, como la Fundación Alana en Brasil,[295] o con organizaciones de expertos como la Internet Watch Foundation,[296] la 5Rights Foundation,[297] UNICEF,[298] INHOPE[299] o la iniciativa «Safe Online» de la Alianza Mundial para Poner Fin a la Violencia contra los Niños.[300]Estas organizaciones contarán con recursos e información, y en muchos casos pueden ayudar a identificar colaboradores locales o de relevancia.

294. Acerca de nosotros, Child Rights Coalition Asia.
295. Sobre nosotros, Fundación Alana.
296. Acerca de nosotros, Internet Watch Foundation (IWF).
297. 5Rights Foundation, 5Rights Foundation.
298. Acerca de nosotros, UNICEF.
299. Nuestra historia, INHOPE, 2021.
300. Safe Online, End Violence Against Children, 2022.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

10 Cooperación global

D **Apoyar a otros países en el desarrollo de políticas de seguridad infantil en Internet**

Cuando corresponda, convendría compartir modelos de leyes y marcos regulatorios, así como los conocimientos fruto de la experiencia u otros materiales que puedan utilizar otros países para desarrollar sus marcos de trabajo y sus políticas de seguridad infantil en Internet.[301]

En caso afirmativo, facilite más información:

En caso negativo, sería conveniente:

1. Identificar a las organizaciones o a los ministerios pertinentes de la región.
2. Tener en cuenta las prácticas recomendadas de otras regiones, como por ejemplo las de la Asociación de Naciones del Sudeste Asiático (ASEAN) o las de la UE.
3. Compartir de forma generosa las soluciones y los recursos propios.
4. Estudiar cómo colaborar con aquellos con menos recursos.
5. Alentar a aquellos con los que se colabora a hacer lo mismo en el futuro.
6. Estar en línea con las prácticas recomendadas a nivel internacional y colaborar de forma proactiva con aquellos países con menos recursos (o facilitarles recursos). Por ejemplo, hermanarse con un país o una región en particular, brindar apoyo técnico —traducción legal o lingüística para partes de la hoja de ruta— u ofrecer talleres a los trabajadores que están en primera línea (incluidos los encargados de aplicar la ley).

Cómo encaja esto con los documentos fundacionales:

Recomendamos que, con carácter urgente, el secretario general de las Naciones Unidas ponga en marcha un proceso de consulta ágil y abierto con el que desarrollar mecanismos actualizados para la cooperación digital a nivel mundial, a partir de las opciones que se exponen en el capítulo 4. Sugerimos como objetivo inicial conmemorar el 75.º aniversario de la ONU en 2020 con un «Compromiso global para la cooperación digital» para consagrar los valores, los principios, los conocimientos y los objetivos compartidos de cara a una arquitectura de cooperación digital mejorada a nivel global. Como parte de este proceso, entendemos que el secretario general de las Naciones Unidas puede nombrar a un enviado tecnológico.

5B: Apoyamos un enfoque de «sistemas» de cooperación y de regulación con múltiples partes interesadas que sea adaptable, ágil, inclusivo y adecuado para una era digital en continuo cambio.

Fuente: The Age of Digital Interdependence (La era de la interdependencia digital), Informe del Panel de Alto Nivel sobre Cooperación Digital del secretario general de las Naciones Unidas, 2019[302]

301. Véase, por ejemplo, «International Leadership and Collaboration Materials», del Comisionado de Seguridad Digital de Australia.
302. The Age of Digital Interdependence (La era de la interdependencia digital), Panel de Alto Nivel sobre Cooperación Digital del secretario general de las Naciones Unidas, 2019.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

10 Cooperación global

Herramientas de apoyo:

1. Lista de marcos de trabajo internacionales que deben formalizarse

El proceso A («Establecer marcos de trabajo formales de relación —por ejemplo, un «Memorando de entendimiento» (MOU)— con las comunidades regionales y globales de seguridad infantil en Internet») expone que se deben cumplir unos requisitos mínimos en un amplio abanico de protocolos internacionales y de documentos de prácticas recomendadas. Los ministerios pertinentes deben trabajar con el resto del Gobierno, y con la ayuda de esta herramienta, para evaluar el cumplimiento.

	Describir cómo se cumplen los requisitos mínimos	**Brechas en el cumplimiento**	**Fecha en la que se notifica sobre dichas brechas al ministerio pertinente**	**Fecha en la que se notifica sobre estas brechas al grupo de partes interesadas de la seguridad infantil en Internet**
Objetivos de Desarrollo Sostenible de la ONU				
Convención de las Naciones Unidas sobre los Derechos de los Niños				
Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la participación de niños en los conflictos armados				
La venta de niños, la prostitución infantil y la utilización de niños en la pornografía				
Procedimiento de comunicación				

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

10 Cooperación global

	Describir cómo se cumplen los requisitos mínimos	Brechas en el cumplimiento	¿Fecha en la que se notificó al ministerio pertinente sobre las brechas?	¿Fecha en la que se notificó sobre estas brechas al grupo de partes interesadas de la seguridad infantil en Internet?
Observación general núm. 25 (2021)	☑			
Modelo de Respuesta Nacional				
Directrices de Luxemburgo sobre la terminología para la protección de los niños contra la explotación y el abuso sexuales				

Otros recursos de referencia:

Marcos de trabajo de apoyo a la cooperación internacional

1. **Hoja de ruta de las Naciones Unidas para la cooperación digital**[303]
   En 2020 se publicó la «Hoja de ruta del secretario general para la cooperación digital[304], apoyada por un Panel de Alto Nivel sobre Cooperación Digital. Ofrece recomendaciones a las diferentes partes interesadas sobre el fortalecimiento de la cooperación digital internacional.

2. **Recursos web de INTERPOL sobre los delitos contra los niños**[305]
   El sitio web de INTERPOL proporciona una serie de recursos —incluida información sobre el trabajo de INTERPOL— e información sobre la base de datos en línea de explotación y abusos sexuales a niños, el bloqueo y la categorización de contenidos y la identificación de las víctimas.

3. **Recomendación del Consejo de la OCDE sobre los niños en el entorno digital**[306]
   Esta recomendación establece principios y brinda orientación para ayudar a los países a encontrar un equilibrio entre la protección de los niños frente a los riesgos de Internet y la promoción de las oportunidades y las ventajas que ofrece el mundo digital.

303. Hoja de ruta del secretario general de las Naciones Unidas para la cooperación digital, Naciones Unidas, 2020.
304. Panel de Alto Nivel sobre Cooperación Digital del secretario general de las Naciones Unidas, Naciones Unidas, 2020.
305. Delitos contra los niños, INTERPOL.
306. Recommendation of the Council on Children in the Digital Environment (Recomendación del consejo sobre los niños en el entorno digital), OCDE, adoptada en 2012, modificada en 2021.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

10 Cooperación global

Otros recursos de referencia:

Marcos de trabajo de apoyo a la cooperación regional

1. **Convenio sobre seguridad cibernética y protección de datos personales la Unión Africana 2014**[307]
   Un convenio de la Unión Africana para crear un «marco de trabajo creíble para la ciberseguridad en África a través de la organización de transacciones electrónicas, la protección de datos personales, la promoción de la ciberseguridad, la gobernanza electrónica y la lucha contra la ciberdelincuencia».

2. **Agenda de la Unión Africana para la Infancia 2040**[308]
   En la agenda de la Unión Africana para el año 2040, «Agenda 2063», se esbozan los objetivos en relación a la infancia para todo el continente. La agenda gira en torno al párrafo 53, en el que se establece que «los niños africanos se empoderarán mediante la plena aplicación de la "Carta africana sobre los derechos del niño"».

3. **Estrategia europea en favor de un Internet más adecuado para los niños**[309]
   Esta es la estrategia europea de la Comisión Europea en favor de un Internet mejor para los niños. La estrategia se centra en las habilidades y en las herramientas digitales para los niños y también subraya el potencial del mercado para desarrollar contenidos en línea interactivos, creativos y educativos.

4. **Modelo de Respuesta Nacional (MRN), Alianza Mundial WeProtect**[310]
   El Modelo de Respuesta Nacional (MNR) tiene como objetivo ayudar a los países a desarrollar sus respuestas a la explotación y el abuso sexual infantil en Internet, aunque señala que esto no puede abordarse de forma aislada. Es necesario contar con un conjunto más amplio de capacidades para prevenir y combatir la explotación y el abuso sexual de los niños, a fin de garantizar la mejor respuesta posible a nivel nacional.

5. **Mapa de políticas, Better Internet for Kids (BIK)**[311]
   El «Mapa de políticas» de Better Internet for Kids (BIK) ofrece una panorámica general de las estrategias y las políticas de BIK que se aplican actualmente en todos los Estados miembros de la UE.

6. **Plan de Acción Regional de la ASEAN para la eliminación de la violencia contra los niños**[312] **y Declaración sobre la protección de los niños contra todas las formas de explotación y abuso en línea en la ASEAN**[313]
   El Plan Regional proporciona una hoja de ruta para ayudar a los Estados miembros a aplicar la declaración de la ASEAN de 2013 sobre la protección de los niños contra todas las formas de explotación en Internet. ▶

307. African Union Convention on Cyber Security and Personal Data Protection (Convención de la Unión Africana sobre ciber seguridad y protección de los datos personales), Unión Africana, 2014.
308. Africa's Agenda for Children 2040 Fostering an Africa Fit for Children, African Committee of Experts on the Rights and Welfare of the Child (Agenda africana para la infancia 2040 Fomentar una África adecuada para los niños, Comité africano de expertos en derechos y bienestar), 2016.
309. Estrategia europea en favor de un Internet más adecuado para los niños, Comisión Europea, 2021.
310. Modelo de Respuesta Nacional, Alianza Mundial WeProtect, 2016.
311. Better Internet for Kids Policy Map, Better Internet for Kids, 2020.
312. ASEAN Regional Plan of Action on Elimination of Violence against Children, Fondo de las Naciones Unidas para la Infancia, 2019.
313. Ending violence against children in ASEAN Member States (Acabar con la violencia contra los niños en los Estados miembros de ASEAN), UNICEF Asia Oriental y Pacífico, 2019.

7. **Estudio de caso: Convenios del Consejo de Europa**
   El «Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual», también conocido como «Convenio de Lanzarote»,[314] exige la penalización de todo tipo de delitos sexuales contra los niños. Establece que los Estados de Europa y algunos más adoptarán una legislación específica y adoptarán medidas para prevenir la violencia sexual, proteger a las víctimas infantiles y perseguir a los criminales.

   El «Comité de Lanzarote»[315] (es decir, el Comité de las Partes del Convenio de Lanzarote) es el órgano que se ha establecido para supervisar[316] si las partes aplican de manera efectiva el «Convenio de Lanzarote». El Comité también se encarga de determinar las prácticas recomendadas,[317] en particular durante las actividades de desarrollo de capacidades[318] (visitas estudiantiles, conferencias, etc.).

   El Consejo de Europa ayuda a proteger a las sociedades de todo el mundo de la amenaza de la ciberdelincuencia mediante el «Convenio de Budapest sobre la ciberdelincuencia» y su «Protocolo contra la xenofobia y el racismo», el Comité del Convenio sobre la Ciberdelincuencia y los programas de cooperación técnica sobre ciberdelincuencia.

   El convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y de otras redes informáticas que trata en particular de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de las redes. También incluye una serie de facultades y procedimientos, como la búsqueda de redes informatizadas y la intercepción.

8. **Principios preliminares y recomendaciones de la Organización de los Estados Americanos sobre protección de datos (Protección de datos personales)**[319]
   Este es el resultado de un estudio del Comité Jurídico Interamericano sobre los marcos de trabajo de la protección de datos. Los principios representan un modelo para el derecho interamericano en relación al acceso a la información pública. Representan la dirección de la Secretaría General a la hora de apoyar a los Estados miembros en el diseño, la ejecución y la evaluación de sus marcos jurídicos locales en materia de acceso a la información pública.

Cooperación entre países y marcos de trabajo de apoyo mutuo

9. **Directrices de Luxemburgo sobre la terminología para la protección de los niños contra la explotación y el abuso sexuales**[320]
   Estas directrices son una iniciativa de 18 colaboradores internacionales para armonizar las definiciones y los términos relacionados con la protección de los niños. Su objetivo es brindar una mayor claridad conceptual de la terminología, a fin de garantizar una promoción, unas políticas y unas leyes más sólidas y coherentes en todos los idiomas y en todas las regiones del mundo.

10. **Apoyo de la Policía de Escocia a la elaboración de una política relativa a los niños e Internet en Ruanda**[321]
    Se trata de una colaboración entre la Policía de Escocia y el Gobierno de Ruanda. En el blog de la 5Rights Foundation se puede consultar una entrada con toda la información sobre esta colaboración.

314. Convenio de Lanzarote, Consejo de Europa.
315. Comité de Lanzarote, Consejo de Europa.
316. Seguimiento del Convenio de Lanzarote, Consejo de Europa.
317. Prácticas recomendadas del Convenio de Lanzarote, Consejo de Europa.
318. Convenio de Lanzarote, Consejo de Europa.
319. Preliminary Principles and Recommendations on Data Protection (Principios preliminares y recomendaciones sobre protección de datos), Consejo Permanente de la Organización de los Estados Americanos, 2011.
320. Directrices de Luxemburgo, ECPAT, 2016.
321. Working with the Government of Rwanda and Police Scotland to support children online (Trabajando con el Gobierno de Ruanda y la Policía de Escocia para apoyar a los niños en línea), 5Rights Foundation, 2020.

10 Cooperación global

11. Declaración Universal de Seguridad Infantil en Línea[322]
Esta es la declaración de la Comisión de la Banda Ancha, que tiene como objetivo alinear a todas las partes interesadas pertinentes en la misión común de defender la causa de la protección de los niños en Internet.

Ejemplos de cooperación entre las fuerzas del orden[323]

12. Virtual Global Taskforce[324]
Este grupo de trabajo representa a organismos nacionales, regionales e internacionales encargados de hacer cumplir la ley que se han unido para luchar contra el abuso sexual de niños en Internet en todo el mundo. También facilita los teléfonos de las fuerzas del orden regionales y de la línea directa de denuncia de contenidos de abuso sexual infantil.

13. Directrices del Consejo de Europa para la cooperación entre las fuerzas del orden y los proveedores de servicios de Internet contra la ciberdelincuencia[325]
Se trata de un conjunto de directrices elaboradas para ayudar a los proveedores de servicios y a las comunidades encargadas de hacer cumplir la ley de cualquier país a establecer relaciones de trabajo eficaces. Está disponible en más de una docena de idiomas.

322. Child Online Safety Universal Declaration (Declaración universal de la seguridad de los niños en línea), Comisión de Banda Ancha, 2019.
323. Notice and Takedown: Company policies and practices to remove online child sexual abuse material (Notificación y retirada: políticas y prácticas de las empresas para retirar el material de explotación sexual infantil de Internet), Fondo de las Naciones Unidas para la Infancia y GSMA, 2016.
324. Virtual Global Taskforce, Virtual Global Taskforce, 2016.
325. Law enforcement - Internet service provider Cooperation (Cumplimiento de la ley; cooperación de los proveedores de servicios de Internet), Consejo de Europa, 2007.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

CARPETA DEL SISTEMA

8 ELEMENTOS | 105 MB EN EL DISCO | SECCIÓN 6

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

Documentos clave

La Convención de las Naciones Unidas sobre los Derechos del Niño y documentos relacionados:

1. **Convención de las Naciones Unidas sobre los Derechos del Niño**[326]
   Aprobada y disponible para su firma, su ratificación y su adhesión en virtud de la resolución 44/25 de la Asamblea General del 20 de noviembre de 1989. Entró en vigor el 2 de septiembre de 1990, de conformidad con el artículo 49.

   Hay disponibles un texto y gráficos de la Convención sobre los Derechos del Niño adaptados para niños (véase también la sección «Por qué son importantes los derechos del niño») para ayudar a los niños a comprender sus derechos.

2. **Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía**[327]
   Aprobado y disponible para su firma, su ratificación y su adhesión en virtud de la resolución 54/263 de la Asamblea General del 25 de mayo de 2000. Entró en vigor el 18 de enero de 2002.

3. **Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la participación de niños en conflictos armados**[328]
   Aprobado y disponible para su firma, su ratificación y su adhesión en virtud de la resolución 54/263 de la Asamblea General del 25 de mayo de 2000. Entró en vigor el 12 de febrero de 2002.

4. **Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a los procedimientos de comunicaciones**[329]
   Resolución aprobada por la Asamblea General el 19 de diciembre de 2011.

5. **Orientación de UNICEF: Cómo protegemos los derechos de los niños con la Convención de las Naciones Unidas sobre los Derechos del Niño**[330]
   Guía breve de UNICEF sobre la Convención y sus protocolos facultativos.

6. **Observación general núm. 25 (2021) sobre los derechos del niño en relación con el entorno digital**[331]
   La «Observación general núm. 25» ofrece un análisis práctico de las formas en que los derechos contenidos en la Convención se aplican a la seguridad de los niños en Internet y al mundo digital.

7. **Versión para los jóvenes de la «Observación general núm. 25» (2021) de la CDN sobre los derechos del niño en relación con el entorno digital**[332]
   Este documento expone en lenguaje para niños los derechos de los niños en el mundo digital y explica sus derechos de una manera accesible.

326. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1995.
327. Convención de las Naciones Unidas sobre los Derechos del Niño (versión para niños), Fondo de las Naciones Unidas para la Infancia.
328. Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2002.
329. Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la participación de niños en conflictos armados, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2002.
330. Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a los procedimientos de comunicaciones, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2014.
331. How we protect Children's rights with the UN Convention on the Rights of the Child (Cómo protegemos los derechos del niño con la Convención de las Naciones Unidas sobre los derechos del niño), Fondo de las Naciones Unidas para la Infancia.
332. In Our Own Words – Children's Rights in the Digital World (En nuestras propias palabras: los derechos del niño en el mundo digital), 5Rights Foundation, 2021.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >

Otros marcos de trabajo y documentos internacionales pertinentes:

1. **Alianza Mundial WeProtect: *Modelo de Respuesta Nacional* (MRN)[333]**
   El Modelo de Respuesta Nacional (MNR) es parte fundamental de cualquier kit de herramientas nacionales para la seguridad de los niños en Internet. El Modelo de Respuesta Nacional tiene como objetivo ayudar a los países a desarrollar sus respuestas a la explotación y el abuso sexual de niños en Internet, aunque señala que esto no puede abordarse de forma aislada. Es necesario contar con un conjunto más amplio de capacidades para prevenir y combatir la explotación y el abuso sexual de los niños, a fin de garantizar la mejor respuesta posible a nivel nacional. Este kit de herramientas proporciona recursos para respaldar la aplicación del MNR. Las herramientas para la seguridad de niñas, niños y adolescentes en Internet pueden ayudar a los signatarios del MNR de la Alianza Mundial WeProtect a garantizar que disponen de la capacidad institucional necesaria para cumplir sus objetivos y que se cumplen las obligaciones en virtud de la «Observación general núm. 25» (2021).

2. **Directrices de la UIT sobre la protección de los niños en Internet[334]**
   Las directrices de la UIT sobre la protección de los niños en Internet son un conjunto exhaustivo de recomendaciones para todas las partes interesadas pertinentes sobre cómo contribuir al desarrollo de un entorno digital seguro y beneficioso para niños y jóvenes.

   Las directrices sobre la protección de los niños en Internet son el resultado del trabajo conjunto de 80 expertos de diferentes sectores, lo que incluye partes interesadas del Gobierno, organizaciones internacionales, ONG, el mundo académico y el sector privado. Redactados por primera vez en 2009, se actualizaron en 2020 e incluyen cuatro conjuntos de directrices para:Niños

   - Padres/cuidadores y educadores
   - Industria
   - Responsables de las políticas

3. **Objetivos de Desarrollo Sostenible de la ONU (ODS)**
   La seguridad infantil en Internet contribuye al logro de varios de los ODS y puede formar parte de las agendas de los responsables políticos para cumplir con sus compromisos en virtud de los ODS. Adoptada por todos los Estados miembros de las Naciones Unidas en 2015, la Agenda 2030 para el Desarrollo Sostenible,[335] proporciona un plan común para la paz y la prosperidad de todos los ciudadanos y del planeta, ahora y en el futuro. Su piedra angular son los 17 Objetivos de Desarrollo Sostenible (ODS), [336]una llamada urgente a la acción conjunta de todos los países, tanto desarrollados como en vías de desarrollo. Se reconoce que poner fin a la pobreza y a otras privaciones debe ir de la mano de estrategias que mejoren la salud y la educación, que reduzcan la desigualdad y que estimulen el crecimiento económico, todo ello al tiempo que se aborda el cambio climático y se trabaja para preservar nuestros océanos y nuestros bosques.

4. **Principios rectores de la ONU sobre las empresas y los derechos humanos[337]**
   «Estos principios rectores se basan en el reconocimiento de:

   a) las actuales obligaciones de los Estados de respetar, proteger y cumplir con los derechos humanos y las libertades fundamentales;
   b) el papel de las empresas como órganos especializados de la sociedad que desempeñan funciones especializadas y que deben cumplir con todas las leyes aplicables y respetar los derechos humanos;
   c) la necesidad de que los derechos y las obligaciones vayan acompañados de recursos adecuados y efectivos en caso de que existan carencias.

   Estos principios rectores se aplican a todos los Estados y a todas las empresas, tanto transnacionales como de otro tipo, con independencia de su tamaño, sector, ubicación, propietarios y estructura». ▶

333. Modelo de Respuesta Nacional, Alianza Mundial WeProtect, 2015.
334. Directrices sobre la protección de la infancia en línea, Unión Internacional de Telecomunicaciones, 2021.
335. Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible, Departamento de Asuntos Económicos y Sociales de las Naciones Unidas, 2015.
336. Los 17 objetivos, Departamento de Asuntos Económicos y Sociales de las Naciones Unidas, 2015.
337. Principios rectores de la ONU sobre las empresas y los derechos humanos, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2011.

5. **INSPIRE, de la Organización Mundial de la Salud: Siete estrategias para poner fin a la violencia contra niños y niñas**[338]
   Un paquete técnico basado en evidencias para apoyar a los países en sus esfuerzos por prevenir la violencia contra niños y jóvenes de entre 0 y 17 años y ofrecer una respuesta adecuada. El paquete incluye el documento central, que describe cuáles son las estrategias e intervenciones de INSPIRE; un manual de implementación que ofrece información sobre cómo implementar las intervenciones; y un conjunto de indicadores para medir la aceptación de INSPIRE y su impacto en los niveles de violencia contra los niños».

6. **Borrador de las «Directrices normativas de UNICEF respecto a la IA para niños»**[339]
   Tiene como objeto promover los derechos de los niños en las políticas y las prácticas de IA del Gobierno y del sector privado y concienciar respecto a cómo pueden proteger o socavar dichos derechos los sistemas de IA. En las directrices normativas se analizan las políticas y los sistemas de AI y se valora cómo pueden afectar a los niños. Se basa en la Convención sobre los Derechos del Niño para presentar tres fundamentos para la IA que salvaguardan los derechos de los niños:

   - Las políticas y los sistemas de IA deben proteger a los niños.
   - Deben satisfacer de manera equitativa las necesidades y los derechos de los niños.
   - Deben empoderar a los niños para que contribuyan al desarrollo y al uso de la IA.

   Sobre la base de estos fundamentos, en las directrices se presentan nueve requisitos para la IA que esté dirigida a los niños y proporciona recursos ilustrativos con los que aplicar las propias directrices.

7. **Directrices de Luxemburgo sobre la terminología para la protección de los niños contra la explotación y el abuso sexuales**[340]
   Estas directrices son una iniciativa de 18 colaboradores internacionales para armonizar las definiciones y los términos relacionados con la protección de los niños. Su objetivo es brindar una mayor claridad conceptual de la terminología, a fin de garantizar una promoción, unas políticas y unas leyes más sólidas y coherentes en todos los idiomas y en todas las regiones del mundo.

8. **El principio de cautela**[341]
   La UNESCO, junto con su órgano consultivo, la Comisión Mundial de Ética del Conocimiento Científico y la Tecnología, elaboró una definición de trabajo del «principio de cautela» que aparece en muchos instrumentos internacionales relacionados con los avances científicos en general y que es pertinente para el diseño centrado en el niñas, niños y adolescentes en la tecnología:

   «Cuando las actividades humanas puedan acarrear un perjuicio moralmente inaceptable que sea científicamente verosímil pero incierto, se adoptarán medidas para evitar o minimizar dicho perjuicio. Un perjuicio moralmente inaceptable es aquel que se causa a seres humanos o al medioambiente y que es:

   1. una amenaza para la salud o la vida humana, o
   2. grave e irreversible, o
   3. injusto para las generaciones presentes o futuras, o
   4. impuesto sin tener debidamente en cuenta los derechos humanos de los afectados. ▶

338. INSPIRE: Siete estrategias para acabar con la violencia contra los niños, Organización Mundial de la Salud, 2021.
339. Policy Guidance on AI for Children (Directrices políticas sobre IA para niños), Fondo de las Naciones Unidas para la Infancia, 2020.
340. Terminología universal: Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, ECPAT International, 2016
341. The Precautionary Principle (El principio de cautela), Comisión Mundial de Ética del Conocimiento Científico y la Tecnología, 2005.

El juicio sobre la verosimilitud debe basarse en el análisis científico. El análisis debe ser continuo para que las medidas elegidas estén sujetas a revisión. La incertidumbre puede aplicarse a la causalidad o a los límites del posible daño, pero no tiene por qué limitarse a ellos.

Las medidas son intervenciones que se llevan a cabo antes de que se cause el perjuicio y cuyo objetivo es evitar o minimizar dicho perjuicio. Deben elegirse medidas que sean proporcionales a la gravedad del daño potencial. Se deben valorar sus consecuencias positivas y negativas y evaluar las implicaciones morales tanto de tomar una medida como de no tomarla. La elección de la medida debe ser el resultado de un proceso participativo».

9. **Marcos de trabajo regionales para la protección de los derechos del niño**
   Por ejemplo, las «Directrices del Consejo de Europa[342] para respetar, proteger y hacer efectivos los derechos del niño en el entorno digital» proporcionan una orientación útil en el contexto europeo. La Unión Africana elaboró la «Carta africana sobre los derechos y el bienestar del Niño»[343] para exponer los derechos del niño en el contexto africano.

10. **Iniciativas nacionales innovadoras de relevancia mundial**
    Por ejemplo, el «Código de diseño apropiado para cada edad»[344] del Reino Unido y la Ley de Seguridad en Línea de Australia.[345]

342. Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (Directrices para respetar, proteger y cumplir con los derechos del niño en el entorno digital), Consejo de Europa, 2018.
343. Carta africana sobre los derechos y el bienestar del niño, Unión Africana, 1990.
344. Introduction to the Age Appropriate Design Code (Introducción al código de diseño adecuado a la edad), Oficina del Comisionado de Información.
345. Consultation on a Bill for a new Online Safety Act (Consultas sobre un proyecto de ley para una nueva Ley de seguridad en línea), Departamento de Infraestructura, Transporte, Desarrollo Regional y Comunicaciones.

CARPETA DEL SISTEMA

8 ELEMENTOS | 105 MB EN EL DISCO | SECCIÓN 7

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

Glosario

En su 86.º período de sesiones, el Comité de los Derechos del Niño aprobó su «Observación general núm. 25» (2021) sobre los derechos del niño en relación con el entorno digital. Se incluyó también este glosario de terminología, aunque no es exhaustivo.

Analítica emocional
La recopilación de datos para determinar o inferir el estado de ánimo de un individuo —a menudo realizada mediante análisis de vídeo, voz, comunicación escrita o datos personales— para identificar marcadores como la expresión facial y el tono, correlacionados con emociones específicas, mediante técnicas de aprendizaje automático, incluidos los algoritmos.

Búsqueda automatizada
El proceso de evaluación de los datos de los usuarios para filtrar el contenido al que acceden en Internet, principalmente para fines comerciales. El contenido se selecciona, por regla general, en función de las percepciones respecto a la reacción del usuario a otros contenidos o en función del contenido que buscaron otros usuarios que actuaron de manera similar.

Ciberagresión
Actos dañinos llevados a cabo por individuos o grupos, en Internet o mediante el uso de tecnología digital, a menudo con la intención de ofender o perjudicar a otro individuo o grupo.

Cultura digital
La capacidad de utilizar las tecnologías de la información y la comunicación para realizar búsquedas, evaluar, crear y comunicarse. Algunos de los términos relacionados son: «alfabetización mediática», «alfabetización informativa» o «alfabetización mediática e informativa».

Desinformación
Compartir información que se sabe que es falsa.

Digitalización
La adaptación de entornos, prácticas, negocios y de la vida cotidiana para introducir servicios e infraestructuras digitales y beneficiarse de ellos. También se refiere a la conversión de información a formatos digitales.

Elaboración de perfiles
La práctica de utilizar los datos personales de una persona para inferir, predecir o analizar las características de esa persona —como por ejemplo lo que le gusta o no le gusta, preferencias, puntos de vista, opiniones o conductas— para recomendarle contenidos, productos o servicios basados en su perfil.

Filtrado de información
El uso de un programa para filtrar contenido digital e identificar u ocultar contenido que coincida con los criterios establecidos. Los usos comunes del filtrado de información incluyen: ocultar el contenido ofensivo para que no aparezca en los resultados de los motores de búsqueda o determinar qué resultados aparecen primero.

Información errónea
Compartir información falsa sin la intención de causar ningún perjuicio.

Minimización de datos
El principio por el cual se recopila solo la cantidad mínima de datos personales necesarios para el propósito para el que se procesan. Además, dichos datos se retendrán solo en la medida en que sea necesario para tal propósito.

< SECCIÓN ANTERIOR SIGUIENTE SECCIÓN >

Moderación de contenido
La práctica de monitorear y revisar el contenido generado por el usuario a partir de reglas predeterminadas para eliminar el contenido considerado inadmisible, ya sea automáticamente o mediante moderadores humanos. La moderación de contenido se puede realizar de manera simultánea a la generación de contenido (como en los servicios de chat) o a posteriori (como en los foros).

Neuromarketing
El estudio de las reacciones cerebrales ante el contenido publicitario y su aplicación en el desarrollo de campañas publicitarias más eficaces. Las reacciones se pueden medir de muchas formas: el escaneo de la actividad cerebral, el tiempo de interacción, los clics o el tiempo que alguien pasa en un sitio web.

Privacidad desde el diseño
La práctica de diseñar servicios en línea con el objetivo de proteger la privacidad de los usuarios tanto como sea posible. Por ejemplo, estableciendo que las cuentas de los usuarios menores de edad sean privadas por defecto o minimizando la cantidad de datos recopilados.

Procesamiento automatizado
El proceso de toma de decisiones por medios automatizados; es decir, mediante un software configurado para analizar los datos proporcionados y seguir reglas establecidas para tomar decisiones basadas en algoritmos, sin la participación humana.

Procesamiento de datos
Incluye procesos de recopilación, registro, retención, análisis, difusión y uso de datos.

Publicidad dirigida
La práctica de mostrar anuncios específicos a los usuarios en función de los datos recopilados sobre ellos, como su actividad en Internet, lo que compran, ubicación, género, edad, preferencias, etc.

Publicidad inmersiva
La integración sin fisuras de los anuncios en los contenidos de Internet o en los servicios digitales, lo que permite que los usuarios permanezcan «inmersos» en los contenidos o los servicios y que, al mismo tiempo, estén expuestos al marketing y a los mensajes de las marcas.

Riesgos contractuales
Perjuicio potencial derivado de la exposición del usuario a relaciones o presiones contractuales comerciales inapropiadas. Por ejemplo: uso compulsivo, juegos de azar, publicidad dirigida, costes ocultos, términos y condiciones injustos y pérdida de control sobre los datos personales.

Riesgos de conducta
Perjuicio potencial que nace del comportamiento o de la conducta del usuario o de sus pares. Por ejemplo: el uso deliberado de plataformas en línea para amenazar u hostigar a otros usuarios, incluido el ciberacoso, el «sexting» y los mensajes de odio. Esto se puede producir de manera involuntaria por la divulgación de información privada de otros usuarios.

Riesgos de contacto
Perjuicio potencial que nace de la posibilidad de que los usuarios contacten entre sí mediante servicios en línea. Por ejemplo: propiciar que desconocidos o personas que ocultan su identidad se pongan en contacto con niños.

Riesgos de contenido
Perjuicio potencial a los usuarios en función de la naturaleza del contenido de Internet, incluido el que no es apropiado para determinadas edades (por ejemplo, pornografía), el que es poco fiable (por ejemplo, información errónea o desinformación) o ciertas otras categorías de contenido (por ejemplo, promoción de conductas de riesgo o de métodos de autolesión y de suicidio).

Robo de identidad
La suplantación fraudulenta de otra persona con el fin de, por ejemplo, acceder a su dinero, dañar su reputación, obtener acceso a sus contactos en Internet u obtener algún otro tipo de beneficio.

Segmentación conductual
Análisis de la actividad en línea de los usuarios con el fin de dirigirles publicidad, mensajes, sugerencias de contenido adicional o contactos con otros usuarios en función de sus preferencias anteriores, a menudo con la intención de manipular su comportamiento futuro.

Seguridad por diseño
La práctica de diseñar servicios en línea con el objetivo de garantizar la seguridad de los usuarios en la medida de lo posible. Por ejemplo, mediante ajustes de seguridad predeterminados para las cuentas de los usuarios menores de edad o impidiendo que los adultos se pongan en contacto con usuarios menores de edad.

Sistemas automatizados
Software y hardware programados para realizar automáticamente una función sin necesidad de que un humano proporcione datos e instrucciones para cada operación.

Tecnología asistencial
Tecnología desarrollada para apoyar o mejorar la independencia de un individuo, incluidos los sistemas y los dispositivos de adaptación y de rehabilitación para personas con discapacidades, como los lectores de pantalla o el reconocimiento de voz.

Tecnología de implantes
Un microchip que se puede implantar en alguien para almacenar, rastrear o recuperar información contenida en una base de datos externa, como identificadores personales, información de contacto o información médica y policial.

Realidad virtual y realidad aumentada

Realidad aumentada:
Una simulación del mundo físico con características alteradas o elementos complementarios que, por regla general, se experimenta a través de una pantalla para permitir la superposición de objetos virtuales sobre una imagen o un vídeo en vivo de la realidad.

Realidad virtual:
La simulación por ordenador de una imagen o de un entorno tridimensionales con los que una persona puede interactuar de una manera aparentemente física o real mediante un equipo electrónico especial, como un casco con una pantalla interior o unos guantes con sensores.

Consulte las «Directrices de Luxemburgo» de la ECPAT para más información sobre los términos específicos relacionados con el abuso sexual de menores.[346]

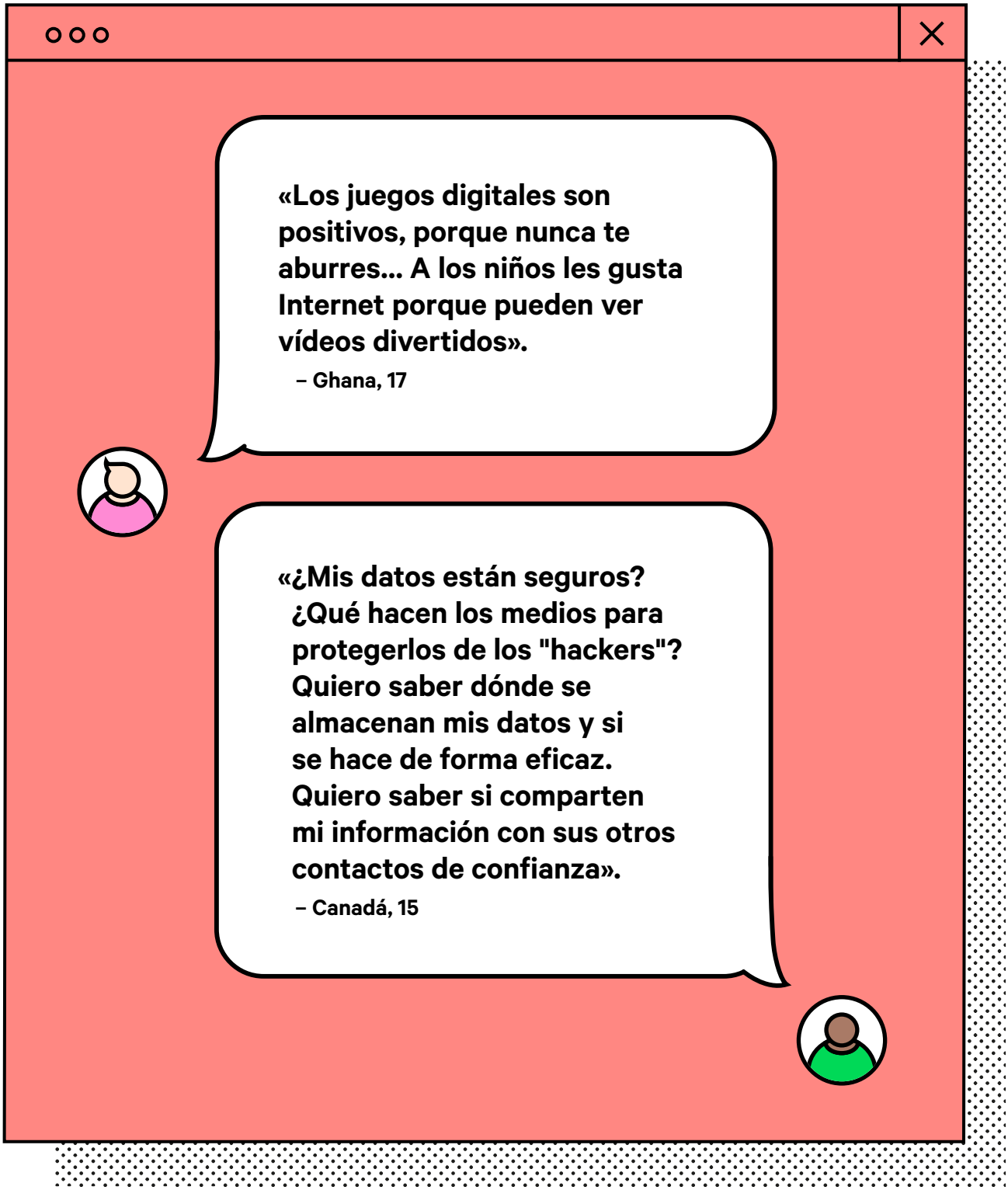
346. Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminología universal: directrices terminológicas para la protección del niño de la explotación y el abuso sexuales), ECPAT International, 2016.

Epílogo

Hacer de la protección de los niños en Internet una realidad es tarea de muchos: líderes mundiales, la comunidad internacional, los responsables de la formulación de políticas, las fuerzas del orden, los profesionales de la salud, los profesores, los padres, los cuidadores y los niños.

< SECCIÓN ANTERIOR

SIGUIENTE SECCIÓN >



CARPETA DEL SISTEMA

8 ELEMENTOS | 105 MB EN EL DISCO | SECCIÓN 8

Proyecto de modelo de política

El siguiente texto es un proyecto de modelo de política que aglutina todas las secciones de este kit de herramientas. Cada país tiene su propio punto de partida al redactar sus políticas de seguridad infantil en Internet. Este modelo expone una manera de abordar la dimensión digital de los derechos del niño.

Introducción

Por qué son importantes los derechos del niño

Los derechos del niño son un hilo conductor que recorre todas las políticas que afectan a la vida de los niños, dentro y fuera de Internet. El objetivo de una política de seguridad infantil en Internet es, fundamentalmente, garantizar que se ejerciten los derechos del niño a la protección y a la participación cuando interactúan con el mundo digital.

Los niños y sus familias tienen derechos humanos en virtud de la Carta Internacional de Derechos Humanos, que incluye la Declaración Universal de Derechos Humanos de 1948, el Pacto Internacional de Derechos Civiles y Políticos de 1966 y el Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966, así como las estructurales regionales y nacionales de derechos humanos.

Concretamente, con respecto a los niños, la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989 («la Convención» o «CDN»),[1] junto con sus «Protocolos facultativos» relativos a la venta de niños[3] y a los niños en conflictos armados,[2] proporciona un marco práctico para comprender cómo se aplican los derechos humanos a los niños. La Convención es el tratado de derechos humanos más ampliamente ratificado de la historia y su protocolo facultativo relativo a los procedimientos de comunicaciones contribuye a que pueda aplicarse de forma que los derechos del niño sean reales y efectivos.

Todos los derechos de la CDN tienen importancia en materia de seguridad infantil en Internet y hablar con los niños es fundamental para comprender qué significan en la práctica dichos derechos. Por ejemplo, debe tenerse en cuenta el derecho de los niños a jugar, a participar y a la vida familiar en Internet. Todos aquellos que participen en las consultas deben recibir una formación adecuada sobre los derechos del niño y sobre lo que significan en la práctica las opiniones y la inclusión de los niños.

5 consideraciones básicas

1. Identificar riesgos y mitigar daños

Las estrategias de seguridad infantil en Internet deben desarrollarse, sobre todo, para maximizar los beneficios que los niños pueden obtener de las tecnologías digitales. Esto implica necesariamente que existe una responsabilidad primordial de mitigar los riesgos, minimizar la probabilidad de que se produzcan daños, abordar los daños en caso de producirse y considerar cómo pueden afectar los productos y los servicios al usuario final si ese usuario es (o es probable que sea) un menor de 18 años. Es fundamental diseñar productos y servicios en los que se tenga en cuenta a priori la participación segura de los niños.

Mientras que algunos niños sufren daños graves, millones más experimentan daños en línea de una forma u otra. A pesar de que son relativamente pocos los niños que sufren las graves consecuencias del abuso sexual infantil, existen muchos riesgos derivados de la vigilancia o de la explotación comercial y de la exposición a informaciones falsas, estafas, depredadores o intimidación. Muchos de los riesgos son acumulativos. Los daños repercuten en cada niño de forma distinta y cualquier tipo de daño puede ser la antesala de otro.[4]

Dada la naturaleza global del mundo digital, los niños se enfrentan a muchos riesgos similares en Internet, independientemente de su ubicación geográfica. Pero cada contexto puede plantear problemáticas específicas. En algunos casos, un niño puede estar en desventaja por la falta de acceso al entorno digital. En otros casos, puede haber un vínculo entre los daños causados en Internet y la experiencia del niño fuera del

1. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
2. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
3. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989.
4. Building the digital world that young people deserve (Creando el mundo digital que la juventud merece), 5Rights Foundation, 2020.

entorno digital. A menudo, determinados riesgos y daños se dan de forma simultánea. Hay muy pocas líneas rectas y las divisiones no suelen estar claras.

Factores como el género, la edad, las circunstancias familiares, el nivel socioeconómico, la ubicación, las experiencias y la disponibilidad de la tecnología digital, pueden alterar los riesgos y las formas en que los niños experimentan los daños. Algunos riesgos y algunos daños afectan a comunidades y a colectivos enteros de niños. Por ejemplo, las niñas suelen atraer más abusos pero los casos de abusos en niños tienden a ser más graves.[5] Las normas culturales en torno a la masculinidad también impiden que se detecten y se comuniquen muchos casos de abuso sexual a niños varones.[6] Los riesgos y los daños también pueden verse potenciados por plataformas diseñadas de manera que se fomente el intercambio de contenidos impactantes o sensacionalistas, o que perfilen o promuevan determinados tipos de comportamiento por parte de sus usuarios, ya que con ello se genera una interacción lucrativa.

Los responsables de formular las políticas deben tener en cuenta todos los riesgos para los niños y dar los pasos necesarios para mitigarlos. Una herramienta clave para identificar riesgos es el marco de trabajo de las «4C».

La clasificación 4C de CO:RE pone de relieve que los riesgos en Internet surgen cuando un niño:

- Interactúa con **contenido** potencialmente dañino o se expone a él
- Experimenta un contacto potencialmente dañino o es el objetivo de dicho **contacto**.
- Es testigo, partícipe o víctima de una **conducta** potencialmente dañina
- Ha firmado un **contrato** potencialmente dañino o está siendo explotado por el mismo

2. Promover el acceso, la accesibilidad y la inclusión

Hoy en día, el acceso al mundo de Internet es crucial para que los niños ejerzan sus derechos y alcancen su máximo potencial. Una política de seguridad infantil en Internet debe ser inclusiva, tanto en la teoría como en la práctica.[7] Esto implica que debe contar con recursos suficientes y basarse en las prácticas recomendadas en los marcos de trabajo existentes, en particular en situaciones en las que los recursos son limitados. Tanto si la aplicación de las políticas de seguridad infantil en Internet conlleva adaptar la legislación existente —por ejemplo, en lo relativo a la protección del niño o del consumidor o a las normativas de telecomunicaciones— al contexto de la seguridad infantil en Internet como si se deben crear nuevos organismos jurídicos, se debe promover la inclusión y la igualdad de todos los niños, sin importar quiénes sean o dónde vivan.

Los niños no son un grupo homogéneo. Las políticas de seguridad infantil en Internet deben ser accesibles e inclusivas para llegar a todas las niñas, niños y adolescentes, sean quienes sean y vivan donde vivan. Es muy probable que surja una «brecha digital» y que algunos niños dispongan de fácil acceso al entorno digital mientras que otros queden completamente excluidos. Los marcos de trabajo deben ser apropiados para las distintas edades y ser aplicables para todos los niños, independientemente de su género, raza, religión, nacionalidad, origen étnico, posible discapacidad o cualquier otra característica. El lenguaje debe ser accesible e inclusivo y, de ser necesario, los materiales deben estar disponibles en diferentes idiomas. Los materiales de seguridad infantil en Internet deben diseñarse previa consulta con niñas, niños y sus figuras parentales/cuidadores. Como mínimo, deben resultar apropiados para las distintas edades, utilizar un lenguaje inclusivo y ser fácilmente accesibles para niños de distintas edades y para sus padres/cuidadores. En zonas con una baja tasa de alfabetización, los materiales visuales servirán para transmitir los mensajes de una forma más eficaz. El uso de términos coherentes en todas las plataformas ayuda a que la seguridad infantil en Internet se entienda mejor y sea accesible para los niños, para sus familias y sus cuidadores.[8]

Los responsables de la formulación de políticas deben garantizar que se promueve el acceso de los niños a Internet e incluirlos en sus decisiones para lograr que los entornos digitales sean seguros.

---

5. Safe Online Investment Portfolio Results 2020 (Resultados 2020 de la cartera de inversión segura en Internet), Alianza mundial para poner fin a la violencia contra niñas, niños y adolescentes, 2020. pág. 2.
6. Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse (Daños perturbadores en Kenia: evidencias de explotación y abusos sexuales infantiles), Alianza Mundial para poner fin a la violencia contra niñas, niños y adolescentes, 2021. pág. 68.
7. Por ejemplo: niños con discapacidades o niños de grupos minoritarios y marginados, niños que viven en la calle, desplazados o migrantes. Esta cuestión se analiza más a fondo en los temas intersectoriales que figuran a continuación. Hay más información sobre el modelo y la lista de verificación en «"Voice" is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child», Laura Lundy, 2013.
8. Véase la introducción sobre la importancia del lenguaje y las definiciones y la sección del glosario.

3. Crear una cadena de responsabilidad

La responsabilidad de la seguridad infantil en Internet está en manos de muchos actores; desde especialistas a organizaciones, incluidos el Gobierno, las fuerzas del orden, las empresas, los educadores, las redes de apoyo psicosocial, las familias y los niños. Algunos eslabones de esa cadena tienen una responsabilidad mayor.[9] Por ejemplo, aquellos servicios a los que sea probable que accedan los niños, o que puedan tener un determinado impacto en ellos, deben valorar si alguna de sus características representa un riesgo para los niños. Se deben tomar medidas a este respecto antes de interactuar con cualquier usuario infantil. Esto suele denominarse como «seguridad por diseño» o «diseño centrado en niñas, niños y adolescentes». La seguridad por defecto debería ser la norma.

Asumir la responsabilidad de la seguridad infantil en Internet implica tanto prevenir los daños antes de que se produzcan como tomar medidas cuando las cosas no vayan bien. Los mecanismos de quejas y denuncias deben ser accesibles y estar claramente identificados para que los niños, los cuidadores y los profesionales que los necesiten puedan encontrarlos y utilizarlos con facilidad. En los sistemas empresariales en línea deben establecerse mecanismos que permitan el seguimiento y la evaluación de las denuncias, de modo que puedan identificarse y abordarse rápidamente las cuestiones problemáticas.

Las leyes y los reglamentos deben establecer marcos de trabajo claros para la prevención y la responsabilidad y para la reparación, en caso de que algo salga mal. Esto incluye la recopilación de datos sobre denuncias y quejas con el fin de realizar un seguimiento y analizarlos de cara a introducir mejoras en el sistema. No se debe hacer responsables a los niños ni a los padres o a los cuidadores de prevenir o abordar riesgos y daños que apenas entienden o sobre los que no tienen casi ningún control. El consentimiento no puede esgrimirse para eximir a las organizaciones públicas o privadas de sus responsabilidades en lo relativo a la seguridad infantil en Internet. Integrar la seguridad infantil en Internet en línea en los marcos de trabajo existentes para la seguridad de los productos[10], la protección de la infancia[11], los derechos del niño[12] y de los consumidores[13] puede ayudar a evitar lagunas en la responsabilidad y la duplicación de recursos, roles y responsabilidades. No debería ni debe hacer vacíos legales que socaven la seguridad de los niños en Internet.

Es fundamental que la seguridad infantil en Internet se incorpore y se integre en todos los ámbitos políticos relacionados, desde los planes nacionales de banda ancha hasta los planes de estudio, de forma transparente, responsable y ejecutable. La creación de silos puede dar lugar a conflictos normativos y a una fragmentación de la formulación y de la aplicación de la política.

4. Integrar un diseño centrado en niñas, niños y adolescentes

La seguridad infantil en Internet debe integrarse en el diseño y en el desarrollo de la tecnología. El diseño centrado en niñas, niños y adolescentes incorpora a los servicios y a los productos, desde un primer momento, la seguridad infantil en Internet. También se debería garantizar que la seguridad infantil en Internet se tenga en cuenta en los requisitos normativos para el diseño de nuevas tecnologías y en la concesión de las licencias pertinentes[14]. El diseño centrado en niñas, niños y adolescentes también puede denominarse como «seguridad/derechos/privacidad/ética por diseño».

Aplicar el principio de cautela[15] a las tecnologías que puedan afectar a los niños y a los jóvenes garantiza que la seguridad del niño se tenga en cuenta desde las fases más tempranas. La Comisión Mundial de Ética del Conocimiento Científico y la Tecnología (COMEST) de la UNESCO presentó una «definición de trabajo» del principio de cautela:

---

9. Véase, por ejemplo, los Principios rectores sobre las empresas y los derechos humanos de las Naciones Unidas.
10. Child Protection Hub (Central de protección infantil), Comisión Europea, 2021.
11. Estrategia del Consejo de Europa para los derechos de los niños y las niñas, 2021.
12. Directiva sobre los derechos de los consumidores, Comisión Europea, 2014.
13. Directrices sobre la protección de la infancia en línea para los responsables de formular las políticas, Unión Internacional de Telecomunicaciones, 2020.
14. Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (Principios voluntarios para contrarrestar la explotación y el abuso sexuales de los niños), GOV.UK, 2021.
15. Véanse los siguientes documentos: Comunicación de la Comisión sobre el recurso al principio de precaución, EUR-Lex, 2000; The precautionary principle: Definitions, applications and governance (El principio de cautela: definiciones, aplicaciones y gobernanza), Parlamento Europeo, 2015.

«Cuando las actividades humanas puedan conducir a un perjuicio moralmente inaceptable que sea científicamente verosímil pero incierto, se tomarán medidas para evitar o minimizar dicho perjuicio.

Un perjuicio moralmente inaceptable es aquel que se causa a seres humanos o al medioambiente y que es:

- una amenaza contra la salud o la vida humanas, o
- grave e irreversible, o
- injusto para las generaciones presentes o futuras, o
- impuesto sin tener debidamente en cuenta los derechos humanos de los afectados».[16]

El principio de cautela debe servir de guía para crear un marco de trabajo para la seguridad y la privacidad por diseño que garantice que la seguridad infantil en Internet y los derechos del niño se incorporen a la tecnología en la fase de diseño. El diseño centrado en niñas, niños y adolescentes no debe ser únicamente un concepto ético, sino un requisito legal.[17] También debería incorporarse a los criterios de financiación de la investigación y el desarrollo que puedan afectar a los derechos del niño en Internet.

La tecnología y la inteligencia artificial (IA) tienen la capacidad de mejorar la seguridad infantil en Internet y de proteger sus derechos. Respaldar el desarrollo de herramientas tecnológicas para hacer efectivos los derechos del niño y mejorar la seguridad infantil en Internet es un aspecto importante de cualquier política de seguridad infantil en Internet. Se deben evaluar el impacto de la IA y de otras tecnologías diseñadas para proteger a los niños y a sus derechos con el fin de[18] evitar que se socaven otros derechos como la privacidad y la no discriminación.

Los niños son extremadamente diversos de por sí y se debe tener en cuenta todo el abanico de características, experiencias y contextos de los niños en la elaboración y la aplicación de la política, así como en la supervisión de su eficacia. Unas medidas eficaces en materia de seguridad infantil en Internet deberían abordar las tensiones que se perciban. Por ejemplo, en los debates sobre el cifrado, los defensores de la protección contra la explotación sexual de niños, niñas y adolescentes (ESIA) podrían encontrarse con que sus argumentos entran en conflicto con los relacionados con la privacidad y la protección de datos. Esos conflictos deben resolverse para alcanzar conclusiones prácticas y de esta manera evitar un círculo vicioso de años de debates mientras los niños corren peligro o sufren daños. En dichos casos, el «interés superior» del niño debe anteponerse a cualquier otra cuestión.[19]

Existen varios marcos de trabajo y procesos que respaldan la aplicación del diseño centrado en niñas, niños y adolescentes a la hora de formular políticas, incluidos el principio de cautela, las evaluaciones de impacto infantil[20] y las consultas a los niños.[21]

Además, el Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) ha creado una norma con pasos prácticos que las empresas pueden seguir para diseñar productos y servicios digitales que sean apropiados para cada edad[22] y la Digital Futures Commission ha establecido cómo la mejora del diseño de los productos y los servicios digitales podría contribuir a proteger el derecho de los niños a jugar libremente en un mundo digital. Los responsables de la formulación de políticas deben procurar siempre que los productos y los servicios reduzcan al mínimo los riesgos antes de ponerlos a disposición de los niños.

La seguridad por diseño y los derechos por diseño son de naturaleza sistémica y, por lo tanto, su objetivo es proteger a millones de niños desde el principio, no después de que pase algo.

16. Informe del Grupo de Expertos sobre el principio de cautela, Comisión Mundial de Ética del Conocimiento Científico y la Tecnología, 2005.
17. Véase, por ejemplo, el artículo 25 del Reglamento General de Protección de Datos, Unión Europea, 2018.
18. Véase, por ejemplo, la «Observación general núm. 25» (2021) relativa a los derechos de los niños en relación con el entorno digital, CDN, 2021.
19. Convención sobre los Derechos del Niño, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1989. (Véase, en concreto, la sección 1 del artículo 3 de los Derechos del Niño).
20. Child Rights Impact Assessment (evaluación del impacto sobre los derechos del niño), Digital Futures Commission, 2021.
21. Child Rights Impact Assessment, Digital Futures Commission, 2021.
22. IEEE 2089-21 Standard for Age-Appropriate Digital Services Framework, IEEE SA, 2021.

5. Garantizar la eficacia

La seguridad infantil en Internet y los derechos de los niños en el entorno digital solo se hará efectivos si se cuenta con intervenciones normativas prácticas, con los recursos adecuados y si se hace cumplir la ley.

La seguridad infantil en Internet es importante para un amplio abanico de ámbitos normativos, como las tecnologías de la información y la comunicación (TIC), la educación, la justicia penal, la salud, las regulaciones de la industria, el apoyo social y familiar, el mundo empresarial, los derechos humanos y la igualdad o el desarrollo internacional, entre muchos otros. Por lo tanto, la cooperación entre los ministerios y los organismos que trabajan en ámbitos normativos es fundamental para la adopción de medidas eficaces en materia de seguridad infantil en Internet. Será necesario elaborar presupuestos para dotar de recursos a las políticas, tanto dentro de los distintos departamentos como entre ellos. Las políticas sin suficientes fondos o las alianzas sin capacidad de acción —es decir, que solo existen sobre el papel— no lograrán proteger eficazmente a los niños en Internet.

Si se quieren desarrollar soluciones eficaces, se deben valorar las repercusiones de las políticas de seguridad infantil en Internet. La supervisión, la evaluación y la recopilación de datos son esenciales para sustanciar buenas políticas. Estudiar las políticas que funcionan en otros países y compartir las experiencias propias es una buena manera de maximizar la eficacia. Comprobar la eficacia de una política de seguridad infantil en Internet no requiere solo de consultas a los actores clave involucrados, sino también a los niños. De esta forma, se podrá comprender mejor cómo les afectan las medidas o cómo podrían afectarles en el futuro.[23] Se trata de un proceso en permanente desarrollo.

Las políticas deben basarse en datos y evidencias. Debería exigirse tanto a las autoridades pertinentes como a las empresas privadas que recopilen y compartan datos para comprender mejor las cuestiones relativas a la protección de los niños en Internet, de conformidad con las leyes y los principios de protección de datos. La seguridad infantil en Internet es un ámbito de actuación relativamente nuevo, por lo que cuando no se disponga de evidencias o estas se rebatan, los responsables de la formulación de políticas deberán adoptar un enfoque preventivo o analizar otros contextos y adoptar un enfoque sobre «lo que funciona». Por ejemplo, con principios de salud y de seguridad o con marcos de trabajo como «INSPIRE: Siete estrategias para poner fin a la violencia contra los niños y las niñas».[24]

La seguridad infantil en Internet no es un problema aislado. La eficacia de una política de seguridad infantil en Internet dependerá de la eficacia de las instituciones clave y de su capacidad para colaborar de cara contar con una protección eficaz. Para garantizar un sistema eficaz de rendición de cuentas en relación a la seguridad infantil en Internet y, en particular, respecto a la prevención de la explotación sexual de niñas, niños y adolescentes se debe contar con el amparo de sistemas judiciales sólidos a nivel nacional. El Modelo de Respuesta Nacional (MNR) ofrece una serie de pautas sobre esta cuestión.

Además, para que el enfoque de la seguridad infantil en Internet sea eficaz, las instituciones involucradas deben disponer de recursos suficientes, incluidos ámbitos como la asistencia psicosocial, las normativas en materia de TIC u otros campos relacionados. Para poder defender los derechos de los niños de forma eficaz mediante una política de seguridad infantil en Internet, se necesitan legislaciones eficaces en materia de derechos humanos y leyes y normativas específicas con organismos de supervisión que garanticen los derechos de los niños tanto dentro como fuera del entorno digital.

Los responsables de formular las políticas deben garantizar que las capacidades institucionales, los recursos y los mecanismos de rendición de cuentas sustenten las políticas de seguridad infantil en Internet. En caso de que surjan conflictos, la prioridad debe ser el «interés superior» de los niños. Si no se tiene en cuenta esta premisa, ni siquiera la mejor política resultará eficaz.

---

23. Digital Futures Commission (Comisión de futuros digitales), 5Rights Foundation, 2021.
24. INSPIRE Indicator Guidance and Results Framework (Guía de indicadores y marco de resultados de INSPIRE), Organización Mundial de la Salud, 2018.

Áreas de acción de la política

1. Capacidad institucional

1a. Reafirmar el compromiso público con la seguridad infantil en Internet al más alto nivel
Los dirigentes nacionales, incluidos el primer ministro o el presidente, deben comprometerse a velar por la seguridad de los niños en Internet tanto en el plano nacional como en el internacional.

1b. Designar a un ministerio o a un organismo para que tome la iniciativa en el desarrollo de una política nacional de seguridad infantil en Internet
En el mundo, la responsabilidad en relación a las políticas de seguridad infantil en Internet la ostentan diferentes organismos y ministerios. La elección de un determinado organismo o ministerio puede afectar al desarrollo de la política de seguridad infantil en Internet y a cómo se priorizan las distintas cuestiones. Por regla general, la seguridad infantil en Internet suele ser una cuestión que involucra a varios ministerios, pero es importante que exista un organismo concreto que lleve las riendas. En algunos países, las políticas de seguridad infantil en Internet están a cargo del ministerio responsable de las TIC; en otros, el peso recae sobre el ministerio responsable de la infancia y las familias; y en otros la voz cantante la lleva el Ministerio de Justicia. En caso de que haya grupos trabajando en cuestiones relacionadas con la violencia contra los niños (VCN) o la ciberseguridad, pueden ampliarse para incluir a determinados expertos y evitar así trabajar «en una burbuja». El organismo responsable se puede elegir en función de su autoridad, su experiencia, sus recursos, su capacidad o su compromiso. Aun así, deberá trabajar con otros ministerios y organismos. Sea cual sea el ministerio que lleve la iniciativa, deberá comprometerse con un enfoque holístico que refleje las necesidades generales de la seguridad infantil en Internet.

1c. Publicar un manual de definiciones y términos
El ministerio responsable deberá publicar una lista completa de definiciones y términos que refleje las definiciones que se emplean en las prácticas recomendadas internacionales.[25]

1d. Crear un comité directivo nacional de seguridad infantil en Internet
El comité directivo nacional de seguridad infantil en Internet se encargará de aplicar y desarrollar políticas y actuará como punto de enlace para la cooperación a nivel nacional y regional. Deberá desarrollar una estrategia para implementar las «Herramientas para la seguridad de niñas, niños y adolescentes en Internet». Esto podría denominarse «plan de acción». El comité se ocupará de un amplio abanico de competencias que abarcan varios ámbitos normativos, entre ellos la educación, la sanidad, la justicia, la protección de los consumidores, la protección de datos, la aplicación de la ley, las TIC y los servicios sociales. Además, supervisará la aplicación y el cumplimiento de las normas. Se exigirá formalmente al comité que coopere con todos aquellos que velen por la seguridad infantil o la ciberseguridad, y deberá mantener un contacto periódico con el ministerio pertinente.

1e. Dialogar con las partes involucradas en la seguridad infantil en Internet
Las fuerzas del orden, las empresas, el sector terciario, las organizaciones de defensa de los derechos del niño, las instituciones, los padres/cuidadores y el mundo académico pueden hacer aportes importantes e interesantes en relación a la seguridad infantil en Internet. En algunos contextos, crear un grupo de partes interesadas puede ser útil para ayudar al comité en sus actividades y basar su plan de acción en situaciones reales. En otros contextos, podrían resultar más útiles las conversaciones informales o solicitar los testimonios de una red abierta de partes interesadas. En cualquier caso, el comité directivo nacional de seguridad infantil en Internet debe tratar de entablar relaciones con partes interesadas de relevancia que puedan respaldar sus actividades. Se debe promover la cooperación entre organismos. El objetivo de involucrar a las partes interesadas tiene que ver con la aplicación de la política, no con el desarrollo de esta.

1f. Definir las funciones y las responsabilidades de las partes interesadas
Debe existir un marco de trabajo corregulador que defina tanto las funciones y las responsabilidades de todas las organizaciones que desarrollen y gestionen la infraestructura, las redes y los servicios digitales como las obligaciones de los departamentos gubernamentales. Se deben establecer normas básicas para todos en la cadena de valor, incluidos tanto los responsables de la infraestructura, del hardware y de los productos y los servicios digitales como aquellos que los gestionan o los utilizan cuando interactúan con los niños. Estas

25. Véase, por ejemplo, Universal Terminology: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Terminología universal: directrices terminológicas para la protección infantil de la explotación y el abuso sexuales), ECPAT International, 2016.

normas deben centrarse en la seguridad infantil y en hacer efectivos los derechos del niño en el mundo digital. Debe garantizarse la participación en los grupos de interesados de la sociedad civil y la consulta a los niños.

1g. Definir indicadores y evaluaciones de rendimiento
Cada aspecto del plan de aplicación debe contar con la correspondiente autoridad al cargo (un individuo, una institución o un organismo) y con recursos humanos y económicos para llevar a buen puerto las tareas previstas. Puede que la misma autoridad sea responsable de más de un área de la política, pero también de un solo ámbito de especialización. Deben introducirse indicadores clave de rendimiento (KPI), mecanismos de evaluación y estructuras claras de presentación de informes para que el comité directivo pueda supervisar y gestionar los progresos. Ya que el entorno digital evoluciona a gran velocidad, los KPI deberán revisarse constantemente.

1h. Garantizar la integración de la seguridad infantil en Internet en todas las áreas de la política gubernamental
Cualquier plan nacional pertinente, como el Plan Nacional de Banda Ancha o los marcos de trabajo de cultura digital, debe incluir la política de seguridad infantil en Internet como parte de su estrategia de implementación. Los planes que se desarrollen a lo largo de varios años deberán revisarse cuando se alcancen objetivos importantes.

2 Marcos jurídicos y reguladores

2a. Reforzar y hacer cumplir las leyes que prohíban los delitos relacionados con la seguridad infantil en Internet
Las leyes y los procedimientos penales facilitan la investigación y el enjuiciamiento de los delitos digitales que vulneran el derecho de los niños a la protección. Por lo tanto, deben reforzarse y modificarse en consonancia con las normas internacionales y con las prácticas recomendadas. Esto debería incluir la introducción de evaluaciones de riesgo obligatorias para reducir los posibles daños y la mejora de las sanciones y de los marcos de trabajo en relación a las sentencias, en caso de que sea necesario. También se debe incluir la posibilidad de emplear procedimientos de notificación y de retirada. Las leyes penales relativas a la seguridad infantil en Internet deben elaborarse teniendo en cuenta todos los derechos del niño, incluido su derecho a ser escuchados y a la participación.[26]

2b. Introducir reglamentos de protección de datos y contar con autoridades de supervisión independientes para garantizar que los datos de los niños se tratan de forma apropiada y que solo se recopilan cuando es necesario, con la máxima seguridad y el mayor de los cuidados.
Dichos reglamentos generales deben incluir una categoría especial para los datos de los niños en la que se exija un mayor nivel de protección y de salvaguarda por defecto, así como la protección contra el uso comercial indebido de los datos de los niños. Cuando se solicite el consentimiento de los niños (o de los padres/cuidadores en su nombre) para recopilar y tratar datos de los niños, debe notificarse de forma clara y hacerse con una finalidad legítima. La recopilación de datos con fines de salvaguarda debe ser objeto de una consideración especial, en circunstancias excepcionales, cuando se lleve a cabo en favor del interés superior del niño.

2c. Reforzar la investigación, los procesos y las condenas penales por explotación o el abuso sexual de niños en Internet[27]
Los organismos de justicia penal con competencias en los delitos relacionados con la seguridad infantil en Internet deben recibir formación en materia de seguridad infantil en Internet con el objetivo de fomentar una mayor prevención, un enjuiciamiento eficaz y unas condenas adecuadas, así como para comprender mejor cómo afectan estas situaciones a las víctimas. Las aptitudes de los equipos de investigación y respuesta pertinentes deben revisarse y reforzarse para detectar y prevenir las amenazas de ciberseguridad y reaccionar ante ellas, especialmente en el caso de las relacionadas con la seguridad infantil en Internet. Los sistemas de justicia penal deben poder garantizar un acceso oportuno a la justicia.

---

26. Por ejemplo, los marcos jurídicos que no dejan claro si las imágenes sexuales autogeneradas que se intercambian de forma consensuada entre niños se considerarán material de explotación sexual de niñas, niños y adolescentes. Incluso aunque en la práctica no se procese a los niños, esta incertidumbre jurídica puede socavar los derechos a la confianza, al control y a la autonomía.
27. La explotación sexual de niños, niñas y adolescentes (ESIA) se produce cuando se obliga a un niño a participar en actividades sexuales o se le convence para que lo haga. Esto puede implicar actividades con o sin contacto físico y puede darse tanto en el entorno digital como fuera de él.

2d. Revisar y reforzar los sistemas de justicia de menores
Garantizar que la ley sea clara y proporcionada para reducir todo lo posible el riesgo de que los niños entren en conflicto con la ley en el contexto de la seguridad infantil en Internet. En el caso de que los niños se enfrenten a sanciones penales relacionadas con la seguridad infantil en Internet —por ejemplo, en relación con el ciberacoso o el abuso sexual basado en imágenes—, el sistema judicial deberá hacer todo lo posible para evitar que se criminalice a los niños y proporcionar el apoyo y la representación legal adecuados para proteger los derechos de aquellos niños que entren en conflicto con la ley.

2e. Identificar y ratificar protocolos internacionales en materia de seguridad infantil en Internet
Para crear un ecosistema sostenible de seguridad infantil en Internet es necesario un enfoque que tenga en cuenta a las diferentes partes interesadas y con participación a escala mundial. Cada país debe identificar y ratificar los protocolos y los tratados internacionales y regionales pertinentes y dar los pasos necesarios para aplicar las diferentes medidas.

2f. Reforzar las capacidades de los organismos de seguridad
Se identificarán las deficiencias en los organismos de seguridad y en el poder judicial y se establecerán medidas para que haya una mayor sensibilización, para fomentar la presentación de denuncias y para que los procesos judiciales tengan éxito. Siempre que sea posible, se solicitará la formación y el intercambio de conocimientos a nivel internacional y se fomentará la coordinación y colaboración entre la industria y las fuerzas del orden.

3 Datos personales e identidad

3a. Establecer marcos de trabajo de protección de datos efectivos respecto a la protección de los datos de los niños o garantizar la efectividad de los ya existentes
Los derechos del niño en el entorno digital están estrechamente relacionados con la manera de recopilar, almacenar y utilizar sus datos. Las leyes y las regulaciones de protección de datos para los niños deben ser accesibles, eficaces y capaces de evolucionar para hacer frente a los riesgos emergentes.[28] Esto no solo implica establecer los marcos jurídicos y regulatorios, sino también asegurarse de que funcionan en la práctica y de que se aplican en consecuencia.

3b. Establecer protocolos y limitaciones para el uso de la toma de decisiones automatizada que puede afectar a los niños
Las normas, las leyes y los códigos de prácticas deben garantizar que los niños se beneficien de los sistemas automatizados y que no salgan perjudicados de la toma de decisiones automatizada.[29] Es particularmente importante evitar las discriminaciones que puedan derivarse de la toma de decisiones automatizada. Estos protocolos y limitaciones pueden aplicarse en el contexto de la justicia penal, el bienestar social, la sanidad y la medicina, la educación y el sector privado, entre otros ámbitos.

3c. Garantizar la protección jurídica y reguladora adecuada para los datos biométricos de los niños
Los Gobiernos y los organismos reguladores deben establecer protocolos jurídicos y reguladores apropiados y limitaciones para el uso de los datos biométricos de los niños, en virtud de los principios de los derechos del niño, la limitación de los fines y los requisitos de la política de seguridad infantil en Internet.

3d. Establecer directrices, leyes y reglamentos claros sobre las prácticas que pueden afectar a la voluntad de los niños
Crear marcos de trabajo legales que impidan la publicidad personalizada dirigida a niños o su seguimiento para fines comercialesa partir de sus datos personales. Establecer códigos sobre el uso de sistemas de recomendación y de otros procesos o tecnologías de toma de decisiones automatizadas que puedan «teledirigir» el comportamiento de los niños, alterar sus preferencias y sus opiniones, socavar reputaciones o limitar la experimentación.[30]

---

28. Reglamento General de Protección de Datos, Unión Europea, 2018.
29. World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert (El mundo se dirige como un zombi a una distopia de bienestar digital, advierte experto en derechos humanos de la ONU), Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2019.
30. Véase, por ejemplo, YouTube Data Breach Claim, McCann vs Google, 2021.

3e. Establecer mecanismos efectivos de supervisión y seguimiento
Crear organismos y sistemas que puedan recopilar información relevante para la seguridad infantil en Internet y garantizar la transparencia y la aplicación efectiva de los derechos y de la protección de los niños por parte de las empresas, el Gobierno y otras organizaciones.

3f. Establecer marcos de trabajo para garantizar la transparencia
La supervisión debe estar a cargo de un organismo regulador designado que cuente con recursos suficientes y con la capacidad y la experiencia necesarias para comprender los sistemas en uso y cómo afectan a los derechos de los niños. Dicho organismo regulador deberá, además, tener acceso a investigadores y a expertos independientes.

4 Sistemas de respuesta y de apoyo

4a. Notificación y retirada
Las instituciones gubernamentales trabajarán con expertos, con las fuerzas del orden y con la industria para establecer y supervisar protocolos efectivos para la notificación y la retirada de contenidos ilegales y dañinos. Entre otras cosas, será necesario diseñar protocolos (y las leyes correspondientes) que garanticen que los proveedores locales de servicios de Internet restrinjan el acceso a los sitios o a las plataformas que no retiren el contenido respecto al que se les ha notificado o que infrinjan sistemáticamente las leyes u otros requisitos legales en materia de seguridad infantil en Internet.

4b. Establecer procesos para la gestión de riesgos en relación a los delincuentes y a la explotación sexual infantil
Debe establecerse un proceso eficaz de gestión en relación con los delincuentes con la participación de múltiples partes interesadas y sobre la base de normas internacionales de prácticas recomendadas. Las fuerzas del orden y otros profesionales de la justicia penal deben estar capacitados para detectar e investigar comportamientos delictivos. La gestión de riesgos en relación a los delincuentes es parte fundamental de la seguridad infantil en Internet, ya que un individuo o un grupo de delincuentes pueden llegar a un gran número de víctimas infantiles a través de Internet.

4c. Facilitar los recursos adecuados para la asistencia psicosocial de las víctimas principales y secundarias y de sus familias
Las organizaciones que forman a los profesionales de los ámbitos de la salud mental, la psicología y el trabajo social que trabajan con niños vulnerables deben tener un conocimiento básico de las cuestiones de seguridad infantil en Internet.[31] La seguridad infantil en Internet debe integrarse en los sistemas más generalizados de seguridad y de protección de los niños, como la protección en los colegios o la violencia contra los niños (VCN).

4d. Establecer marcos de trabajo para la identificación y la protección de las víctimas
Un objetivo primordial en la prevención de los perjuicios en Internet será evaluar las necesidades de los niños vulnerables y la mejor manera de ayudarlos. Los centros de atención integral actúan como coordinadores para las víctimas de explotación y proporcionan acceso a un amplio abanico de servicios esenciales, desde la asistencia médica hasta el asesoramiento jurídico, todo desde un mismo lugar. Ofrecen un marco de trabajo para los procedimientos de salvaguarda y protección infantil, proporcionan apoyo a las víctimas y transmiten rápidamente las denuncias de delitos en Internet a las autoridades pertinentes.[32]

4e. Garantizar que los marcos de trabajo pertinentes no criminalicen a los niños
Es importante establecer marcos de trabajo adecuados para tratar con niños que puedan encontrarse en conflicto con la ley en el contexto de la seguridad infantil en Internet (por ejemplo, en casos de ciberacoso, divulgación de información maliciosa o «hackeo»). Siempre que sea posible, debe apartarse a los niños del sistema de justicia penal y barajar la posibilidad del asesoramiento o de la justicia restauradora. Sobre todo, es fundamental garantizar que se entienden todas las circunstancias del niño. Por ejemplo, la forma de actuar de un niño puede ser producto del acoso escolar, del engaño por parte de pederastas (o «grooming») u de otra forma de coacción.

---

31. What Works to Prevent Violence Against Women and Girls Evidence Reviews Paper 3: Response mechanisms to prevent violence, What Works, 2015. pág. 28.
32. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response (Evitar y abordar la explotación y el abuso sexuales de niñas, niños y adolescentes (ESIA): modelo de respuesta nacional), Alianza Mundial WeProtect , 2016.

5 Las empresas y los derechos de los niños:

5a. Implementar la seguridad, los derechos y la ética desde el diseño

Se deben desarrollar normas y códigos de prácticas que exijan que los diseñadores de productos, los fabricantes y los proveedores de servicios defiendan los derechos de los niños y contribuyan a la seguridad y a la protección infantil en Internet. Los términos y las condiciones deben reflejar el interés superior del niño. Entre otras cosas, las normas y los códigos de prácticas tendrán por objeto evitar que se ofrezca a los niños contenidos o contactos dañinos o inapropiados; proteger la privacidad de los niños en Internet, a nivel de sistemas o dispositivos; y abordar las preocupaciones de seguridad planteadas por el «internet de las cosas» (juguetes y servicios conectados con una función de transmisión de flujo continuo) para garantizar que las empresas privadas hayan tenido en cuenta, a partir de una evaluación de impacto infantil, un proceso de mitigación y prevención de riesgos de cara a ofrecer a los niños un servicio apropiado para su edad.

5b. Introducir normas básicas[33]

La industria tiene la responsabilidad de garantizar que los niños estén protegidos en Internet. Esto implica la creación de un espacio en Internet seguro y accesible para los niños. No se trata solo de impedir su acceso a contenidos dañinos. Se exigirá a las empresas que expongan qué procedimientos y qué consideraciones especiales han adoptado para garantizar la seguridad de los niños y el respeto de sus derechos, en el marco de trabajo de las «4C» de la gestión de riesgos,[34] a medida que desarrollen y establezcan sus servicios en línea.[35] El ministerio o el organismo pertinentes deben crear un código bajo la supervisión del comité directivo. Estas normas serán obligatorias y se exigirá su cumplimiento.

5c. Aplicación de la clasificación por edades

La aplicación de una clasificación coherente y por edades para los contenidos comerciales, los medios de comunicación de servicio público y los juegos y las actividades en Internet propicia un enfoque transparente y eficaz de la gestión de aquellos contenidos y servicios que afectan a los niños. Esto puede ser necesario para artículos y servicios a los que se les deba aplicar dicha clasificación y para los contenidos que estén pensados para diferentes rangos de edad. Se requerirá la verificación de la edad o la creación de espacios solo para adultos si se trata de contenidos prohibidos o de actividades que no sean adecuadas para niños. Para esto, quizá se deban proporcionar filtros de contenido que bloqueen los contenidos no deseados.[36]

5d. Introducir sistemas de moderación y de presentación de denuncias

Se exigirá que los proveedores de servicios introduzcan mecanismos para identificar contenidos molestos o inadecuados y sistemas de seguimiento transparentes y sólidos para todos los servicios en línea, incluida la implantación de mecanismos de retirada. Habrá una línea directa pública y gratuita para ofrecer tanto información como ayuda o asesoramiento por parte de expertos. Los niños deben poder acceder con facilidad a los mecanismos de denuncia de contenidos. Los sistemas para señalar la existencia de contenidos inadecuados deben considerarse una herramienta adicional.

5e. Garantizar la protección de los niños contra la presión comercial

Las medidas para proteger a los niños de las presiones comerciales incluirán: fomentar diseños apropiados para cada edad, deshabilitar la publicidad dirigida y el intercambio con terceros y concienciar sobre el contexto en el que crecen los niños. Los productos y los servicios que pongan énfasis en los derechos y la seguridad infantil en Internet podrán contar con un certificado. Asimismo, se podrá actuar contra los desarrolladores de productos y de servicios que violen dichos valores.

5f. Garantizar que se apliquen los principios del diseño centrado en niñas, niños y adolescentes para minimizar los posibles riesgos para la seguridad infantil en Internet

Esto incluye, por ejemplo, la posibilidad de que adultos desconocidos puedan entrar en contacto con los niños, la publicidad dirigida sobre juegos de azar o la recomendación de contenidos dañinos. La seguridad infantil en Internet debe integrarse en la fase de diseño para evitar que surjan problemas más adelante.

---

33. Véase, por ejemplo, «Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse», GOV.UK, 2020.
34. Véase la sección sobre «Riesgos y daños».
35. Los derechos del niño en evaluaciones de impacto, Fondo de las Naciones Unidas para la Infancia, 2013.
36. But how do they know it is a child? (Pero, ¿cómo saben que es un niño?), 5Rights Foundation, 2021.

6 Formación

6a. Facilitar formación, desarrollo de habilidades y orientación a todos los involucrados en la seguridad infantil en Internet
Desde los que ofrecen contenidos o servicios hasta los jueces, todos los que forman parte de la cadena de aplicación de la ley y los profesionales que trabajan con niños en otros entornos como la educación o la sanidad, deben estar familiarizados con la seguridad infantil en Internet. Se les debe facilitar una formación completa, en concreto sobre cómo su función particular se relaciona con la seguridad infantil en Internet, cómo reconocer los comportamientos delictivos y cómo proporcionar a las víctimas acceso a la asistencia necesaria.

6b. Facilitar formación especializada sobre la asistencia psicosocial y la identificación de todas aquellas señales que alerten de problemas respecto a la seguridad infantil en Internet
Para trabajar con eficacia, los profesionales pertinentes deben recibir formación en materia de seguridad infantil en Internet, formación sobre políticas de salvaguarda y de protección infantil y formación sobre asesoramiento familiar e infantil. La concienciación sobre la seguridad infantil en Internet debe incorporarse a los marcos de trabajo existentes relacionados con la protección de los niños. Los profesionales que trabajan con niños en la educación, la sanidad, la comunidad y en otros entornos deben estar capacitados para reconocer las señales y los síntomas que alerten de problemas respecto a la seguridad infantil en Internet.

6c. Crear planes de educación terciaria
Las sesiones de seguridad infantil en Internet deben ser obligatorias en la enseñanza, el trabajo social, la sanidad, la psicología y en otras especialidades relacionadas que se impartan en universidades o en instituciones públicas o privadas. Es necesario revisar con periodicidad la eficacia de estos conocimientos a la luz de los avances en la formación sobre seguridad infantil en Internet y de las cuestiones emergentes. Los planes de estudio deben abarcar todos los aspectos de la seguridad infantil en Internet, como se establece en esta política.

6d. Fomentar el desarrollo profesional
Se crearán, se revisarán de forma periódica y se actualizarán programas de educación continua sobre la seguridad y la protección de los niños Internet para aquellos profesionales
que trabajen en los ámbitos pertinentes para no quedar desfasados respecto a las tecnologías emergentes y para abordar los nuevos obstáculos y las nuevas problemáticas a medida que vayan surgiendo.

7 Educación

7a. Designar orientadores de protección infantil
Cada colegio debe designar un orientador de protección infantil.[37] Cada orientador debe recibir formación sobre los procedimientos de protección infantil y formación específica sobre seguridad infantil en Internet. Los orientadores serán los responsables de garantizar que se adopten, se promulguen y se hagan cumplir en los colegios las políticas de seguridad infantil en Internet (incluidos los procedimientos de salvaguarda y los sistemas de denuncia anónima). El orientador de protección infantil será la persona de contacto en relación a las cuestiones relacionadas con la protección infantil y la seguridad infantil en Internet. Asimismo, comunicará a las autoridades pertinentes los perjuicios que se denuncien. Los orientadores deben facilitar, además, los planes de intervención para proteger a los niños contra cualquier posible perjuicio.

7b. Promover una educación digital accesible
Promover contenidos —incluidos los programas entre pares— de probada eficacia que ayuden a los niños a desarrollar habilidades digitales y los empoderen de cara a construir comunidades respetuosas que fomenten la seguridad infantil en Internet. La educación digital debe ser holística y abarcar los datos y la alfabetización mediática, junto con las cuestiones de salvaguarda (sobre todo, cuestiones como la sexualidad y el consentimiento). La educación debe hacerse extensiva a los padres/cuidadores para respaldar el papel de estos en el fomento de la seguridad infantil en Internet.

37. Podría tratarse de alguien de una junta de seguridad escolar, un educador o alguien de un comité de protección infantil de la aldea o de la comunidad en el que estén representados los colegios.

7c. Promover los contenidos educativos
A medida que se generalice la adopción digital, se proporcionarán a los alumnos y a los profesores los conocimientos necesarios para interactuar con los sistemas digitales y para beneficiarse plenamente de los contenidos del plan de estudios, tanto en idiomas locales como internacionales.

7d. Promover la alfabetización de datos
Se introducirá un programa de alfabetización de datos en todo el plan de estudios. El programa educará a los niños sobre la forma en que se pueden utilizar sus datos y proporcionará una comprensión básica de la economía de los datos. Se enfatizará y se fomentará el uso positivo, autónomo y creativo de las tecnologías digitales por parte de los niños; se definirán claramente los riesgos, las ventajas y los beneficios sociales del uso de la tecnología; y se tendrá como objetivo garantizar que las medidas de protección y de prevención se difundan, se comprendan y se apliquen en profundidad. En la educación sobre alfabetización de datos debe quedar claro quiénes son los responsables de la seguridad en Internet.

7e. Promover el pensamiento crítico
La educación de los niños y los de los padres/cuidadores respecto al pensamiento crítico y a los riesgos de la desinformación en Internet deben incorporarse a la educación sobre cultura digital. Lo anterior debe incluir una educación más amplia que promueva la comprensión y el conocimiento de los derechos humanos —en particular de los derechos del niño— y de sus mecanismos dentro y fuera de Internet.[38]

7f. Introducir en los colegios procedimientos formales para la seguridad infantil en Internet
La formación en materia de seguridad infantil en Internet debe ser obligatoria en las titulaciones relacionadas con la enseñanza, tanto para primaria como para secundaria, y dicha formación deberá continuar durante la carrera profesional. Todos los profesores deben completar la formación obligatoria sobre la seguridad infantil en Internet, conocer la política escolar en relación con la seguridad infantil en Internet e impartir conocimientos sobre la seguridad infantil en Internet a sus alumnos. Todos los colegios deben designar a un orientador en materia de seguridad infantil en Internet que defienda las normas de seguridad infantil en Internet y se haga cargo de hacer cumplir la política escolar sobre seguridad infantil en Internet.

8 Sensibilización del público y comunicación

8a. Crear un programa de concientización pública
Las estrategias de sensibilización ayudarán a la gente a comprender y a abordar la cuestión de la seguridad infantil en Internet para que puedan seguir disfrutando de las ventajas del espacio digital. El material que se diseñe debe dejar claros los principios de la seguridad infantil en Internet y las medidas que se pueden tomar para comprender los riesgos, mitigar los daños, denunciar los delitos y corregir/reparar, de ser necesario. Esta información se facilitará en los sitios web oficiales y en términos sencillos. El material y los mensajes específicos deben desarrollarse previa consulta con los niños, los jóvenes y los padres/cuidadores. Se deben tener en cuenta las necesidades específicas de los padres/cuidadores y de los niños, con especial atención para los niños más pequeños y vulnerables, incluidos los que tienen dificultades de aprendizaje o los que no cuentan con orientación parental. La educación entre pares es una estrategia valiosa para que los niños de todas las edades conozcan sus derechos y sus responsabilidades en Internet. Este programa de mensajes públicos puede ayudar a los niños y a los adultos a comprender los problemas y a tomar decisiones acertadas en sus interacciones en Internet, pero no sustituye la educación formal, la formación profesional, la seguridad por diseño ni la responsabilidad corporativa. Dicha información debe abarcar todo el abanico de problemas de la seguridad infantil en Internet, tal y como se establece en esta política.

Las cinco cuestiones transversales
1. Identificar riesgos y mitigar daños
2. Promover el acceso, la accesibilidad y la inclusión
3. Crear una cadena de responsabilidad y de colaboración
4. Integrar un diseño centrado en niñas, niños y adolescentes
5. Garantizar la eficacia

Las diez áreas de acción de la política
1. Capacidad institucional
2. Marcos jurídicos y reguladores
3. Datos personales, identidad y autonomía
4. Sistemas de respuesta y de apoyo
5. Responsabilidad corporativa
6. Formación
7. Educación
8. Sensibilización del público y comunicación
9. Investigación y desarrollo
10. Cooperación global

38. Véase el artículo 29 de la Convención sobre los Derechos del Niño y las secciones pertinentes de la observación general.

8b. Proporcionar información y materiales educativos accesibles
La educación sobre seguridad en Internet comenzará en la primera infancia y se desarrollará de acuerdo con las necesidades cambiantes de los niños a medida que crecen. Se creará material específico para guiar y apoyar a los niños de todas las edades, así como a sus familias y cuidadores. El material de información promoverá el uso positivo de la tecnología digital y tocará cuestiones como la sexualidad y el consentimiento. Asimismo, se tendrán en cuenta las necesidades de todos los niños, independientemente de su género, su edad, su nivel económico o su contexto sociocultural. La información que se proporcione a través de terceros reflejará los derechos y los principios de los niños y tendrá como objetivo ayudar a los niños de todas las edades a conocer los riesgos que corren y sus derechos en Internet. El material debe dejar claro que los niños y los usuarios no son responsables cuando les suceden cosas malas. Los grupos comunitarios, los clubes juveniles, las familias, las instituciones religiosas y las plataformas digitales desempeñarán un papel decisivo en la sensibilización sobre la seguridad infantil en Internet y en la educación informal a nivel comunitario.

8c. Sensibilizar sobre la seguridad infantil en Internet a través de los medios de comunicación
Debe facilitarse información adaptada para los niños que complemente la cobertura mediática de los problemas de seguridad infantil en Internet. Las empresas de comunicación y de entretenimiento deben estar familiarizadas con la cuestión de la seguridad infantil en Internet y se les debe alentar a apoyar campañas de sensibilización pública, cuando proceda, de una manera equilibrada, responsable e informativa. Debe darse cobertura a todo el abanico de cuestiones relacionadas con la seguridad infantil en Internet, no solo a los titulares más sensacionalistas.

8d. Involucrar a padres/cuidadores y a niños en diálogos sobre la seguridad infantil en Internet
Los padres/cuidadores y las familias deben estar capacitados para comprender lo que implica la seguridad infantil en Internet y para tomar medidas al respecto en casa. Es necesario hablar con las familias y con los niños para identificar los problemas, las soluciones y la manera de concienciar de manera efectiva respecto a la seguridad infantil en Internet en sus comunidades.

9 Investigación y desarrollo

9a. Establecer marcos de trabajo para la investigación de la seguridad infantil en Internet
Los países deben establecer un fondo central de investigación para desarrollar un programa de investigación con términos de referencia y objetivos claramente definidos que no queden obsoletos, a fin de facilitar las investigaciones en curso sobre la seguridad infantil en Internet en relación con diversas cuestiones de relevancia. Siempre que sea posible, los países deben ponerse en contacto y cooperar entre sí en la investigación y el desarrollo de la seguridad infantil en Internet. El análisis de las carencias debería ayudar a garantizar que se dé prioridad a los recursos de las áreas con mayores necesidades y a evitar duplicaciones innecesarias. La investigación debe ponerse a disposición de los colaboradores regionales o internacionales, en particular los que cuentan con menos recursos.

9b. Innovación continua
Las evidencias que se extraigan de las investigaciones servirán de referencia para el desarrollo de productos y servicios que incorporen la seguridad por diseño. Asimismo, facilitarán la evaluación de las prácticas de seguridad infantil en Internet y proporcionarán una comprensión de las experiencias y de las soluciones relativas al uso de Internet por parte de los niños en el contexto nacional.

9c. Establecer centros de excelencia en investigación y desarrollo de la seguridad infantil en Internet
Los países deben desarrollar centros de excelencia dentro de las instituciones existentes —universidades, centros sanitarios, centros de innovación— que puedan trabajar juntos en el desarrollo de herramientas, servicios y habilidades relacionadas con la seguridad de los niños en Internet a través de la participación nacional, regional e internacional.

9d. Establecer marcos de trabajo éticos y sólidos para la investigación y el desarrollo en materia de seguridad infantil en Internet[39]
Los países deben desarrollar directrices para los investigadores que trabajan en el ámbito de la seguridad infantil en Internet, lo que incluye tener en cuenta los derechos de los niños de una manera efectiva como parte del proceso de investigación. Debe incluirse una orientación clara sobre la recopilación de datos y las

39. Children and the Data Cycle: Rights and Ethics in a Big Data World (Niños y el ciclo de los datos: derechos y ética en el mundo del Big Data), Fondo de las Naciones Unidas para la Infancia, 2017.

implicaciones éticas, y respecto a los derechos, del procesamiento de los datos de los niños. Los intereses del niño deben ser la consideración principal de los marcos de trabajo éticos para la investigación y el desarrollo sobre la seguridad infantil en Internet, incluso en los escenarios en los que el acceso sea una cuestión de interés público.

9e. Establecer marcos de trabajo para la recopilación de información
Los reguladores que trabajan en el ámbito de la seguridad infantil en Internet deben establecer marcos de trabajo para la recopilación de información que les permitan supervisar y evaluar la efectividad de la seguridad infantil en Internet en diferentes contextos y el impacto que tiene en diferentes grupos de niños. La supervisión y la evaluación de las medidas relacionadas con la seguridad infantil en Internet deben formar parte del proceso de investigación y desarrollo.

9f. Permitir el acceso a los datos de las empresas privadas por el bien del interés general
Se deben crear marcos de trabajo en los que las redes sociales y otras empresas estén obligadas a compartir sus datos para respaldar las investigaciones que se realizan en el interés superior del niño.

9g. Garantizar que los datos y las estadísticas se ajusten al contexto
Los modelos estadísticos deben reflejar el panorama local, para propiciar una mejora en la comprensión de las cuestiones locales y en la respuesta a las mismas. Deben facilitar, además, el seguimiento de los efectos transfronterizos.

10 Cooperación global

10a. Establecer marcos de trabajo formales de relación —por ejemplo, un «Memorando de entendimiento» (MOU)— conlas comunidades regionales y globales de seguridad infantil en Internet
El fortalecimiento de la cooperación internacional a lo largo y ancho del planeta en la mejora de la seguridad infantil en Internet es fundamental para garantizar la seguridad a nivel global. Los países deben formalizar colaboraciones para inversiones conjuntas de asociaciones público-privadas en áreas relacionadas con, entre otras cuestiones, la ciberseguridad, el desarrollo de capacidades de seguridad infantil en Internet, la innovación, la aplicación de la ley, el sistema judicial y la educación.

10b. Adscribirse a los instrumentos jurídicos regionales e internacionales que promueven la cooperación en materia de seguridad infantil en Internet
Los países deben identificar instrumentos clave a nivel regional e internacional que les permitan cooperar con otros países en materia de seguridad infantil en Internet. Esto debería incluir, entre otras cosas: acuerdos internacionales sobre cooperación en materia de cumplimiento de la ley; prácticas recomendadas internacionales; programas internacionales que puedan proporcionar recursos para la cooperación en materia de seguridad infantil en Internet; y acceso a cualquier normas sobre derechos humanos o similares que faciliten la cooperación entre los países.

10c. Identificar organizaciones y países colaboradores que puedan proporcionar los modelos y el apoyo adecuados para el desarrollo de la seguridad infantil en Internet
Puede que no haga falta desarrollar las políticas desde cero. Los países deben buscar ejemplos oportunos de marcos de trabajo y de herramientas de seguridad infantil en Internet que puedan utilizar y adaptar a su propio contexto. El intercambio de información sobre los desafíos y los problemas que se detecten en materia de seguridad infantil en Internet puede ser muy valioso para la planificación, el desarrollo y la aplicación de políticas de seguridad infantil en Internet.

10d. Apoyar a otros países en el desarrollo de políticas de seguridad infantil en Internet
Cuando corresponda, convendría compartir modelos de leyes y marcos regulatorios, así como los conocimientos fruto de la experiencia u otros materiales que puedan utilizar otros países para desarrollar sus marcos de trabajo y sus políticas de seguridad infantil en Internet.[40]

40. Véase, por ejemplo, International Leadership and Collaboration Materials del Comisionado de Seguridad Electrónica de Australia, 2021.

5RIGHTS FOUNDATION

End Violence Against Children