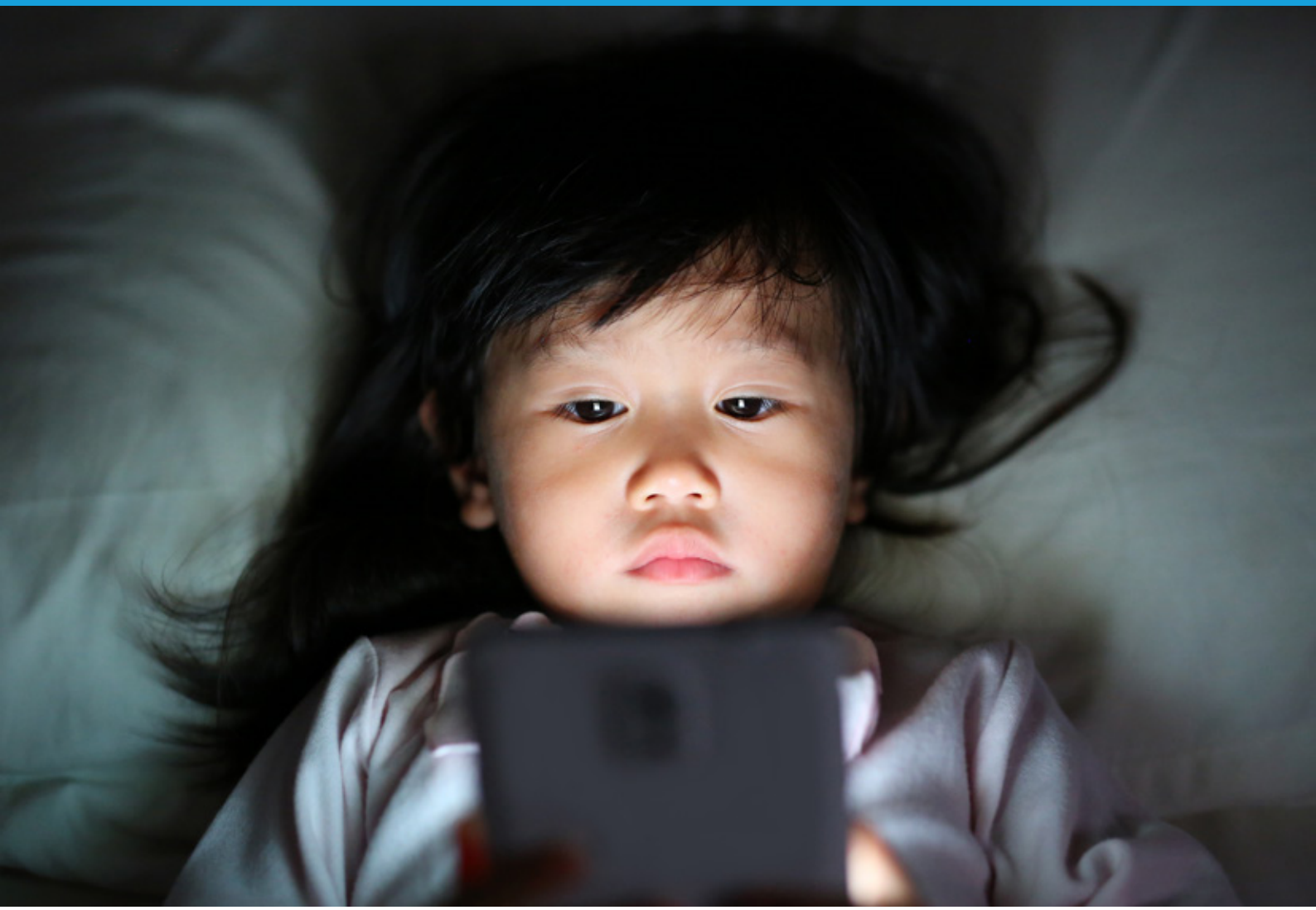
ITUPublicaciones

Unión Internacional de Telecomunicaciones
Sector de Desarrollo

Directrices sobre la protección de la infancia en línea para los encargados de formular políticas

2020



Directrices sobre la protección de la infancia en línea para los encargados de formular políticas

2020

Agradecimientos

Las presentes directrices han sido elaboradas por la Unión Internacional de Telecomunicaciones (UIT) y un grupo de trabajo integrado por autores pertenecientes a prestigiosas instituciones dedicadas al sector de las tecnologías de la información y la comunicación (TIC) y a cuestiones relacionadas con la protección de la infancia (en línea), entre las que cabe destacar las siguientes organizaciones:

ECPAT International, la red Global Kids Online, la Alianza Mundial para Acabar con la Violencia contra los Niños, el proyecto HABLATAM, la red de Centros de Internet Segura (Insafe), INTERPOL, el Centro Internacional para Niños Desaparecidos y Explotados (ICMEC), la Alianza Internacional de la Discapacidad, la Unión Internacional de Telecomunicaciones (UIT), la Escuela de Economía y Ciencias Políticas de Londres, la Oficina del Representante Especial del Secretario General sobre la Violencia contra los Niños y la Relatora Especial sobre la venta y la explotación sexual de niños, Privately SA, RNW Media, los Centros de Internet Segura del Reino Unido, la Alianza Mundial WePROTECT (WPGA) y la World Childhood Foundation de los Estados Unidos de América.

El grupo de trabajo estuvo presidido por David Wright (Centros de Internet Segura del Reino Unido/SWGfL) y coordinado por Fanny Rotino (UIT).

Estas Directrices no habrían sido posibles sin la entrega, el entusiasmo y la dedicación de los autores que contribuyeron a su elaboración. También se recibieron inestimables contribuciones de COFACE-Families Europe, el Consejo de Europa, el Comisionado de Ciberseguridad de Australia, la Comisión Europea, el e-Worldwide Group (e-WWG), la OCDE, el proyecto Youth and Media del Berkman Klein Center for Internet and Society de la Universidad de Harvard, así como gobiernos nacionales e interesados del sector privado cuyo objetivo común es hacer de Internet un lugar mejor y más seguro para los niños y jóvenes.

La UIT desea manifestar su agradecimiento a los siguientes asociados, que han contribuido con su tiempo y valiosos análisis (enumerados por orden alfabético de organización):

- Martin Schmalzried (COFACE-Families Europe)
- Livia Stoica (Consejo de Europa)
- John Carr (ECPAT International)
- Julia Fossi y Ella Serry (Comisionado de Ciberseguridad)
- Manuela Marta (Comisión Europea)
- Salma Abbasi (e-WWG)
- Amy Crocker y Serena Tommasino (Alianza Mundial para Acabar con la Violencia contra los Niños)
- Lionel Brossi (HABLATAM)
- Sandra Marchenko (ICMEC)
- Karl Hopwood (Insafe)[1]
- Lucy Richardson (Alianza Internacional de la Discapacidad)

[1] *En el marco del Mecanismo "Conectar Europa", la Red de Escuelas europeas administra, en nombre de la Comisión Europea, la plataforma "Better Internet for Kids", que incluye la coordinación de la red Insafe de Centros Europeos de Internet Segura. Se puede consultar más información en www.betterinternetforkids.eu.*

- Matthew Dompier (INTERPOL)
- Fanny Rotino (UIT)
- Tess Leyland (Internet Watch Foundation)
- Sonia Livingstone (Escuela de Economía y Ciencias Políticas de Londres y Global Kids Online)
- Elettra Ronchi (OCDE)
- Manus De Barra (Oficina del Representante Especial del Secretario General sobre la Violencia contra los Niños)
- Deepak Tewari (Privately SA)
- Pavithra Ram (RNW Media)
- Maud De Boer-Buquicchio (Relatora Especial de las Naciones Unidas sobre la venta y la explotación sexual de niños)
- David Wright (Centros de Internet Segura del Reino Unido/SWGfL)
- Iain Drennan y Susannah Richmond (Alianza Mundial WePROTECT)
- Lina Fernandez y la Dra. Joanna Rubinstein (World Childhood Foundation, Estados Unidos de América)
- Sandra Cortesi (Youth and Media)

ISBN

978-92-61-30123-1 (versión en papel)

978-92-61-30453-9 (versión electrónica)

978-92-61-30113-2 (versión EPUB)

978-92-61-30463-8 (versión Mobi)

Antes de imprimir este informe, piense en el medio ambiente.

Prefacio

En un mundo en que Internet está presente en casi todos los aspectos de la vida moderna, el mantenimiento de la seguridad de los jóvenes usuarios en línea se ha convertido es una cuestión cada vez más apremiante en todos los países.

La UIT elaboró su primer conjunto de Directrices para la protección de la infancia en línea en 2009. Desde entonces, la evolución de Internet ha transcendido lo imaginable. Si bien se ha convertido en un recurso infinitamente más enriquecedor para la recreación y el aprendizaje de los niños, también se ha transformado en un lugar mucho más peligroso para que estos se aventuren en solitario.

Los riesgos que afrontan los niños actualmente son abundantes y van desde cuestiones relacionadas con la privacidad hasta contenidos violentos e inapropiados, estafas por Internet y todo el espectro de actividades de seducción, abuso y explotación sexuales en línea. Las amenazas se multiplican y los agresores actúan cada vez más de manera simultánea en diferentes jurisdicciones, limitando con ello la eficacia de las actividades de respuesta y reparación llevadas a cabo por cada país.

Por otra parte, a raíz de la pandemia mundial de la COVID-19 aumentó repentinamente la incorporación de niños al mundo digital para cursar sus estudios y socializarse. Las restricciones impuestas por este virus hicieron que numerosos niños pequeños comenzaran a interactuar en línea a una edad mucho más temprana que la que sus padres habían previsto, y, por añadidura, muchos de ellos, ocupados en sus quehaceres laborales no pudieron supervisar a sus hijos, con el consiguiente riesgo de que estos accedieran a contenidos inapropiados o fueran blanco de delincuentes que producen material de abuso sexual infantil.

El mantenimiento de la seguridad de la infancia en línea requiere ahora más que nunca una respuesta internacional colaborativa y coordinada, que exige la participación y el apoyo activos de muchas partes interesadas, desde los actores del sector privado como las plataformas, los proveedores de servicios y los operadores de redes hasta los gobiernos y la sociedad civil.

Habida cuenta de lo anterior, los Estados Miembros de la UIT solicitaron en 2018 que la actualización de las Directrices de PIeL no se limitase a la habitual revisión periódica. Por ese motivo, estas nuevas Directrices revisadas han sido reformuladas, reescritas y rediseñadas, con el fin de integrar los muy significativos cambios en el panorama digital en el que se encuentran los niños.

Además de responder a los nuevos adelantos en las tecnologías y plataformas digitales, esta nueva edición examina un importante tema pendiente: la situación de los niños con discapacidades, a quienes el mundo en línea brinda la oportunidad especialmente vital de participar plenamente en la sociedad. También se han tenido en cuenta las necesidades especiales de los niños migrantes y otros grupos vulnerables.

Esperamos que las presentes directrices ofrezcan a los encargados de formular políticas una base sólida para elaborar estrategias nacionales multipartitas e inclusivas, que abarquen la celebración de consultas y debates abiertos con niños, a fin de concebir medidas mejor orientadas y acciones más eficaces.

Al preparar estas nuevas directrices, la UIT y sus asociados procuraron crear un marco sumamente práctico, flexible y adaptable, firmemente asentado en las normas y los objetivos

compartidos a escala internacional, en particular la Convención sobre los Derechos del Niño y los Objetivos de Desarrollo Sostenible de las Naciones Unidas. Fiel al verdadero espíritu de la UIT, en su función de coordinador mundial, me siento orgullosa de que estas directrices revisadas sean el fruto de una colaboración mundial y hayan sido redactadas conjuntamente por expertos internacionales procedentes de una amplia comunidad multipartita.

Asimismo, me complace presentar a Sango, nuestra nueva mascota de la PIeL, un personaje amistoso, enérgico e intrépido concebido enteramente por un grupo de niños, en el marco del nuevo programa internacional de divulgación de la UIT destinado a la juventud.

En una época en la que son cada vez más los jóvenes conectados a Internet, estas Directrices de PIeL resultan más indispensables que nunca. Los encargados de formular políticas, miembros del sector privado, padres, educadores y los propios niños desempeñan un papel fundamental en esta esfera. Una vez más, les agradezco su apoyo y espero que nuestra estrecha colaboración en torno a esta cuestión vital siga prosperando.

Doreen Bogdan-Martin
Directora de la Oficina de Desarrollo de las Telecomunicaciones

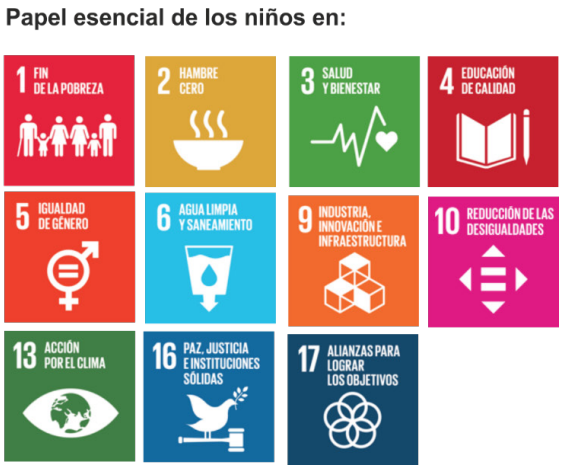
Prefacio

Hace 30 años, casi todos los gobiernos se comprometieron a respetar, proteger y promover los derechos del niño. La Convención de las Naciones Unidas sobre los Derechos del Niño es el tratado internacional de derechos humanos que ha recibido el mayor número de ratificaciones en la historia. Si bien en los tres últimos decenios se han logrado avances importantes, aún sigue habiendo desafíos considerables y también han salido a la luz nuevos focos de riesgo para la infancia.

En 2015, todas las naciones reafirmaron su compromiso con la infancia, al apoyar la Agenda 2030 y los 17 Objetivos de Desarrollo Sostenible (ODS) universales. Por ejemplo, en la meta 16.2 de los ODS se aboga por poner fin al maltrato, la explotación y todas las formas de violencia y tortura contra los niños a más tardar en 2030. No obstante, la protección de la infancia constituye un denominador común de 11 de los 17 ODS. Como se ilustra en la Figura 1, UNICEF sitúa a la infancia en el centro de la Agenda 2030.

Figura 1: Infancia, TIC y ODS

#ICT4SDG



La Agenda 2030 para el Desarrollo Sostenible reconoce que las TIC posibilitan de manera decisiva el logro de los ODS. La expansión de las tecnologías de la información y la comunicación (TIC) y la interconexión mundial brinda posibilidades para acelerar el progreso humano, reducir la brecha digital y desarrollar sociedades del conocimiento. En la Agenda también se definen metas específicas relacionadas con la utilización de las TIC para el desarrollo sostenible en las esferas de la educación (Objetivo 4), la igualdad de género (Objetivo 5), la infraestructura (Objetivo 9 - acceso universal y asequible a Internet) y las alianzas y los medios para su puesta en práctica (Objetivo 17)[1]. Las TIC tienen la capacidad de transformar profundamente la economía en su conjunto al ser un factor decisivo en el logro de todos y cada uno de los 17 ODS. Asimismo, ya han comenzado su contribución al respecto, al empoderar a miles de millones de personas en todo el mundo dándoles acceso a recursos educativos y sanitarios, además de a servicios como el cibergobierno y los medios sociales, por sólo citar algunos.

[1] PNUD, Objetivos de Desarrollo Sostenible, undp.org, consultado el 29 de enero de 2020, https://www.undp.org/content/undp/es/home/sustainable-development-goals.html; Houlin Zhao, *Why ICTs Are so Crucial to Achieving the SDGs*; UIT, Revista Actualidades de la UIT, núm. 48, consultado el 29 de enero de 2020, https://www.itu.int/en/itunews/Documents/2017/2017-03/2017_ITUNews03-es.pdf.

El auge de las tecnologías de la información y la comunicación ha generado oportunidades sin precedentes para que los niños y jóvenes comuniquen, interactúen, intercambien, aprendan, accedan a la información y expresen su opinión sobre asuntos que inciden en sus vidas y sus comunidades.

Sin embargo, la ampliación y facilitación del acceso disponible a Internet y a las tecnologías móviles también plantea retos considerables para la seguridad y el bienestar de los niños, tanto en línea como fuera de línea.

A fin de reducir los riesgos del mundo digital y permitir al mismo tiempo que un mayor número de niños y jóvenes aprovechen sus beneficios, los gobiernos, la sociedad civil, las comunidades locales, las organizaciones internacionales y el sector deben unir sus esfuerzos en torno a un objetivo común. En particular, es necesario que los encargados de formular políticas se impliquen a fin de lograr el objetivo internacional de mantener la seguridad de la infancia en línea.

Con miras a responder a los desafíos que plantea la rápida evolución de las TIC y a los correspondientes retos que suponen para la protección de la infancia, la Unión Internacional de Telecomunicaciones (UIT) lanzó en noviembre de 2008 la Iniciativa para la Protección de la Infancia en Línea (PIeL) en forma de iniciativa internacional multipartita. Esta iniciativa tiene por objeto reunir a los asociados de todos los sectores de la comunidad mundial a fin de crear una experiencia en línea segura y formadora para los niños de todo el mundo.

Además, en la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones celebrada en Dubái en 2018 se reafirmó la importancia de la Iniciativa para la PIeL, al reconocerla como una plataforma para crear conciencia, compartir las prácticas idóneas y brindar asistencia y apoyo a los Estados Miembros, especialmente a los países en desarrollo, en la elaboración y aplicación de las hojas de ruta en relación con la PIeL. En ella también se reconoció la importancia de la protección de la infancia en línea en el marco de la Convención de las Naciones Unidas sobre los Derechos del Niño y de otros tratados de derechos humanos, alentando la colaboración entre todos los interesados implicados en la protección de la infancia en línea.

La Conferencia reconoció la Agenda 2030 para el Desarrollo Sostenible, en la que se abordan diversos aspectos de la protección de la infancia en línea en el marco de los Objetivos de Desarrollo Sostenible (ODS), en particular los ODS 1, 3, 4, 5, 9, 10 y 16; también reconoció la Resolución 175 (Rev. Dubái, 2018), sobre la accesibilidad de las telecomunicaciones/tecnologías de la información y la comunicación (TIC) para las personas con discapacidad y personas con necesidades especiales, y la Resolución 67 (Rev. Buenos Aires, 2017) de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT), sobre la función del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D)) en la protección de la infancia en línea.

A finales de 2019, la Comisión de la Banda Ancha para el Desarrollo Sostenible de la UIT y la UNESCO publicó un informe sobre la seguridad de la infancia en línea con recomendaciones concretas para conseguir que Internet sea más seguro para los niños.

En 2009, la UIT publicó el primer conjunto de directrices sobre la protección de la infancia en línea en el marco de la Iniciativa para la PIeL. Durante los últimos diez años, las Directrices de PIeL se han traducido en muchas lenguas y numerosos países de todo el mundo las han utilizado como referencia para elaborar hojas de ruta y estrategias nacionales relacionadas con la protección de la infancia en línea. Han sido útiles en las medidas destinadas a la protección de la infancia en línea por parte de entidades gubernamentales nacionales, organizaciones de

la sociedad civil, instituciones de atención de la infancia, miembros del sector privado y otras muchas partes interesadas.

Más concretamente, las directrices se han utilizado para redactar, elaborar y aplicar estrategias nacionales de protección de la infancia en línea en muchos Estados Miembros como Camerún, Gabón, Gambia, Ghana, Kenya, Sierra Leona, Uganda y Zambia en la región de África; Bahréin y Omán en la región árabe; Brunei, Camboya, Kiribati, Indonesia, Malasia, Myanmar y Vanuatu en la región de Asia y el Pacífico; y Bosnia, Georgia, Moldova, Montenegro, Polonia y Ucrania en la región de Europa.

Además, las directrices han sembrado los cimientos de eventos regionales como la Conferencia Regional sobre la Protección de la Infancia en Línea para África (ACOP), centrada en el empoderamiento de los futuros ciudadanos digitales y celebrada en Kampala, Uganda (2014), y la Conferencia Regional de la Asociación de Naciones de Asia Sudoriental (ASEAN) sobre la Protección de la Infancia en Línea, celebrada en Bangkok, Tailandia (2020).

En virtud de la Resolución 179 (Rev. Dubái, 2018), la UIT, en colaboración con los asociados de la iniciativa para la PIeL y las partes interesadas, recibió el cometido de actualizar los cuatro conjuntos de directrices teniendo en cuenta los avances tecnológicos logrados en el sector de las telecomunicaciones, incluidas las directrices destinadas a los niños con discapacidad y con necesidades específicas.

Como resultado de dicho proceso, estas directrices han sido actualizadas y examinadas de manera considerable por expertos e interesados pertinentes, que han definido un amplio conjunto de recomendaciones para mantener la seguridad de la infancia en el mundo digital. Constituyen el fruto de la colaboración entre múltiples partes interesadas y aúnan los conocimientos, la experiencia y el bagaje especializado de muchas organizaciones y particulares de todo el mundo en el ámbito de la protección de la infancia en línea. Con ellas se persigue el objetivo de sentar las bases de un mundo cibernético seguro para las futuras generaciones. La finalidad es que estas directrices sirvan de referencia y se adapten y utilicen en consonancia con las costumbres y leyes nacionales o locales. Además, en ellas se abordan cuestiones que afectan a todos los niños y jóvenes menores de 18 años, a la vez que se reconocen las diferentes necesidades de cada grupo de edad. Asimismo, tienen por objeto atender las necesidades de los niños con condiciones de vida diferentes y los niños con necesidades especiales y discapacidad. Las directrices también refuerzan el alcance de la protección de la infancia en línea, ya que abordan todos los riesgos, amenazas y daños a los que los niños se pueden exponer en línea y los sopesan detenidamente con las ventajas que el mundo digital puede aportar a las vidas de esos niños.

Se espera que con estas directrices no solo se consiga construir una sociedad de la información más inclusiva, sino también que los Estados Miembros de la UIT puedan cumplir sus obligaciones de proteger y hacer efectivos los derechos del niño, estipuladas en la Convención sobre los Derechos del Niño[2], adoptada por la Asamblea General de las Naciones Unidas en su

[2] UNICEF, La Convención sobre los Derechos del Niño, uncief.org, consultado el 29 de enero de 2020, https://www.unicef.org/es/convencion-derechos-nino.

Resolución 44/25 de 20 de noviembre de 1989, y en el Documento de Resultados de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)[3].

Mediante la publicación de estas directrices, la Iniciativa para la PIeL hace un llamamiento a todos los interesados para que adopten políticas y estrategias encaminadas a proteger a los niños en el ciberespacio y fomenten su acceso seguro a todas las extraordinarias oportunidades que pueden ofrecer los recursos en línea.

[3] La CMSI se celebró en dos fases: la primera en Ginebra (del 10 al 12 de diciembre de 2003) y la segunda en Túnez (del 16 al 18 de noviembre de 2005). La CMSI concluyó con el firme compromiso de "construir una sociedad de la información centrada en las personas, integradora y orientada hacia el desarrollo, en la que todos puedan crear, utilizar y compartir información y conocimientos y acceder a ellos".

Índice

Lista de cuadros, figuras y recuadros

Cuadros

Figuras

Recuadros

1 Presentación del documento

1.1 Finalidad

Los gobiernos nacionales tienen la obligación de proteger a los niños tanto en el mundo físico como en el virtual. En buena medida ya no tiene sentido tratar de mantener una distinción rígida entre los eventos del mundo real y los eventos en línea, pues hoy en día las nuevas tecnologías se encuentran absolutamente integradas en la vida de incontables niños y jóvenes de diversas formas importantes. Ambos mundos están cada vez más entrelazados y son cada vez más interdependientes.

Los encargados de formular políticas[1] y los demás interesados pertinentes tienen cometidos muy importantes en esta esfera. Dada la velocidad a la que evolucionan las tecnologías, muchos de los métodos tradicionales para formular políticas han perdido su utilidad. Los encargados de formular políticas han de elaborar un marco jurídico que sea adaptable, inclusivo y adecuado para su finalidad, a fin de lograr que la era digital de rápida evolución proteja a la infancia en línea.

Las presentes directrices tienen por objeto ofrecer a los encargados de formular políticas de los Estados Miembros de la UIT un marco flexible y fácil de utilizar para que entiendan y cumplan su obligación legal de proteger a los niños tanto en el mundo real (físico) como en el virtual.

Esto se consigue abordando diversas cuestiones importantes para los encargados de formular políticas:

1) ¿En qué consiste la protección de la infancia en línea?
2) ¿Por qué debo preocuparme por la protección de la infancia en línea, en mi condición de encargado de formular políticas?
3) ¿Cuál es el contexto jurídico, sociopolítico y de desarrollo de mi país?
4) ¿Cómo deben los encargados de formular políticas empezar a examinar y dar forma a una política de protección de la infancia en línea que sea eficaz y sostenible en sus correspondientes países?

Para abordar estas cuestiones, las directrices se basan en modelos, marcos y recursos actuales a fin de contextualizar y aportar información sobre buenas prácticas aplicadas en todo el mundo.

1.2 Alcance

El alcance de la protección de la infancia en línea cubre todo daño al que se exponen los niños en línea, abarcando una amplia variedad de riesgos que suponen una amenaza para su seguridad y bienestar. Se trata de un problema complejo que se debe abordar desde diversas perspectivas, entre otras las relativas a la legislación, la gobernanza, la educación, la política y la sociedad.

Además, la protección de la infancia en línea se debe basar en un entendimiento de los riesgos, amenazas y daños a que se enfrentan los niños en los entornos digitales, tanto de manera general como en cada país. Para ello, es preciso contar con definiciones claras y definir parámetros de intervención inequívocos que abarquen y establezcan una distinción entre los

[1] En este documento, el término encargados de formular políticas engloba todos los interesados que se ocupan de la elaboración y aplicación de políticas, en particular los que forman parte del gobierno.

actos delictivos y otros que, aunque no son ilegales, suponen no obstante una amenaza para el bienestar del niño.

A tales efectos, las directrices proporcionan un panorama de las amenazas y daños a los que se exponen actualmente los niños en los entornos digitales. Dicho esto, en vista de la velocidad a la que las tecnologías y las amenazas y daños conexos evolucionan a día de hoy, el tradicional ritmo y método para elaborar políticas no bastan para adaptarse a dicha evolución. Los encargados de formular políticas en la era digital tienen que elaborar marcos jurídicos y políticos que sean lo suficientemente adaptables e inclusivos para afrontar los retos actuales y, en la medida de lo posible, anticipar los futuros. Para ello, es necesario que colaboren con todos y cada uno de los interesados, incluidos el sector de las TIC, la comunidad científica, la sociedad civil, la población y los propios niños. Este proceso se puede facilitar teniendo en cuenta los principios fundamentales de la protección de la infancia en línea.

1.3 Principios fundamentales

En esta sección se exponen 11 principios transversales que, en su conjunto, servirán para elaborar una estrategia nacional de protección de la infancia en línea integral y con miras de futuro.

Se presentan siguiendo una lógica narrativa y no por orden de importancia.

Toda estrategia nacional de protección de la infancia en línea debe:

1) basarse en una visión integral que incluya al gobierno, el sector privado y la sociedad;
2) derivarse de un entendimiento y análisis exhaustivos del entorno digital general y a su vez adaptarse a las circunstancias y prioridades del país;
3) respetar y estar en consonancia con los derechos fundamentales de los niños, consagrados en la Convención de las Naciones Unidas sobre los Derechos del Niño y otros instrumentos internacionales y leyes fundamentales;
4) respetar y estar en consonancia con las leyes y estrategias nacionales similares y conexas que estén en vigor, como las leyes sobre el maltrato infantil y las estrategias en materia de seguridad de los niños;
5) respetar los derechos civiles y las libertades de los niños, que no se deben sacrificar a expensas de su protección;
6) elaborarse con la participación activa de todos los interesados pertinentes, incluidos los niños, abordando sus necesidades y responsabilidades y atendiendo las necesidades de las minorías y los grupos marginados;
7) concebirse de manera que se ajuste a los planes generales del Gobierno para la prosperidad económica y social y optimice la contribución de las TIC al desarrollo sostenible y la integración social;
8) servirse de los instrumentos de política más apropiados de que se disponga a fin de lograr su objetivo, teniendo en cuenta las circunstancias específicas del país;
9) establecerse en el más alto nivel del Gobierno, que tendrá la responsabilidad de atribuir las funciones y responsabilidades pertinentes y asignar suficientes recursos humanos y financieros;
10) contribuir a la construcción de un entorno digital en el que puedan confiar los niños, los padres/cuidadores y las partes interesadas;
11) orientar la labor de las partes interesadas para empoderar y formar a los niños en materia de alfabetización digital a fin de que se protejan mientras realizan actividades en línea.

1.4 Utilización de estas directrices

En estas directrices se examinan la investigación pertinente y los modelos y materiales existentes, y se establecen recomendaciones claras para elaborar una estrategia nacional de protección de la infancia en línea.

- En la sección 2 se ofrece una introducción a la protección de la infancia en línea y se facilitan datos sobre investigaciones recientes, entre otros, aspectos relativos a las nuevas tecnologías emergentes, las principales amenazas y los daños a que se exponen los niños.
- En la sección 3 se expone la manera en que se debe preparar una estrategia nacional de protección de la infancia en línea, indicando entre otras cosas las partes interesadas pertinentes, algunos ejemplos de respuestas a las amenazas y daños en línea y las ventajas de contar con una estrategia nacional.
- En la sección 4 se formulan recomendaciones sobre la elaboración de marcos y su aplicación.
- En la sección 5 se expone una serie de actividades que se han de llevar a cabo en cada país para elaborar una estrategia de protección de la infancia en línea.
- En la sección 6 se facilitan materiales de referencia de utilidad.

2 Introducción

En 2019, más de la mitad de la población mundial utilizaba Internet. Los menores de 44 años conforman el grueso de los usuarios y se registran niveles de uso igualmente elevados en las personas de edades comprendidas entre 16 y 24 años y entre 35 y 44 años. A nivel mundial, uno de cada tres niños utiliza Internet (de 0 a 18 años)[2]. En los países en desarrollo, los niños y los jóvenes encabezan la utilización de Internet[3] y se estima que esta población se duplicará con creces en los próximos cinco años. Las nuevas generaciones están creciendo con Internet y la mayoría se conectan a ella con tecnologías de redes móviles, especialmente en el hemisferio sur[4].

Aunque el acceso a Internet es fundamental para hacer efectivos los derechos del niño, sigue presentando importantes diferencias en función de las regiones, los países, el género y otros factores que limitan las oportunidades de las niñas, los niños con discapacidad, los pertenecientes a minorías y otros grupos vulnerables. En lo que respecta a la brecha digital de género, las investigaciones muestran que en todas las regiones, salvo en los Estados Unidos de América, el número de usuarios de Internet de sexo masculino es muy superior al número de usuarios de sexo femenino. En muchos países, las niñas no tienen las mismas oportunidades de acceso que los niños y, cuando las tienen, no solo están sujetas a una vigilancia y restricciones mucho más estrictas respecto de su utilización de Internet, sino que además pueden poner en peligro su seguridad al intentar acceder a Internet[5]. Asimismo, es evidente que los niños y jóvenes que carecen de competencias digitales o hablan idiomas minoritarios no pueden encontrar fácilmente contenidos pertinentes en línea, y que los niños de las zonas rurales no disponen de las mismas competencias en materia digital, pasan más tiempo en línea (especialmente jugando) y son objeto de una mediación y supervisión parental menor[6].

No obstante, es imposible hablar de los riesgos y amenazas sin reconocer a la vez el carácter extremadamente enriquecedor y capacitador de la tecnología digital. Internet y las tecnologías digitales están transformando nuestros modos de vida y han creado numerosas formas nuevas de comunicarse, jugar, disfrutar de la música y participar en un amplio abanico de actividades culturales, educativas y de capacitación. Internet puede facilitar un acceso fundamental a los servicios sanitarios y educativos y ofrecer información sobre temas que revisten importancia para los jóvenes pero que pueden ser tabú en sus sociedades.

---

2 OCDE, *New Technologies and 21st Century Children: Recent Trends and Outcomes*, Documento de Trabajo de la OCDE núm. 179 (Dirección de Educación y Competencias de la OCDE), consultado el 27 de enero de 2020, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage=En.

3 Ofcom, *Children and Parents: Media Use and Attitudes Report 2018*, consultado el 17 de enero de 2020, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf.

4 UIT, *Measuring the Information Society Report*, consultado el 16 de enero de 2020, https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

5 *Young Adolescents and Digital Media: Uses, Risks and Opportunities in Low-and Middle-Income Countries*, GAGE, consultado el 29 de enero de 2020, https://www.gage.odi.org/publication/digital-media-risks-opportunities/.

6 Livingstone, S., Kardefelt Winther, D. y Hussein, M. (2019). *Global Kids Online Comparative Report, Innocenti Research Report*. Oficina de Investigación de UNICEF, Centro de Investigación Innocenti, Florencia, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html. Esto puede dar lugar a resultados inesperados. Por ejemplo, las investigaciones realizadas por HABLATAM en cinco países de América Latina han demostrado que los niños de las comunidades vulnerables pueden utilizar las plataformas de citas, los videojuegos y las redes sociales para realizar operaciones monetarias con fines ilícitos. Red Conectados al Sur, "Hablatam", Proyecto Hablatam de 2020, consultado el 6 de febrero de 2020, https://hablatam.net/es/.

Así como los niños y los jóvenes suelen estar a la vanguardia de la adopción de las nuevas posibilidades que Internet ofrece y de la adaptación al cambio, también están expuestos a una serie de problemas relacionados con la seguridad y el bienestar que la sociedad debe reconocer y afrontar. Es fundamental debatir abiertamente los riesgos a los que se exponen los niños y los jóvenes en línea.

El debate ofrece un foro en el que se puede enseñar a los niños y jóvenes a reconocer los riesgos y prevenir o abordar los daños si llegan a producirse, así como a aprovechar las ventajas y oportunidades que Internet puede ofrecer.

En muchas partes del mundo, los jóvenes entienden adecuadamente algunos de los riesgos a que se enfrentan en línea[7], [8]. Por ejemplo, las investigaciones han demostrado que la mayoría de los niños y jóvenes son capaces de distinguir entre el ciberacoso y las bromas o burlas en línea. Si bien reconocen que el ciberacoso tiene una dimensión pública cuya finalidad es causar daño, sigue siendo difícil encontrar un equilibrio entre las oportunidades y los riesgos en línea para los niños[9].

Para los Estados Miembros de la UIT, la protección de los niños y jóvenes en línea sigue siendo una prioridad que debe sopesarse detenidamente con las medidas encaminadas a promover las oportunidades que Internet les ofrece[10], y que debe lograrse de una manera que no afecte al acceso de estos o de la población general a la información, ni a la capacidad de disfrutar de las libertades de expresión y de asociación.

Es evidente que se deben realizar inversiones específicas y diseñar soluciones creativas para abordar los riesgos que encaran los niños y jóvenes, sobre todo en vista de la brecha digital existente entre menores y adultos, que limita la orientación brindada por los padres, profesores y tutores. Al mismo tiempo, a medida que los niños y jóvenes crecen y se convierten en adultos, padres y miembros activos de la sociedad, esto brinda una posible e ineludible oportunidad para que ellos reduzcan a su vez la brecha digital.

Teniendo en cuenta lo anterior, el fomento de la confianza en Internet debe estar en primera línea y en el centro de las políticas públicas. Los gobiernos y la sociedad deben trabajar con los niños y los jóvenes para entender sus perspectivas y suscitar un verdadero debate público sobre los riesgos y las oportunidades. Ayudar a los niños y jóvenes a gestionar los riesgos en línea puede ser una medida eficaz, pero los gobiernos también deben velar por que haya servicios de apoyo adecuados para quienes sufren situaciones dañinas en línea, y por que los menores sepan cómo acceder a esos servicios.

Algunos países tienen dificultades a la hora de asignar suficientes recursos para abordar la alfabetización digital y la seguridad de la infancia en línea. Sin embargo, los niños comunican que la función de los padres, profesores, empresas tecnológicas y gobiernos es importante para elaborar soluciones encaminadas a respaldar su seguridad en línea. Los Estados Miembros de la UIT también han indicado que se presta un importante apoyo para la mejora del intercambio

[7] Desde 2016, la UIT celebra consultas con niños y adultos interesados en el marco de la Iniciativa para la PIeL sobre cuestiones pertinentes como el ciberacoso, la alfabetización digital y las actividades de los niños en línea.

[8] UIT, Consulta a los jóvenes, https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx.

[9] UNICEF, *Global Kids Online Comparative Report* (2019).

[10] UIT, *Celebrating 10 Years of Child Online Protection,* Actualidades de la UIT, 6 de febrero de 2018, https://news.itu.int/celebrating-10-years-child-online-protection/.

de conocimientos y la coordinación de actividades a fin de garantizar la seguridad de un mayor número de niños en línea[9].

Los niños y jóvenes se enfrentan a un mundo digital cada vez más complejo y la adopción de la inteligencia artificial para el aprendizaje automático, la analítica de macrodatos, la robótica, la realidad virtual y aumentada y la Internet de las cosas van a transformar los medios que utilizan. Esto requiere que se elaboren políticas y se realicen inversiones tanto para los niños, padres y comunidades del futuro como para los de hoy.

2.1 ¿En qué consiste la protección de la infancia en línea?

Las tecnologías en línea ofrecen muchas posibilidades para que los niños y jóvenes comuniquen, adquieran nuevas habilidades, sean creativos y contribuyan a crear una sociedad mejor. Sin embargo, también entrañan nuevos riesgos. Por ejemplo, pueden exponerlos a problemas en materia de privacidad, contenido ilícito, acoso, ciberacoso, uso inadecuado de datos personales o seducción con fines sexuales e incluso abuso sexual de menores.

Las presentes directrices exponen un enfoque integral para responder a todas las posibles amenazas y daños a que se exponen los niños y jóvenes cuando adquieren habilidades digitales. En ellas se reconoce el papel que desempeñan todos los interesados pertinentes en su resiliencia digital, bienestar y protección, al tiempo que se aprovechan las oportunidades que Internet puede ofrecer.

La protección de los niños y jóvenes es una responsabilidad compartida e incumbe a todos los interesados pertinentes garantizar un futuro sostenible para todos. Para ello, los encargados de formular políticas, el sector privado, los padres, cuidadores, educadores y otros interesados deben velar por que los niños y jóvenes desarrollen todo su potencial, tanto en línea como fuera de línea.

Si bien no existe ninguna definición universal de la protección de la infancia en línea, las presentes directrices tienen por objeto adoptar un enfoque integral a fin de crear espacios digitales para niños y jóvenes que sean seguros, apropiados para su edad, inclusivos y participativos, y se caractericen por lo siguiente:

- la respuesta, el apoyo y la autoayuda frente a la amenaza;
- la prevención de daños;
- un equilibrio dinámico entre el hecho de brindar protección y el de ofrecer oportunidades para que los niños sean ciudadanos digitales;
- el respeto de los derechos y el cumplimiento de las responsabilidades tanto de los niños como de la sociedad.

Además, debido a los rápidos avances de la tecnología y la sociedad y la inexistencia de fronteras para Internet, la protección de la infancia en línea debe ser ágil y adaptable para ser efectiva. Si bien en las presentes directrices se presentan los principales riesgos para los niños y jóvenes en línea, como el contenido perjudicial e ilícito, el acoso, el ciberacoso, el uso inadecuado de datos personales o la seducción con fines sexuales y el abuso y explotación sexual de menores, la evolución de las innovaciones tecnológicas acarreará nuevos desafíos, que a menudo variarán de una región a otra. No obstante, dado que los nuevos desafíos requieren nuevas soluciones, se afrontarán mejor si se colabora en el marco de una comunidad mundial.

2.2 Los niños en el mundo digital

Internet ha transformado nuestra manera de vivir. Su total integración en la vida de los niños y jóvenes desdibuja los límites entre el mundo físico y el digital. A día de hoy, un tercio de los usuarios de Internet son niños y jóvenes, y UNICEF estima que el 71% de los jóvenes ya están en línea.

Esta conectividad ha sido sumamente capacitadora. El mundo en línea permite a los niños y jóvenes superar sus desventajas y discapacidades, y ha proporcionado nuevos espacios para el entretenimiento, la educación, la participación y el establecimiento de relaciones. Actualmente, las plataformas digitales se utilizan para diversas actividades y constituyen a menudo experiencias multimedios.

Para que los jóvenes se desarrollen, se considera fundamental que tengan acceso a estas tecnologías, aprendan a utilizarlas y a valerse de ellas, y comiencen a familiarizarse con estas a una edad temprana. Los encargados de formular políticas deben entender que, con frecuencia, los niños y jóvenes empiezan a utilizar las plataformas y servicios antes de alcanzar la edad mínima establecida, por lo que su educación al respecto debe comenzar en una etapa temprana.

Los niños y los jóvenes desean entablar conversaciones y gozan de una valiosa experiencia como "nativos digitales" que puede ser compartida. Los encargados de formular políticas y especialistas deben dialogar con los niños y jóvenes en el marco de un debate continuo sobre el entorno en línea a fin de respaldar sus derechos.

Acceso a Internet

En 2019, más de la mitad de la población mundial utilizaba Internet (un 53,6%) y se estima que el número de usuarios era de 4 100 millones. En todo el mundo, uno de cada tres usuarios de Internet es menor de 18 años[1]. En algunos países de bajos ingresos, esta relación asciende aproximadamente a uno de cada dos usuarios, mientras que en los países con ingresos más altos gira en torno a uno de cada cinco usuarios. Según UNICEF, el 71% de los jóvenes de todo el mundo ya están en línea[2]. Por consiguiente, la presencia actual de los niños y los jóvenes en Internet es considerable, permanente y persistente[3]. Internet cumple otros fines sociales, económicos o políticos y se ha convertido en un producto o servicio familiar o de consumo que forma parte integrante del modo de vida de las familias, los niños y los jóvenes.

En 2017, en el plano regional, el acceso de los niños y jóvenes a Internet estaba estrechamente vinculado con el nivel de ingresos. El número de usuarios de Internet menores de edad en los países de bajos ingresos suele ser inferior al de los países de altos ingresos.

En la mayoría de los países, los niños y jóvenes pasan más tiempo en línea los fines de semana que entre semana, y los adolescentes (entre 15 y 17 años) son los que registran la mayor duración de conexión, de entre 2,5 y 5,3 horas por término medio, en función del país de que se trate.

Uso de Internet

El dispositivo que más utilizan los niños y jóvenes para acceder a Internet es el teléfono móvil, seguido de los ordenadores de sobremesa y los portátiles. Por término medio, los niños y los jóvenes pasan en línea dos horas al día entre semana y aproximadamente el doble de tiempo los fines de semana. Algunos se sienten permanentemente conectados. Sin embargo, otros no tienen todavía acceso a Internet en sus hogares.

---

1 Livingstone, S., Carr, J., y Byrne, J. (2015) *One in three: The task for global internet governance in addressing children's rights*. Global Commission on Internet Governance: Paper Series. Londres: CIGI y Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

2 Comisión de la Banda Ancha para el Desarrollo Sostenible, *Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)*, octubre de 2019, pág. 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

3 Livingstone, Carr y Byrne, *One in Three: Internet Governance and Children's Rights*.

En la práctica, la mayoría de los niños y jóvenes que utilizan Internet, acceden a ella a través de varios dispositivos: los niños y jóvenes que se conectan al menos una vez a la semana utilizan a veces hasta tres dispositivos diferentes. Los niños de edades más avanzadas y los de los países más ricos suelen utilizar más dispositivos, y en todos los países analizados se ha observado que el número de dispositivos utilizados por los varones es ligeramente superior al de las hembras.

La actividad más popular, tanto en niñas como en niños, es la visualización de videoclips. Más de tres cuartas partes de los niños y jóvenes que utilizan Internet afirman visualizar vídeos en línea al menos una vez a la semana, ya sea solos o con otros familiares. Muchos niños y jóvenes se pueden considerar "socializadores activos", ya que utilizan varias plataformas de medios sociales como Facebook, Twitter, TikTok o Instagram.

Los niños y jóvenes también participan en actividades políticas en línea y expresan sus opiniones a través de los blogs.

Su nivel general de participación en los juegos en línea varía en función de los países, coincidiendo aproximadamente con la disponibilidad de su acceso a Internet, mientras que el porcentaje de niños y jóvenes que utilizan semanalmente Internet para participar en actividades creativas en línea oscila entre un 10% y un 30%.

En lo que respecta a los fines educativos, muchos niños y jóvenes de todas las edades utilizan Internet todas las semanas para hacer sus deberes, o incluso para ponerse al día tras faltar a clase o buscar información médica en línea. Los niños de edades más avanzadas parecen tener más sed de información que los más pequeños.

2.3 Los efectos de la tecnología en la experiencia digital de los niños

Internet y la tecnología digital pueden ofrecer oportunidades y presentar riesgos para los niños y los jóvenes. Por ejemplo, cuando los niños utilizan los medios sociales, se benefician de numerosas oportunidades para explorar, aprender, comunicar y desarrollar habilidades fundamentales. Además, los niños piensan que las redes sociales son plataformas que les permiten explorar su identidad personal en un entorno seguro. Los jóvenes consideran importante tener las habilidades pertinentes y saber cómo afrontar los problemas relacionados con la privacidad y la reputación.

En Chile, un niño de 14 años declaró ser consciente de que todo lo que se publica en Internet permanece en la red para siempre y puede afectar a la vida futura de cada persona.

No obstante, dado que las consultas demuestran que la mayoría de los niños utilizan los medios sociales antes de la edad mínima establecida en trece años[11], y que los servicios de verificación de edad son por lo general deficientes o insuficientes, los riesgos para la infancia pueden adquirir una intensidad mayor. Asimismo, si bien los niños desean adquirir habilidades digitales y convertirse en ciudadanos digitales, preocupándose especialmente por su privacidad, tienden a asociar la cuestión de la privacidad con sus amigos y conocidos (¿Qué pueden ver mis amigos?) más que con los desconocidos y terceros. Todo esto, sumado a la

[11] Red Conectados al Sur, "Hablatam"; UNICEF, *Global Kids Online Comparative Report* (2019).

curiosidad innata de los niños y su umbral de percepción del riesgo, situado generalmente en un nivel inferior al normal, los hace vulnerables a la seducción, explotación, intimidación u otros tipos de contenidos o contactos perjudiciales.

La popularidad generalizada de la compartición de imágenes y vídeos mediante aplicaciones móviles y, en particular, la utilización de plataformas de transmisión en directo por los niños plantea problemas adicionales relacionados con la privacidad y los riesgos. Algunos niños crean imágenes sexuales exponiéndose a sí mismos, sus amigos y hermanos, y las comparten en línea. Algunos de ellos, en especial los de edades más avanzadas, pueden considerarlo un método natural para explorar su sexualidad e identidad sexual, mientras que otros, en especial los más pequeños, están con frecuencia coaccionados por un adulto u otro menor. En cualquier caso, el contenido que resulta de ese acto es ilícito en muchos países y puede exponer a los niños al riesgo de que se ejerza la acción penal en su contra, o incluso podría utilizarse para cometer otros actos de explotación del niño.

De manera análoga, los juegos en línea permiten a los niños hacer efectivo su derecho fundamental al juego, así como construir redes, hacer nuevos amigos y pasar tiempo con ellos, y desarrollar habilidades importantes. Sin duda alguna, todos estos aspectos pueden ser positivos. Sin embargo, cada vez hay más pruebas de que la utilización de las plataformas de juegos en línea, cuando no está acompañada de la supervisión y el apoyo de un adulto responsable, también puede presentar riesgos para los niños, desde los trastornos relacionados con el juego, los riesgos financieros o la recopilación y monetización de los datos personales de los niños, hasta el ciberacoso, el discurso de odio, la violencia y la exposición a conductas o contenidos inapropiados[12], así como la seducción mediante el uso de imágenes y vídeos reales, creados por ordenador o incluso de realidad virtual, que ilustran o banalizan el abuso y la explotación sexual de niños.

Además, la evolución tecnológica ha conducido a la aparición de la Internet de las cosas, haciendo que cada vez sean más variados y numerosos los dispositivos capaces de conectarse, comunicar e interactuar por Internet. Entre ellos están los juguetes, los controladores de bebés y los dispositivos que funcionan con inteligencia artificial, que pueden presentar riesgos respecto de la privacidad y los contactos no deseados.

2.4 Principales amenazas en línea para los niños

Los adultos y los niños están expuestos a diversos riesgos y peligros en línea. No obstante, los niños constituyen una población mucho más vulnerable. Algunos niños también son más vulnerables que otros, por ejemplo, los niños con discapacidad[13] o los niños migrantes. Los encargados de formular políticas deben garantizar que todos los niños puedan desarrollarse y formarse en un entorno digital seguro. En la Convención de las Naciones Unidas sobre los Derechos del Niño está consignada la idea de que los niños son vulnerables y deben ser protegidos contra todas las formas de explotación.

El entorno digital consta de varias esferas que ofrecen excelentes oportunidades a los niños pero que a su vez pueden generar riesgos que podrían provocar profundos daños a los menores y socavar su bienestar. Tanto en relación con los adultos como con los niños, preocupa por

12 UNICEF, *Global Kids Online Comparative Report* (2019). (UNICEF, 2019)

13 Lundy y otros, *TWO CLICKS FORWARD AND ONE CLICK BACK, Report on children with disabilities in the digital environment* (Consejo de Europa, octubre de 2019), https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

ejemplo que se pueda utilizar Internet para violar su privacidad, difundir información errónea o, aún peor, permitir el acceso a la pornografía.

A este respecto, es fundamental distinguir entre los riesgos y los daños para los niños. No son peligrosas todas las actividades que puedan llevar aparejados factores de riesgo y no todos los riesgos causarán necesariamente daños a los niños. Como ejemplo de ello cabría citar el *sexting*, que es un método por el cual los jóvenes podrían explorar su sexualidad y sus relaciones, y que no es necesariamente perjudicial.

Figura 2: Clasificación de las amenazas en línea para los niños[14]

	Contenido (el niño es el receptor (de producciones masivas)), 2) Contacto (el niño es un participante (actividad iniciada por un adulto))	Contacto (el niño es un participante (actividad iniciada por un adulto))	Conducta (el niño es un actor (perpetrador/víctima))
Agresivo	Contenido violento/sangriento	Hostigamiento, acecho	Acoso, actividad hostil de los compañeros
Sexual	Contenido pornográfico	Seducción, abuso sexual al encontrarse con extraños	Acoso sexual, sextear
Valores	Contenido racista/de odio	Persuasión ideológica	Contenido potencialmente dañino generado por el usuario
Comercial	Publicidad, marketing integrado	Explotación y utilización indebida de datos personales	Apuestas, infracción de derechos de autor

Fuente: EU Kids Online (Livingstone, Haddon, Görzig y Ólafsson (2011)

El advenimiento de la era digital ha presentado nuevos retos para la protección de la infancia. Los niños deben estar facultados para navegar por el mundo virtual de manera segura y aprovechar sus múltiples beneficios.

Los encargados de formular políticas deben velar por que existan leyes, salvaguardias e instrumentos pertinentes que permitan que los niños se desarrollen y aprendan con seguridad. Es fundamental que los niños dispongan de las habilidades necesarias para detectar las amenazas y entiendan completamente las repercusiones y los matices de su conducta en línea.

Mientras están en línea, los niños pueden enfrentarse a múltiples amenazas procedentes de organizaciones, adultos y compañeros.

Contenido y manipulación

- La exposición a contenido inapropiado o incluso delictivo puede hacer que los niños adopten conductas extremas como las autolesivas, destructoras y violentas. Asimismo, la exposición a dicho contenido también puede hacer que se radicalicen o se sumen a ideologías racistas o discriminatorias. Se sabe que muchos niños no respetan las limitaciones relativas a la edad indicadas en los sitios web.

[14] Livingstone, S., Haddon, L., Görzig, A., y Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, Londres: EU Kids Online, http://eprints.lse.ac.uk/33731/.

- La exposición de los niños a información inexacta o incompleta limita su entendimiento del mundo que los rodea. La tendencia consistente en personalizar el contenido con base en la conducta del usuario puede conducir a los niños a "burbujas de filtro", que les impiden desarrollarse y acceder a una gran variedad de contenidos.
- La exposición de los niños a contenidos filtrados mediante algoritmos con la intención de manipularlos puede influir considerablemente en su desarrollo, sus opiniones, valores y hábitos. El aislamiento de los niños en "cámaras de resonancia" o "burbujas de filtro" les impide acceder a una amplia variedad de opiniones e ideas.

Contactos con adultos o compañeros

Los niños pueden enfrentarse a una gran variedad de amenazas derivadas del contacto con compañeros o adultos.

- La propagación del ciberacoso puede ser mayor y más rápida que la que tendría lugar fuera de línea. Esto puede ocurrir en cualquier momento del día o la noche, invadiendo con ello lo que hasta ahora eran "espacios seguros", y producirse de forma anónima.
- Los niños que son víctimas fuera de línea tienen probabilidades de serlo en línea. Esto expone a los niños con discapacidad a un riesgo mayor en línea, ya que las investigaciones han demostrado que estos niños son más propensos a sufrir abusos de todo tipo y, en particular, abusos sexuales. La victimización de los niños puede abarcar actos como la intimidación, el acoso, la exclusión y la discriminación con base en su discapacidad real o percibida, o en aspectos relacionados con dicha discapacidad, como la manera de comportarse o hablar o los equipos o servicios que utilizan.
- La difamación y el daño a la reputación: las imágenes y los vídeos se pueden modificar y compartir con miles de millones de personas. Los comentarios insensatos pueden permanecer disponibles durante décadas, a la vista de todos.
- Los niños pueden ser objeto de ataques, actos de seducción y abusos cometidos a través de Internet por un agresor situado tanto cerca de su lugar como al otro lado del mundo, que con frecuencia se hace pasar por otra persona. Esto puede adoptar diversas formas, por ejemplo, la radicalización del menor o su coacción para que envíe contenidos sexualmente explícitos de sí mismo.
- Los niños pueden ser sometidos a presión, engañados o coaccionados para realizar compras con la autorización de quien realmente las paga o sin ella.
- La publicidad no deseada suscita problemas en relación con el consentimiento y la venta de datos.

La conducta del menor y sus posibles consecuencias

- El ciberacoso puede ser particularmente perturbador y dañino, ya que conlleva un mayor grado de propagación y publicidad, y el contenido distribuido electrónicamente puede salir a la superficie en cualquier momento, por lo que la víctima tendrá mayor dificultad para poner término al incidente; puede incluir imágenes visuales dañinas o mensajes hirientes; el contenido se encuentra disponible durante las 24 horas del día; el acoso por medios electrónicos puede tener lugar cualquier día y a cualquier hora, invadiendo con ello la privacidad de la víctima incluso en lugares como su hogar, que de lo contrario son "seguros"; asimismo, se puede manipular la información personal, modificar las imágenes visuales y comunicarlas a terceros. Además, todos estos actos pueden cometerse de manera anónima. La divulgación de información personal entraña un riesgo de daños físicos, por ejemplo, en el marco de encuentros en la vida real con conocidos en línea, con el consiguiente riesgo de abuso físico y/o sexual.
- La violación de sus propios derechos o de los derechos de terceros mediante actos de plagio y telecarga de contenido sin autorización, en particular la toma y publicación de fotografías inapropiadas sin autorización.

- La violación de derechos de autor de terceros, por ejemplo, mediante la descarga de música, películas o programas de televisión para los que debería realizarse el correspondiente pago, acto que podría causar daños a la víctima de tal violación.
- El uso compulsivo y excesivo de Internet y/o de los juegos en línea, en detrimento de actividades sociales o de exterior que son importantes para la salud, el fomento de la confianza, el desarrollo social y el bienestar general.
- El intento de dañar, acosar o intimidar a alguien, en particular haciéndose pasar por otra persona, a menudo otro menor.
- Una conducta que los adolescentes adoptan cada vez más es el *sexting* (compartir imágenes o mensajes de texto de contenido sexual mediante los teléfonos móviles). Con frecuencia, estas imágenes y mensajes de texto se intercambian con la pareja o posible pareja de la persona que adopta dicha conducta, pero a veces terminan siendo transmitidas a muchas más personas. Se considera poco probable que los jóvenes adolescentes entiendan correctamente las implicaciones de estas conductas y los posibles riesgos que entrañan.

2.5 Principales daños para los niños en línea

La sección anterior se refiere a las amenazas a las que los niños se pueden exponer en línea. En esta, se destacan los daños que pueden surgir a raíz de dichas amenazas.

Daños

Según estudios de UNICEF sobre el uso de Internet, se consideran riesgos y daños las categorías de actos que se enumeran a continuación:

- Realización de actos dañinos y lesiones en contra de sí mismo:
  - Contenido suicida
  - Discriminación
- Exposición a material inapropiado:
  - Exposición a contenido extremista, violento o sangriento
  - Marketing integrado
  - Apuestas en línea
- En torno al 20% de los niños encuestados en relación con esta cuestión afirmaron haber visto en el último año sitios web o discusiones en línea sobre personas que se infligían daños o lesiones a sí mismas.
- Radicalización:
  - Persuasión ideológica
  - Discurso de odio
- Se observó una mayor probabilidad de que los niños fueran perturbados por discursos de odio o contenidos sexuales en línea, fuesen tratados de manera hiriente en línea o fuera de línea o, reuniéndose físicamente con alguien que habían conocido primeramente en línea.
- Abuso y explotación sexual:
  - Contenido autogenerado
  - Seducción con fines sexuales
  - Material de abuso sexual infantil (MASI)
  - Trata
  - Explotación sexual de niños en los viajes y el turismo

Un estudio realizado en 2017 sobre los niños en Dinamarca, Hungría y el Reino Unido reveló que se habían difundido imágenes explícitas del 6% de los niños sin su consentimiento.

En 2019, la Internet Watch Foundation (IWF) señaló que en más de 132 000 sitios web se había confirmado la presencia de imágenes y vídeos de abuso sexual infantil. En cada uno de esos sitios web podía haber entre una y miles de imágenes que ilustraban este abuso.

Los riesgos relacionados con la violencia en línea, como la difusión de fotografías de desnudos sin el correspondiente consentimiento y el ciberacoso con fines sexuales se caracterizan por una dinámica de género desigual, ya que las presiones sexistas ejercidas para que la víctima adopte un determinado comportamiento sexual son más frecuentes en las niñas, que sufren con ello consecuencias más negativas y dañinas.

- Violación y uso indebido de datos personales:
  - Piratería
  - Fraude y robo

Si bien muchos están familiarizados con la piratería y los timos, la invasión de la privacidad respecto de las actividades de los niños en línea se considera una violación diferente. Con frecuencia, los adultos ponen coto a los jóvenes escrutando sus teléfonos móviles y vigilando sus actividades en línea. Por ejemplo, según comunicaron unos niños en Brasil, tanto los niños como las niñas de diferentes edades consideran que los padres controlan más el uso de Internet por las niñas. Para tratar de explicar esta situación, se suele alegar que, en algunos casos, las niñas pueden ser más vulnerables debido a las estructuras sociales del lugar donde viven, en particular en lo que atañe a su seguridad, en un contexto en el que cada vez se desdibujan más los límites entre las interacciones en línea y fuera de línea.

- Ciberacoso, hostigamiento y acoso: Actividad hostil y violenta ejercida por compañeros

Las salas de charlas (*chat rooms*) y los sitios de redes sociales pueden dar paso a la violencia y la intimidación, con la posibilidad de que sus usuarios anónimos, incluidos los jóvenes, comuniquen de manera agresiva o abusiva. En siete países europeos (Bélgica, Dinamarca, Irlanda, Italia, Portugal, Rumania y el Reino Unido)[1] se determinó que, por término medio, el porcentaje de niños víctimas de ciberacoso era del 8% en 2010, mientras que esa relación fue del 12% en 2014.

Es fundamental señalar que los niños vulnerables corren a menudo un riesgo mayor de ser víctimas de ciberacoso.

[1] Livingstone, S., Mascheroni, G., Ólafsson, K. y Haddon, L., (2014) *Children's online risks and opportunities: comparative findings from EU Kids Online and Net Children Go Mobile*. Londres: Escuela de Economía y Ciencias Políticas de Londres, www.eukidsonline.net y http://www.netchildrengomobile.eu/.

Cuestión de interés: Corrección de desigualdades

En 2017, aproximadamente un 60% de los niños no tenían acceso a Internet en la región de África, mientras que esa proporción solo era del 4% en Europa. En todas las regiones del mundo había más usuarios de Internet de sexo masculino que de sexo femenino y, con frecuencia, el uso de Internet por las niñas era objeto de supervisión y restricciones. La

expansión de la banda ancha en lugares del mundo que hasta ahora carecen de conexión acentuará considerablemente esta desigualdad[15].

Los niños que dependen de los teléfonos móviles para realizar sus actividades en línea y no disponen de ordenadores tendrán que conformarse con la segunda mejor alternativa. Con frecuencia, los niños que hablan idiomas minoritarios no pueden encontrar contenidos pertinentes en línea y los niños de zonas rurales tienen más probabilidades de sufrir robos de contraseñas o dinero.

Las investigaciones demuestran que muchos adolescentes de todo el mundo deben hacer frente a importantes obstáculos a su participación en línea. Para muchos de ellos, siguen siendo obstáculos fundamentales los problemas de acceso como la mala conexión, los costos prohibitivos de los datos y dispositivos y la falta de equipos apropiados.

La expansión de la banda ancha asequible en los países en desarrollo ha generado una necesidad apremiante de adoptar medidas a fin de reducir al mínimo los riesgos y amenazas para los niños que viven en ellos, permitiéndoles al mismo tiempo aprovechar los beneficios del mundo digital.

Cuestión de interés: Material de Abuso Sexual Infantil (MASI)

La magnitud del problema

Internet ha transformado la magnitud y la naturaleza de la producción, distribución y disponibilidad de materiales de tipo MASI. En 2018, empresas tecnológicas situadas en los Estados Unidos de América comunicaron más de 45 millones de imágenes y vídeos en línea de los que se sospechaba que mostraban actos de abusos sexuales cometidos contra niños en todo el mundo. Se trata de una industria mundial y la magnitud y gravedad del abuso van en aumento a pesar de las medidas desplegadas para ponerle fin.

En el pasado, cuando no existía Internet, los agresores tenían que correr importantes riesgos y asumir considerables gastos para acceder a este tipo de materiales. Ahora, gracias a Internet, pueden acceder a ellos de manera relativamente fácil y adoptar conductas cada vez más arriesgadas. Dado que las cámaras son más pequeñas y están cada vez más integradas en todas las facetas de nuestra vida, el proceso de producción de MASI y la adquisición de contenidos a raíz de un abuso sin contacto son más fáciles que nunca.

Es imposible determinar el tamaño o la forma exacta que puede tener este negocio clandestino e ilegal. Sin embargo, es evidente que el número de imágenes ilegales que circulan actualmente se puede contar por millones. Se han hecho copias de casi todas las imágenes en que aparecen menores. En 2018, la IWF hizo un seguimiento de la frecuencia con la que salían a la superficie imágenes de un niño del que se sabía que había sido rescatado en 2013. Durante un periodo de tres meses, los analistas de la IWF detectaron la aparición de las imágenes en 347 ocasiones, con una frecuencia de 5 veces por cada día hábil.

El panorama actual

[15] Comisión de la Banda Ancha, *Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019).*

Cada vez que la imagen del abuso de un niño aparece y vuelve a aparecer en línea o es descargada por un agresor, ese niño vuelve a ser víctima de abuso. Las víctimas se ven obligadas a ver durante el resto de sus vidas que esas imágenes permanecen y circulan por Internet.

En cuanto se descubre un material que ilustra un abuso sexual infantil o una página web que lo aloje, es importante retirar o bloquear dicho contenido lo antes posible. La naturaleza mundial de Internet dificulta esta tarea: los agresores pueden producir materiales en un país, alojarlos en otro y destinarlos a consumidores situados en un tercer país. Es casi imposible que las órdenes de detención o las notificaciones de las autoridades nacionales se ejecuten sin no hay un sistema de cooperación internacional perfeccionado.

El ritmo de la innovación en el mundo digital implica un cambio constante del panorama de agresores. Entre las principales amenazas que han surgido recientemente están las siguientes:

- El auge del cifrado permite de manera involuntaria que los agresores actúen y compartan materiales con canales ocultos, haciendo que cada vez sea más difícil detectarlos y hacer que se cumpla la ley.
- Los foros dedicados a la seducción de menores adquieren dimensiones cada vez más importantes en rincones protegidos de Internet, lo cual banaliza y fomenta esta conducta, y a menudo exigen la presentación de "nuevos contenidos" para la inscripción de sus miembros.
- La rápida expansión de Internet está permitiendo a los usuarios acceder en línea a lugares para los que aún se deben elaborar e implementar estrategias de protección integrales o la infraestructura pertinente.
- Los niños utilizan dispositivos a edades tempranas sin supervisión y la conducta sexual en línea se está banalizando. El número de imágenes de abuso autogeneradas aumenta cada año.

Cuestión de interés: Contenido autogenerado

Los niños y adolescentes pueden realizar fotografías o vídeos comprometedores de sí mismos. Si bien esta conducta no es de por sí necesariamente ilegal y puede tener lugar como parte de un desarrollo sexual sano y normal, hay riesgos de que dicho contenido pueda circular en línea o fuera de línea para causar daños a los niños o se utilice como base para extorsionar favores. Aunque es posible que algunos niños estén sometidos a presión o sean coaccionados para compartir imágenes sexuales, otros, en particular los adolescentes, pueden producir contenido sexual de manera voluntaria. Esto no significa que consientan que esas imágenes se utilicen o distribuyan con fines de explotación o abuso ni que sean responsables de dicha utilización o distribución.

El *sexting* se ha definido como la "producción propia de imágenes sexuales",[16] o el "intercambio de mensajes o imágenes sexuales" y la "creación, compartición y reenvío de imágenes sexualmente provocativas de una persona desnuda o casi desnuda a través de los teléfonos móviles y/o de Internet"[17]. El *sexting* es una forma de contenido autogenerado y sexualmente

[16] Karen Cooper y otros, *Adolescents and Self-Taken Sexual Images: A Review of the Literature*, *Computers in Human Behaviour, núm.* 55 (febrero de 2016): 706–16, https://doi.org/10.1016/j.chb.2015.10.003.

[17] Jessica Ringrose y otros, *A Qualitative Study of Children, Young People and 'Sexting': A Report Prepared for the NSPCC* (Londres, Reino Unido: National Society for the Prevention of Cruelty to Children, 2012), http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x.

explícito,[18] y la práctica presenta "notables diferencias en cuanto al contexto, el significado y la intención"[19].

Si bien el *sexting* es posiblemente la forma más habitual de contenido autogenerado sexualmente explícito en relación con los niños, y a menudo es practicado por y entre adolescentes consintientes que gozan de la experiencia, también hay muchas formas de *sexting* no deseado. Esto guarda relación con los aspectos no consensuados de dicha actividad, como la difusión o recepción de fotografías, vídeos o mensajes sexualmente explícitos y no deseados enviados, por ejemplo, por personas conocidas o desconocidas que intentan ponerse en contacto con el menor, ejercer presión sobre él o seducirlo. El *sexting* también puede ser una forma de intimidación sexual, cuando se ejerce presión sobre un menor para que envíe una fotografía a su pareja o compañero que a continuación la difunde en una red de amigos sin su consentimiento.

Cuestión de interés: Ciberacoso

Si bien el acoso es un fenómeno muy anterior a la aparición de Internet, la ampliación de la magnitud, el alcance y la continuidad del acoso cometido en línea puede agravar aún más una experiencia que de por sí es perturbadora y a menudo dañina para sus víctimas. El ciberacoso se define como el daño premeditado y repetido infligido mediante el uso de ordenadores, teléfonos móviles y otros dispositivos electrónicos. A menudo se produce paralelamente al acoso fuera de línea en la escuela u otro lugar, puede tener además dimensiones racistas, religiosas o sexistas y puede constituir una extensión del daño causado fuera de línea, por medios como la piratería de cuentas, la difusión de fotografías y vídeos en línea y la presencia diaria y a todas horas de mensajes dañinos y contenidos disponibles. Dado que, de manera general, se trata de una cuestión social más que delictiva, es necesario que las políticas que abordan el ciberacoso adopten un criterio integral que implique a las escuelas, familias y, esencialmente, a los propios niños.

Cuestión de interés: Seducción en línea y chantaje sexual (sextorsión)

A raíz de los rápidos avances tecnológicos y del mayor acceso a Internet y a las comunicaciones digitales que se han registrado durante los últimos años, se ha agravado inevitablemente el riesgo de que se cometan actos delictivos en línea contra niños. Entre estas nuevas formas de explotación sexual infantil en línea están la seducción en línea y el chantaje sexual de menores. En términos generales, por seducción en línea se entiende el proceso por el cual un adulto trata de ganarse la amistad de un niño (menor de 18 años) e influenciarlo, utilizando Internet u otras tecnologías digitales a fin de facilitar la interacción sexual con o sin contacto con dicho niño. Mediante el proceso de seducción, el agresor trata de obtener el compromiso del menor de edad para mantener el secretismo y así evitar ser detectado y castigado[20]. Asimismo, es importante reconocer que también existen casos de abuso entre compañeros.

INTERPOL ha comunicado que Internet facilita la seducción debido a que ofrece un gran número de blancos posibles fácilmente accesibles y permite que los agresores se presenten

---

18 Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, pág. 22 (Viena: Naciones Unidas, 2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.

19 Cooper y otros, *Adolescents and Self-Taken Sexual Images*.

20 Centro Internacional para Niños Desaparecidos y Explotados, *Grooming por Internet de niños, niñas, y adolescentes con fines sexuales: Modelo de legislación y revisión global*, 1ª edición, 2017, https://www.icmec.org/wp-content/uploads/2017/09/Grooming-Por-Internet-de-Ninos_FINAL_9-18-17_ES_FINAL.pdf.

ante los niños de una manera atractiva. Los agresores sexuales de niños en línea recurren a la manipulación, la coacción y la seducción a fin de reducir la inhibición de los niños e inducirlos a participar en actividades sexuales. El agresor lleva a cabo un proceso deliberado a fin de identificar a una posible víctima vulnerable y reunir información sobre el apoyo familiar del niño, para luego presionarlo o hacerle pasar vergüenza o miedo con miras a abusar de él. Los agresores pueden utilizar material pornográfico para adultos y material que muestre el abuso o la explotación infantil para desinhibir a sus víctimas potenciales, presentándoles la actividad sexual infantil como algo natural y normal. Internet ha modificado la manera en que las personas interactúan y ha redefinido el concepto de "amigo". Un agresor puede entablar una amistad con un niño en línea con gran facilidad y rapidez, lo cual obliga a revisar los tradicionales mensajes educativos acerca del "peligro de los extraños".

La seducción en línea fue reconocida oficialmente por primera vez en un instrumento jurídico internacional en 2007, a saber, el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual (el Convenio de Lanzarote). El artículo 23 tipifica como delito las "proposiciones a niños con fines sexuales", lo cual requiere que se haya propuesto de manera intencional un encuentro con el niño con el fin de cometer contra él un delito sexual y que tras dicha proposición se hayan cometido "actos materiales conducentes a dicho encuentro". En numerosos casos de seducción, los niños son víctimas de abuso y explotación sexual en línea (el "encuentro" que exige el Convenio de Lanzarote y muchas leyes nacionales en vigor se realiza enteramente de manera virtual) pero, no obstante, esos actos causan el mismo daño al niño que los encuentros físicos. Es fundamental que la tipificación de la seducción abarque "los casos en que el abuso sexual no resulta de un encuentro físico, sino que se comete en línea"[21].

La sextorsión o chantaje sexual[22] puede tener lugar como parte del fenómeno de seducción en línea o como un delito independiente. Si bien el chantaje sexual puede producirse fuera del proceso de seducción en línea, este proceso puede conducir en algunos casos a esta forma de chantaje[23]. El chantaje sexual puede tener lugar en el contexto de la seducción en línea, ya que el agresor manipula al niño y ejerce su influencia sobre él durante el proceso de seducción mediante amenazas, actos de intimidación y coacción, a fin de que envíe imágenes sexuales de sí mismo (contenido autogenerado)[24]. Si la víctima no accede a los favores sexuales solicitados o no proporciona imágenes íntimas adicionales, dinero u otros beneficios, sus imágenes podrían ser publicadas en línea con el fin de causar humillación o angustia al niño o coaccionarlo para que genere más materiales sexualmente explícitos[25].

---

21 Comité de Lanzarote, Comité de las Partes en el Convenio del Consejo de Europa sobre la protección de los niños contra la explotación y el abuso sexual, *Solicitation of children for sexual purposes through information and communication technologies (grooming), Opinion on Article 23 of the Lanzarote Convention and its explanatory note*, 17 de junio de 2015, en https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html (última consulta realizada el 6 de noviembre de 2019).

22 National Center for Missing and Exploited Children (NCMEC), *Sextorsión*, en https://esp.missingkids.org/theissues/sextortion (última consulta realizada el 6 de noviembre de 2019).

23 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales,* Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes, 28 de enero de 2016, apartado D.4.iii, págs. 31 y 32, en http://luxembourgguidelines.org/es/.

24 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales,* Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes, 28 de enero de 2016, apartado D.4.iii, págs. 31 y 32, en http://luxembourgguidelines.org/es/.

25 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales,* Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes, 28 de enero de 2016, apartado D.4.iii, págs. 31 y 32, en http://luxembourgguidelines.org/es/.

También se ha utilizado el término "agresión sexual virtual" con referencia a la sextorsión o chantaje sexual, debido a los efectos emocionales y psicológicos similares que provoca en las víctimas[26]. En algunos casos, el abuso es tan traumatizante que las víctimas han intentado infligirse daños a sí mismas o suicidarse como medio para escapar del abuso.

La Agencia de la Unión Europea para la Cooperación Policial (Europol) señaló la dificultad que plantea la recopilación de información para evaluar el alcance del chantaje sexual contra menores y la posibilidad de que haya muchos casos que no se denuncien[27]. Además, la falta de términos y definiciones comunes para la seducción en línea y el chantaje sexual obstaculizan la recopilación de datos precisos y el entendimiento del verdadero alcance de estos problemas en todo el mundo.

2.6 Niños con vulnerabilidades

Los niños y los jóvenes pueden ser vulnerables por diversos motivos diferentes. En el marco de una investigación realizada en 2019 se declaró que "las vidas digitales de los niños vulnerables rara vez reciben la misma atención minuciosa y razonable que suele recibir la adversidad de la 'vida real'". Además, en el informe se añade que "en el mejor de los casos, [esos niños y jóvenes] reciben los mismos consejos generales en materia de seguridad en línea que los demás niños y jóvenes, cuando es necesario que intervengan especialistas".

Aunque evidentemente hay muchas categorías de niños con vulnerabilidades específicas, se podrían citar tres de ellas a modo de ejemplo: los niños migrantes, los que sufren de un trastorno del espectro autista y los niños con discapacidad.

Niños migrantes

Con frecuencia, los niños y jóvenes procedentes de la inmigración llegan a un país (o ya viven en él) con una determinada serie de experiencias y expectativas socioculturales. Aunque se suele considerar que la tecnología es un facilitador para establecer contactos y participar, los riesgos y oportunidades que entraña varían mucho en función de los contextos. Además, los resultados empíricos y las investigaciones demuestran que, por lo general, los medios digitales desempeñan una función vital:

- Son importantes para orientarse (al viajar a otro país).
- Desempeñan un papel central para apropiarse de la sociedad/cultura del país de acogida y familiarizarse con ella.
- Los medios sociales pueden contribuir de manera decisiva al mantenimiento del contacto con familiares y compañeros y al acceso a la información general.

Además de los múltiples aspectos positivos, los medios digitales también pueden plantear retos para los migrantes, entre otras cosas en relación con lo siguiente:

- La infraestructura – es importante concebir espacios seguros en línea para que los niños y jóvenes migrantes se puedan beneficiar de la privacidad y la seguridad.

---

[26] Benjamin Wittes y otros, *Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault*, (Brookings Institution, 11 de mayo de 2016), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

[27] Europol, *Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective* (Centro Europeo contra la Ciberdelincuencia, mayo de 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

- Los recursos – los migrantes gastan la mayor parte de su dinero en la compra de tarjetas telefónicas de prepago.
- La integración – además de tener acceso a las tecnologías, los niños y jóvenes migrantes también necesitan recibir una educación digital adecuada.

Niños con Trastornos del Espectro Autista (TEA)

El espectro autista concentra dos trastornos principales del proceso de diagnóstico de los trastornos de conducta recogido en el Manual diagnóstico y estadístico de los trastornos mentales (DSM-5):

- conducta limitada y repetitiva ("necesidad de rutina constante");
- dificultad con los comportamientos sociales y comunicativos;
- frecuentes discapacidades intelectuales, problemas del lenguaje y otros problemas conexos.

La tecnología e Internet ofrecen infinitas oportunidades para el aprendizaje, la comunicación y el juego de los niños. Sin embargo, además de estos beneficios hay muchos riesgos que pueden afectar en mayor medida a los niños y jóvenes con TEA:

- Internet puede ofrecer a los niños y jóvenes con autismo oportunidades para socializarse e intereses especiales que tal vez no tengan fuera de línea.
- Los problemas sociales, como la dificultad de entender las intenciones de los demás, pueden hacer que este grupo vulnerable haga "amigos" con malas intenciones.
- Los problemas relativos a las actividades en línea guardan a menudo relación con las características propias del autismo: una orientación concreta y específica podría mejorar la experiencia en línea de las personas, pero no resolvería los problemas subyacentes.

Niños con discapacidad

Los niños con discapacidad se exponen a riesgos en línea de manera muy similar a la de los niños sin discapacidad, aunque también se enfrentan a riesgos específicos relacionados con su discapacidad. Con frecuencia, los niños con discapacidad se ven excluidos, estigmatizados y se enfrentan a obstáculos (físicos, económicos, sociales y actitudinales) para participar en sus comunidades. Estas experiencias pueden contribuir a que un niño con discapacidad intente interactuar socialmente y hacer amigos en espacios en línea, lo cual puede ser positivo, aumentar su autoestima y crear redes de apoyo. Sin embargo, de este modo también pueden exponerse a un mayor riesgo de incidentes de seducción, solicitaciones en línea y/o acoso sexual. Las investigaciones muestran que el riesgo de que se produzcan incidentes de ese tipo es mayor en los niños que tienen dificultades fuera de línea y los que sufren problemas psicosociales[28].

En general, los niños que son víctimas fuera de línea tienen probabilidades de serlo en línea. Esto expone a los niños con discapacidad a un mayor riesgo en línea, pero sus necesidades de utilizar este medio son mayores. Las investigaciones han demostrado que los niños con discapacidad son más propensos a sufrir abusos de todo tipo[29], y, en particular, a ser víctimas

[28] Andrew Schrock y otros, *Solicitation, Harassment, and Problematic Content*, Berkman Center for Internet & Society, Universidad de Harvard, diciembre de 2008, pág. 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.

[29] UNICEF, *El Estado Mundial de la Infancia 2013: Niñas y niños con discapacidad,* 2013, https://www.unicef.org/spanish/publications/index_69378.html.

de abusos sexuales[30]. La victimización de los niños puede abarcar actos como la intimidación, el acoso, la exclusión y la discriminación con base en su discapacidad real o percibida, o en aspectos relacionados con dicha discapacidad, como la manera de comportarse o hablar o los equipos o servicios que utilizan.

Entre las personas que cometen actos de seducción, solicitación en línea y/o acoso sexual contra niños con discapacidad pueden estar no sólo agresores cuyo objetivo son los niños sino también otros que ponen el punto de mira en los niños con discapacidad. En este grupo de agresores puede haber "adeptos", es decir, personas sin discapacidad que se sienten atraídas sexualmente por personas con discapacidad (en la mayoría de los casos, amputados y personas que utilizan equipos de movilidad), y algunos de ellos incluso se pueden hacer pasar por personas con discapacidad[31]. Entre los actos que estas personas pueden cometer están la descarga de fotografías y vídeos de niños con discapacidad (inofensivos por naturaleza) y su difusión a través de foros específicos o cuentas de medios sociales. Las herramientas de notificación presentes en los foros y medios sociales a menudo no cuentan con un procedimiento específico o apropiado para tratar dichos actos.

Resulta preocupante que la práctica del *sharenting* (la divulgación en línea de información y fotografías de niños por parte de sus progenitores) pueda violar la privacidad del niño, dar lugar a actos de intimidación, causar vergüenza o tener consecuencias negativas en un momento ulterior de su vida[32]. Los padres de niños con discapacidad pueden compartir dicha información al buscar ayuda o asesoramiento y exponer con ello a esos niños a un mayor riesgo de sufrir efectos adversos.

Algunos niños con discapacidad pueden experimentar dificultades al utilizar entornos en línea o incluso verse excluidos de ellos debido a su diseño inaccesible (por ejemplo, las aplicaciones que no permiten ampliar el tamaño del texto), se les pueden denegar los ajustes solicitados (por ejemplo, un programa informático de lectura de pantalla o equipos adaptativos para el control de ordenadores) o la ayuda apropiada necesaria (por ejemplo, orientación sobre cómo utilizar equipos o apoyo individual para interactuar socialmente[33]).

En relación con el riesgo contractual o la firma de cláusulas, los niños con discapacidad se exponen a un mayor riesgo de aceptar condiciones jurídicas que a veces ni los propios adultos logran entender.

---

30 Katrin Mueller-Johnson, Manuel P. Eisner e Ingrid Obsuth, *Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors*, Journal of Interpersonal Violence 29, núm. 17 (noviembre de 2014): 3180–3206, https://doi.org/10.1177/0886260514534529.

31 Richard L Bruno, *Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder*, Sexual and Disability 15, núm. 4 (1997), pág. 18, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

32 UNICEF, *Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy*, Innocenti Discussion Paper 2017-03 (Oficina de Investigación de UNICEF, Centro de Investigación Innocenti,), consultado el 16 de enero de 2020, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf

33 Si desea orientación sobre estos derechos, consulte la Convención sobre los Derechos de las Personas con Discapacidad, en particular el artículo 9 en materia de accesibilidad y el artículo 21 sobre la libertad de expresión y de opinión y el acceso a la información.

2.7 Percepción de los riesgos en línea por los niños

Los riesgos que destacan los niños son la exposición mundial a la violencia, el acceso a contenidos, bienes y servicios inapropiados, y las cuestiones relativas a la protección de datos y la privacidad[34].

Los adolescentes manifiestan diversas preocupaciones en relación con su utilización de las tecnologías digitales. Entre ellas están las preocupaciones que se plantean frecuentemente respecto de la seguridad en línea, como el miedo a interactuar con desconocidos en línea, a acceder a contenidos inapropiados o a la posibilidad de sufrir ataques de programas maliciosos o virus, mientras que otras guardan relación con la fiabilidad de su acceso a la tecnología, la intrusión de los padres en sus vidas "privadas" en línea y sus habilidades digitales[35].

Las investigaciones de EU Kids Online muestran que la pornografía y el contenido violento son las principales preocupaciones que tienen los niños en Europa en relación con sus actividades en línea. Por lo general, parece ser que la violencia preocupa más a los niños, mientras que las niñas manifiestan mayor preocupación por los riesgos relacionados con el contacto[36]. La preocupación por los riesgos es mayor en los niños procedentes de países con "mayores niveles de uso y riesgo".

En América Latina, las consultas realizadas a niños han demostrado que sus principales preocupaciones son la pérdida de privacidad, la violencia y el acoso[37]. Los niños indicaron que desconocidos se ponen en contacto con ellos, especialmente cuando juegan en línea. En esas circunstancias, parece ser que la principal estrategia consiste en no comunicar con esa persona o bloquearla. Las niñas sufren acoso en los medios sociales desde una edad temprana. Consiguen afrontar esas formas de violencia por sí mismas, bloqueando a los usuarios y cambiando los parámetros de privacidad. Los actos de acoso son cometidos por usuarios que a veces no hablan español pero logran enviarles imágenes, solicitar su amistad y formular comentarios sobre sus publicaciones. Algunos varones también indican haber recibido esas solicitudes.

En muchas partes del mundo, los niños entienden adecuadamente algunos de los riesgos a que se enfrentan en línea[38]. Las investigaciones han demostrado que la mayoría de ellos son capaces de distinguir entre el ciberacoso y las bromas o burlas en línea, y reconocen que el primero tiene una dimensión pública cuya finalidad es causar daño[39].

---

34 Amanda Third y otros, *Children's Rights in the Digital Age* (Melbourne: Young and Well Cooperative Research Centre, septiembre de 2014), http://www.uws.edu.au/__data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf.

35 Amanda Third y otros, *Young and Online: Children's Perspectives on Life in the Digital Age*, *The State of the World's Children 2017 Companion Report* (Sydney: Universidad de Western Sydney, 2017). En el informe se resumen las opiniones de 490 niños de entre 10 y 18 años, procedentes de 26 países diferentes y que abarcan en total 24 lenguas oficiales.

36 Livingstone, S. (2014) *EU Kids Online: Findings, methods, recommendations*. LSE, Londres: EU Kids Online, https://lsedesignunit.com/EUKidsOnline/.

37 Red Conectados al Sur network, "Hablatam".

38 Desde 2016, la UIT celebra consultas con niños y adultos interesados en el marco de la Iniciativa para la PIeL sobre cuestiones pertinentes como el ciberacoso, la alfabetización digital y las actividades de los niños en línea.

39 UNICEF, *Global Kids Online Comparative Report* (2019).

3 Preparación de una estrategia nacional de protección de la infancia en línea

Al elaborar una estrategia nacional de protección de la infancia en línea con el fin de promover la seguridad en línea de niños y jóvenes, los gobiernos nacionales y las instituciones encargadas de formular políticas deben identificar las prácticas idóneas y colaborar con los interesados claves.

En las secciones que figuran a continuación se destacan los actores e interesados habituales y se exponen las posibles funciones y responsabilidades que pueden tener respecto de la protección de la infancia en línea.

3.1 Actores y partes interesadas

Los encargados de formular políticas pueden identificar a las personas, grupos y organizaciones adecuadas que representen a cada uno de esos actores y partes interesadas en su jurisdicción. Es importante que valoren cada una de sus actividades actuales, previstas y posibles en toda labor de coordinación y orquestación de estrategias de la protección de la infancia en línea.

Niños y jóvenes

Los niños y jóvenes de todo el mundo han demostrado que pueden adaptarse con gran facilidad a las nuevas tecnologías y utilizarlas. Internet adquiere cada vez mayor importancia en las escuelas y se considera un lugar donde los niños pueden trabajar, jugar y comunicarse.

Según el último informe de ChildFund Alliance, tan solo el 18,1% de los niños entrevistados piensan que quienes gobiernan actúan en aras de su protección. Es importante que los encargados de formular políticas colaboren con los niños a este respecto y reconozcan su derecho a ser escuchados (art. 12 de la Convención sobre los Derechos del Niño).

Para poder brindar protección a los niños, los encargados de formular políticas deben normalizar la definición del concepto de niño en todos los documentos jurídicos. Un niño debe definirse como toda persona menor de 18 años. Esto está en consonancia con el Artículo 1 de la Convención de las Naciones Unidas sobre los Derechos del Niño, que establece que "se entiende por niño todo ser humano menor de 18 años de edad". No se debería permitir que las empresas tratasen como a un adulto a cualquier menor de 18 años, aunque haya alcanzado la edad legal para dar su consentimiento relativo al procesamiento de datos. Esta escueta definición no se fundamenta en ninguna prueba sobre los logros conseguidos en materia de desarrollo de la infancia y, además, menoscaba los derechos y pone en peligro la seguridad de los niños.

Si bien muchos niños pueden manifestar cierta seguridad en el uso de las tecnologías, otros muchos se sienten inseguros[40] en línea y tienen diversas preocupaciones[41] en relación con Internet.

La falta de experiencia de los niños y jóvenes con el mundo en general puede hacerlos vulnerables a una serie de riesgos. Tienen derecho a esperar que se les brinde ayuda y

[40] ChildFund Alliance, *VIOLENCE AGAINST CHILDREN AS EXPLAINED BY CHILDREN*, *Save Voices Big Dreams*, 2019, https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf.

[41] Consejo de Europa, *It's Our World: Children's Views on How to Protect Their Rights in the Digital World, Report on child consultations* (Consejo de Europa, División de Derechos del Niño, octubre de 2017), https://rm.coe.int/it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-/1680765dff.

protección. También es importante recordar que las vivencias de Internet o de las nuevas tecnologías que tienen todos los niños y jóvenes difieren. Algunos niños con necesidades especiales provocadas por discapacidad física o de otro tipo podrían ser particularmente vulnerables en un entorno en línea y necesitarán apoyo adicional.

Las encuestas realizadas han demostrado reiteradamente que existe una gran diferencia entre lo que los adultos piensan que hacen los niños y jóvenes en línea y lo que realmente ocurre. La mitad de los niños entrevistados afirmaron que en sus países respectivos los adultos no escuchaban su opinión sobre cuestiones que les atañen[42]. Por esta razón, es importante velar por que en los acuerdos concertados a escala nacional para establecer políticas en esta esfera se incluyan mecanismos adecuados para que se pueda oír la voz de todos los niños y jóvenes y se tengan en cuenta sus experiencias concretas con el uso de la tecnología.

Padres, tutores y educadores

Los padres, tutores y educadores pasan la mayor parte de su tiempo con niños. Deben recibir una educación digital para entender el entorno en línea y ser capaces de proteger a los niños y enseñarles a protegerse a sí mismos.

Las instituciones educativas tienen la responsabilidad concreta de enseñar a los niños la manera de garantizar su seguridad en línea, ya estén utilizando Internet en la escuela, el hogar o cualquier otro sitio, y los encargados de formular políticas deben incluir en el programa nacional la formación digital desde una edad muy temprana (de los 3 a los 18 años). De este modo, los niños podrían protegerse a sí mismos, conocer sus derechos y, por consiguiente, utilizar Internet como facilitador del conocimiento[43].

Cabe recordar a los encargados de formular políticas que los padres y tutores siempre serán la primera, última y más sólida línea de defensa y apoyo para sus propios hijos y niños bajo su responsabilidad. Sin embargo, estos pueden sentirse un poco perdidos en lo que se refiere a Internet. Una vez más, las escuelas pueden actuar en este contexto como un canal importante para llegar a los padres y tutores, a fin de informarlos sobre los riesgos y las numerosas oportunidades positivas que entrañan las nuevas tecnologías. No obstante, las escuelas no deben ser la única ruta que se tome para llegar a los padres y tutores. Es importante utilizar múltiples y diferentes canales con miras a aumentar al máximo las posibilidades de llegar al mayor número posible de padres y tutores. A este respecto, el sector privado desempeña un papel fundamental para apoyar a sus usuarios o clientes. Los padres y tutores tienen la opción de administrar la actividad y el acceso en línea de los niños, hablar con ellos sobre la conducta adecuada que deben adoptar frente a las tecnologías y el uso que les deben dar, y entender qué hacen los niños en línea de manera que la familia integre en sus conversaciones las experiencias en línea y fuera de línea como un conjunto.

Los padres y tutores también deben dar ejemplo a los niños sobre cómo utilizar sus dispositivos y comportarse de manera apropiada en Internet.

Se debe recordar a los encargados de formular políticas que los padres y cuidadores han de ser consultados para recabar sus opiniones, experiencias y entendimiento de la protección de sus hijos y niños en línea.

---

42 ChildFund Alliance, *Violence against children as explained by children*.

43 UNICEF, *Policy Guide on Children and Digital Connectivity* (Policy Lab, Data, Research and Policy, Fondo de las Naciones Unidas para la Infancia, junio de 2018), https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

Por último, los encargados de formular políticas junto con otras instituciones públicas pueden elaborar campañas de sensibilización pública para padres, cuidadores y educadores, entre otros destinatarios. Las bibliotecas públicas, los centros de salud, e incluso los centros comerciales y otros importantes centros de venta al por menor pueden ofrecer vías accesibles para la difusión de información en materia de ciberseguridad y aptitudes digitales. Al llevar a cabo esta tarea, los gobiernos deben velar por que el asesoramiento que se dé sea neutral, carezca de intereses privados y cubra una amplia variedad de cuestiones relacionadas con el espacio digital.

Sector privado

El sector privado es uno de los interesados clave del ecosistema, ya que cuenta con los conocimientos tecnológicos que los encargados de formular políticas necesitan abordar y entender a fin de elaborar el marco jurídico correspondiente. Por consiguiente, es fundamental que los encargados de formular políticas incluyan al sector privado en el proceso de elaboración de leyes en materia de protección de la infancia en línea.

Asimismo, es importante alentar al sector privado a que incorpore en sus actividades un enfoque de seguridad desde el diseño a la hora de desarrollar nuevas tecnologías. Evidentemente, las empresas que están desarrollando o proporcionando productos y servicios basados en nuevas tecnologías deben ayudar a sus usuarios a entender cómo funcionan y cómo pueden utilizarlos de una manera segura y apropiada.

El sector privado también tiene la importante responsabilidad de ayudar a promover la conciencia acerca del programa de seguridad en línea, en particular ante los niños y sus padres o tutores, pero también ante la comunidad en general. Al implicarse de este modo, el sector privado conocerá mejor las inquietudes de otras partes interesadas y los riesgos y daños a que se exponen los usuarios finales. Con esos conocimientos, el sector privado podría corregir los productos y servicios existentes e identificar los peligros de los que estén en fase de desarrollo.

Los recientes avances en la esfera de la inteligencia artificial están allanando el camino para que el sector privado se base en mecanismos de control mucho más sólidos a fin de identificar al usuario y proporcionar a los niños un entorno que favorezca una conducta en línea positiva. Asimismo, estos avances también podrían plantear nuevos riesgos para los niños.

En algunos países, Internet se rige por un marco de autorregulación o corregulación. Sin embargo, determinados países están contemplando la posibilidad de instaurar o ya han instaurado marcos jurídicos y reglamentarios que entre otras cosas imponen a las empresas la obligación de detectar, bloquear y/o retirar de las plataformas o servicios los elementos nocivos para los niños, y la de proporcionar vías de notificación claras y un servicio de soporte.

La comunidad científica y las organizaciones no gubernamentales

En las universidades y la comunidad científica, es muy probable que haya personas instruidas y eruditos con un interés profesional en las repercusiones sociales y técnicas de Internet, y con un conocimiento muy detallado al respecto. Estas personas son una fuente de ayuda muy valiosa para los gobiernos nacionales y los encargados de formular políticas a la hora de elaborar estrategias basadas en hechos concretos y pruebas fidedignas. Asimismo, podrían actuar como un contrapeso intelectual de los intereses empresariales que a veces pueden tener una duración demasiado corta y un carácter comercial.

De manera análoga, en la comunidad de las organizaciones no gubernamentales (ONG) hay un acervo de conocimientos especializados y datos que pueden constituir un recurso inestimable para llegar a los niños, padres, cuidadores y educadores y proporcionarles servicios con el fin de promover el programa de seguridad en línea y, de manera general, defender el interés público.

Observancia de la ley

Triste es advertir que, por maravillosa que sea la tecnología, también ha atraído la atención de elementos delictivos y antisociales. Internet ha contribuido a aumentar en gran medida la circulación de materiales de tipo MASI y de otros elementos dañinos en línea. Los depredadores sexuales han utilizado Internet para entablar un contacto inicial con niños, seduciéndolos para que establezcan formas de contacto muy dañinas, tanto en línea como fuera de línea. La intimidación y otras formas de acoso pueden ser muy perjudiciales para la vida de los niños, e Internet ha proporcionado una nueva forma de hacerlo.

Por estos motivos, es indispensable que la comunidad encargada de hacer cumplir la ley participe plenamente en toda estrategia general encaminada a lograr que Internet sea más segura para los niños y jóvenes. Los funcionarios encargados de hacer cumplir la ley deben recibir formación adecuada para efectuar investigaciones sobre delitos cometidos contra niños y jóvenes en relación con Internet. Deben poseer el nivel adecuado de conocimientos técnicos y tener acceso a instalaciones forenses que les permitan extraer e interpretar los datos obtenidos de ordenadores o de Internet con la mayor brevedad posible.

Además, es muy importante que los organismos encargados de hacer cumplir la ley establezcan mecanismos inequívocos para que los niños y jóvenes, o cualquier miembro de la población, puedan notificar todo incidente o preocupación que tengan respecto de la seguridad de un niño o un joven en línea. Por ejemplo, muchos países han creado líneas de ayuda para facilitar las notificaciones relativas a los materiales de tipo MASI y mecanismos especializados similares para notificar otros tipos de problemas, como la intimidación. Los encargados de formular políticas deben colaborar con la INHOPE (asociación internacional de líneas de ayuda acerca de Internet), brindarle apoyo para evaluar y tramitar las notificaciones relativas a los materiales de tipo MASI, y aprovechar asimismo la asistencia que esta asociación presta a organizaciones de todo el mundo que carecen de líneas de ayuda para que las establezcan. Los encargados de formular políticas deben velar por que haya canales de comunicación abiertos entre los responsables de hacer cumplir la ley y otras partes interesadas. Los organismos encargados de la observancia de la ley constituyen la principal fuente de incautación de material de tipo MASI dentro de las fronteras de un país. Se debe establecer un proceso para examinar estos materiales con miras a determinar si se pueden o no identificar las víctimas locales. Cuando no es posible, se deben remitir los materiales a INTERPOL para que los incluya en la Base de Datos Internacional sobre Explotación Sexual de Niños. Dado que se trata de una amenaza mundial, los encargados de formular políticas deben velar por la cooperación internacional entre los organismos encargados de hacer cumplir la ley de todo el mundo. Esto reduciría el tiempo destinado a las formalidades y permitiría a los agentes del orden recibir una respuesta rápida.

Servicios sociales

Es probable que los niños o jóvenes que hayan sufrido daños o abusos en línea, por ejemplo, cuando se haya publicado una imagen inapropiada o ilícita de ellos, necesiten apoyo o asesoramiento especializado y a largo plazo. También puede ser necesario que haya servicios integrales y prácticas restaurativas para agresores, en particular jóvenes agresores que también

podrían haber sido víctimas de abusos en línea o fuera de línea. Los profesionales dedicados a la prestación de servicios sociales tendrán que recibir formación apropiada para ofrecer este tipo de apoyo. Este apoyo deberá prestarse a través de canales en línea y fuera de línea.

Servicios de atención sanitaria

El servicio de atención sanitaria que se necesita después de todo caso de violencia infantil deberá estar cubierto por el plan de atención sanitaria básica a nivel nacional. Las instituciones de asistencia sanitaria deben cumplir con sus obligaciones en materia de notificación de abusos. Los profesionales de la salud deben tener los equipos y conocimientos adecuados para poder apoyar a los niños a este respecto. Los servicios de atención sanitaria deben abarcar el apoyo a la salud y el bienestar de los niños.

Ministerios

La política de protección de la infancia en línea es competencia de varios ministerios y es importante que todos ellos participen en ella para que toda estrategia y plan de acción nacional tenga éxito. Entre esos ministerios pueden estar los que se encargan de:

- los asuntos interiores
- la salud
- la educación
- la justicia
- el entorno digital y la información
- los organismos reguladores

Los organismos reguladores son los que están en mejores condiciones para contribuir a la función de control y rendición de cuentas en colaboración con las instituciones gubernamentales. Entre ellos podrían figurar los organismos reguladores que se encargan de los medios de comunicación y la protección de datos.

Operadores de redes de banda ancha, móviles y WiFi

Los operadores pueden detectar, bloquear y notificar contenido ilícito en sus redes y proporcionar herramientas, servicios y configuraciones fáciles de utilizar por las familias para que los padres decidan cómo administrar el acceso de sus hijos. Es importante que los proveedores velen también por el respeto de las libertades civiles y la privacidad.

Derechos del niño

Las instituciones independientes de derechos humanos para la infancia pueden desempeñar un papel fundamental para garantizar la protección de los niños en línea. Aunque sus mandatos difieran, estas instituciones tienen a menudo las siguientes funciones:

- supervisar los efectos de la ley, la política y la práctica en la protección de los derechos del niño;
- promover la aplicación de las normas internacionales de derechos humanos a nivel nacional;
- investigar las violaciones de los derechos de los niños;
- facilitar a los tribunales sus conocimientos especializados sobre los derechos del niño;
- velar por que se escuchen las opiniones de los niños sobre cuestiones relativas a sus derechos humanos, en particular la elaboración de leyes y políticas pertinentes;
- promover la comprensión y sensibilización públicas sobre los derechos del niño; y

- emprender iniciativas de educación y formación en materia de derechos humanos.

Es importante que se incluyan consultas directas con los niños, ya que forman parte de sus derechos en virtud del artículo 12 de la Convención de las Naciones Unidas sobre los Derechos del Niño. Todas las funciones educativas, de asesoramiento, investigación y sensibilización de las instituciones independientes de derechos humanos para la infancia son pertinentes para prevenir los daños que los niños pueden sufrir en línea y reaccionar ante ellos. Por consiguiente, dichas instituciones deben ser un elemento central del proceso de elaboración de un enfoque integral y basado en derechos, encaminado a fortalecer los marcos jurídicos, reglamentarios y de política que regulan la protección de la infancia en línea, que incluya la celebración de consultas directas a niños, con arreglo a su derecho recogido en el art. 12 de la Convención de las Naciones Unidas sobre los Derechos del Niño.

Recientemente, también se han dado casos en que algunas jurisdicciones han establecido o estudiado la posibilidad de establecer organismos estatales encargados concretamente de apoyar los derechos de los niños en línea, incluida su protección frente a la violencia y el daño. En caso de existan tales organismos, también deberían contribuir en sumo grado a las medidas encaminadas a reforzar las actividades de respuesta para la protección de la infancia en línea en el plano nacional.

3.2 Actividades de respuesta en curso para la protección de la infancia en línea

Se han elaborado varias iniciativas a fin de actuar en los planos nacional e internacional frente a la creciente importancia de las TIC en las vidas de los niños en todo el mundo y los riesgos inherentes que suponen para los más jóvenes de nuestras sociedades.

Modelos nacionales

A nivel nacional, deben destacarse varios instrumentos legislativos debido a que abarcan aspectos importantes de un marco exhaustivo sobre la protección de la infancia en línea. Entre ellos cabría citar como ejemplo los siguientes:

- la Directiva de Servicios de Comunicación Audiovisual (DSCA) (revisada en 2018, UE); y
- el Reglamento General de Protección de Datos (RGPD) (2018, UE).

Ha habido avances innovadores en la respuesta de las autoridades reguladoras e instituciones de los Estados Miembros a las amenazas para la seguridad y el bienestar de los niños en línea. Aunque no existe una única vía para reaccionar ante los materiales de tipo MASI, el ciberacoso y otros daños que los niños pueden sufrir en línea, cabe destacar que se han puesto a prueba nuevos métodos durante los últimos años, entre ellos:

El Código de diseño apropiado para la edad (2019, Reino Unido)

A principios de 2019, la Oficina del Comisionado de Información publicó unas propuestas para su "código de diseño apropiado para la edad" a fin de mejorar la protección de la infancia en línea. El código propuesto se centró en el interés superior del niño, establecido en la Convención de las Naciones Unidas sobre los Derechos del Niño, y determinó varias expectativas para el sector privado. Entre ellas figuraban sólidas medidas de verificación de la edad, la desactivación por defecto de los servicios de localización para niños, la estricta reducción al mínimo de la cantidad de datos personales de niños que el sector privado puede

recabar y conservar, la elaboración de productos seguros desde el diseño y la presentación de explicaciones adaptadas a la edad y accesibles.

La Ley de comunicaciones digitales nocivas (revisada en 2017, Nueva Zelandia)

La Ley de 2015 tipificó específicamente como delito el ciberabuso y se centra en una amplia variedad de actos dañinos, desde el ciberacoso hasta la pornovenganza. Su objetivo es desalentar, prevenir y reducir las comunicaciones digitales dañinas, prohibiendo por ley la publicación de comunicaciones digitales destinadas a provocar una gran angustia a terceros, y establece un conjunto de diez principios para las comunicaciones. Otorga a los usuarios la capacidad de presentar reclamaciones ante una organización independiente en caso de incumplimiento de dichos principios y de solicitar por vía judicial que se dicte una orden contra el autor de la comunicación o el sistema que la aloja si la cuestión no se resuelve por la primera vía.

El Comisionado de Ciberseguridad (2015, Australia)

El Comisionado de Ciberseguridad es el primer organismo gubernamental del mundo dedicado específicamente a la seguridad en línea. Instaurado en 2015, el Comisionado de Ciberseguridad tiene la función legislativa de dirigir, coordinar, educar y asesorar sobre cuestiones de seguridad en línea a fin de velar por que la experiencia en línea de todos los australianos sea segura, positiva y capacitadora. El Comisionado de Ciberseguridad administra programas de investigación que se centran en diversos daños como los actos graves de ciberacoso infantil, el abuso basado en imágenes y los contenidos prohibidos. Está facultado para llevar a cabo investigaciones y adoptar medidas para tratar reclamaciones o denuncias relativas a estos tipos de daños e incluso puede, en determinados casos, emitir notificaciones a particulares y servicios en línea para retirar materiales. Además de estas facultades de investigación, el Comisionado de Ciberseguridad aplica un enfoque comunitario integral, basado en iniciativas e intervenciones sociales, culturales y tecnológicas. Su labor de prevención, protección y proactiva permite abordar de manera exhaustiva la seguridad en línea.

Modelos internacionales

Diferentes partes interesadas han formulado recomendaciones y normas en los planos internacional y transnacional. Las presentes directrices se basan en la labor realizada en el marco de las siguientes medidas:

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.

Directrices del Consejo de Europa para respetar, proteger y hacer efectivos los derechos del niño en el entorno digital[44].

Las directrices se destinan a todos los Estados miembros del Consejo de Europa, con el fin de ayudar a estos y otros interesados pertinentes en su labor encaminada a adoptar un enfoque integral y estratégico para potenciar toda la gama de derechos del niño en el entorno digital.

[44] Consejo de Europa (2020), *The Digital Environment,* https://www.coe.int/en/web/children/the-digital-environment. Las Directrices del Consejo de Europa para respetar, proteger y hacer efectivos los derechos del niño en el entorno digital es el primer conjunto de normas de ese tipo adoptadas por un órgano intergubernamental (CM/Rec, 2018).

Entre los múltiples temas que se abordan en ellas están la protección de los datos personales, el suministro de contenidos adaptados a los niños y a la evolución de sus capacidades, las líneas de ayuda y de emergencia, la vulnerabilidad y la resiliencia, así como la función y las responsabilidades de las empresas. Además, en las directrices se insta a los estados a que cooperen con los niños, en particular en los procesos de toma de decisiones, a fin de velar por que las políticas nacionales aborden adecuadamente los avances del entorno digital. Estas directrices se encuentran disponibles en 19 idiomas. Estarán acompañadas de una versión del documento adaptada a los niños, así como de un Manual para los encargados de formular políticas, en que se proporcionarán medidas concretas para llevarlas a la práctica.

Consejo de Europa - Convenio de Lanzarote

El Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual (el Convenio de Lanzarote) exige a los Estados que ofrezcan una respuesta integral a la violencia sexual contra niños, adoptando el "criterio de las cuatro P": prevención, protección, persecución y promoción de la cooperación nacional e internacional. La aplicación del Convenio en relación con el entorno digital ha sido aclarada por el Comité de las Partes en el Convenio sobre la protección de los niños contra la explotación y el abuso sexual (el "Comité de Lanzarote"), mediante la adopción de una serie de documentos. Estos son: una opinión sobre los vídeos e imágenes de niños, sexualmente sugerentes o explícitos, generados, compartidos y recibidos por niños (de 6 de junio de 2019); una opinión interpretativa sobre la aplicabilidad del Convenio de Lanzarote a los delitos sexuales contra niños facilitados por la utilización de las TIC (12 de mayo de 2017); una declaración sobre sitios web en que se anuncian materiales o imágenes de abusos sexuales a niños u otros delitos establecidos de conformidad con el Convenio de Lanzarote (16 de junio de 2016); y una Opinión sobre el artículo 23 del Convenio de Lanzarote sobre las proposiciones hechas a niños con fines sexuales mediante tecnologías de la información y la comunicación (seducción). El Comité de Lanzarote supervisa la aplicación del Convenio: su segunda ronda de supervisión temática se centra en la protección de los niños contra la explotación y el abuso sexual facilitados por las TIC, sobre la que se publicará un informe en 2020. En 2019, había un total de 46 Estados Parte en el Convenio, entre ellos Túnez, que fue el primer Estado no miembro en adherirse a él.

Otras directrices del Consejo de Europa

El Consejo de Europa ha creado otras normas e instrumentos que contribuyen a un acervo colectivo para elaborar un marco integral destinado a todos los interesados. En el Convenio sobre la Ciberdelincuencia del Consejo de Europa se imponen obligaciones a las Partes para que tipifiquen como delito una serie de actos relacionados con el material de abuso sexual infantil. Hasta la fecha, lo han ratificado 64 Estados parte. Entre otras cosas, el Consejo de Europa tiene por objeto capacitar a los niños y a quienes los rodean para utilizar de manera segura el entorno digital. Este objetivo se promueve mediante herramientas pedagógicas como un manual sobre el alfabetismo en Internet, completamente revisado (2017), un manual sobre la educación en materia de ciudadanía digital (2019) y manuales destinados a los padres (*Parenting in the digital age – Parental guidance for the online protection of children from sexual exploitation and sexual abuse* (2017); *Digital citizenship…and your child – What every parent needs to know and do* (2019)). Por último, el Consejo de Europa ha llevado a cabo una investigación en consulta con niños acerca de sus derechos en el entorno digital (*It's our world: Children's views on how to protect their rights in the digital environment*, 2017) y realizó algunas de las primeras investigaciones por consultas centradas en las experiencias de los niños con

discapacidad en el entorno digital (*Two clicks forward and one click back: Report on children with disabilities in the digital environment*, 2019).

Informe sobre la seguridad de la infancia en línea

Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online y *Child Online Safety Universal Declaration*[45].

Recomendaciones de la OCDE sobre la protección de la infancia en línea (2012, revisadas en 2019-2020).

También deberían destacarse otras iniciativas nacionales y transnacionales que contribuyen a la cooperación internacional así como medidas nacionales destinadas a elaborar estrategias para la protección de la infancia en línea. Entre otros ejemplos, cabría citar:

La Base de Datos Internacional sobre Imágenes relacionadas con la Explotación Sexual de Niños

Administrada por INTERPOL, la Base de Datos Internacional sobre Imágenes relacionadas con la Explotación Sexual de Niños (Base de Datos ICSE) constituye un potente instrumento de investigación e información policial que permite a los investigadores especializados intercambiar datos con colegas de todo el mundo. Disponible a través del sistema mundial de comunicación policial protegida (conocido como I-24/7), la Base de Datos ICSE utiliza programas informáticos avanzados de comparación de imágenes para establecer relaciones entre víctimas, agresores y lugares. La Base de Datos ICSE permite a los usuarios certificados de los países miembros acceder a ella en tiempo real, consultar los elementos de que ya se dispone, cargar nuevos datos, clasificar y organizar materiales, evitar la duplicación de esfuerzos, llevar a cabo análisis y comunicar con otros expertos del mundo para responder a las consultas relacionadas con investigaciones sobre casos de explotación sexual infantil.

La Alianza Mundial WePROTECT

La Alianza Mundial WePROTECT (WPGA) es un movimiento mundial que aúna la influencia, los conocimientos especializados y los recursos necesarios para transformar la manera de abordar en todo el mundo la explotación sexual de niños en línea. Se trata de una alianza entre gobiernos, empresas tecnológicas mundiales y organizaciones de la sociedad civil. En ella participan múltiples actores y es única en este ámbito. La Alianza Mundial WePROTECT tiene por objeto identificar y proteger a un número mayor de víctimas, detener a más agresores y poner fin a la explotación sexual de niños en Internet.

La Alianza Mundial WePROTECT consta de varios elementos, en particular un Modelo de Respuesta Nacional y una Respuesta Estratégica Global. En el Anexo 3 figura más información al respecto.

El Índice de Seguridad de la Infancia en Línea de 2020

El Índice de Seguridad de la Infancia en Línea, desarrollado por el DQ Institute, constituye la primera plataforma analítica en tiempo real a nivel mundial que ayuda a las naciones a controlar mejor la seguridad de los niños en línea.

[45] Comisión de la Banda Ancha para el Desarrollo Sostenible (2019), *The State of Broadband 2019: Broadband as a Foundation for Sustainable Development,* https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

El Índice de Seguridad de la Infancia en Línea se basa en seis pilares que conforman su marco. Los pilares primero y segundo, sobre los ciberriesgos y la utilización digital disciplinada, guardan relación con el uso prudente de las tecnologías digitales. Los pilares tercero y cuarto, sobre las competencias y la orientación y educación en materia digital, se refieren a la capacitación. Los dos últimos pilares guardan relación con la infraestructura y versan sobre la infraestructura social y la conectividad.

3.3 Ejemplos de respuestas a los elementos dañinos en línea

En el Anexo 4 se exponen una serie de ejemplos de respuestas a elementos dañinos en línea. En ellos se abordan respuestas educativas, medidas legislativas y la identificación de elementos dañinos en línea.

3.4 Beneficios de una estrategia nacional de protección de la infancia en línea

Armonización legislativa

Para lograr el objetivo de la ciberseguridad mundial, es fundamental que en todos los países se adopte una legislación apropiada contra la utilización indebida de las TIC con fines delictivos o de otra índole. Puesto que las amenazas pueden proceder de cualquier lugar del planeta, los problemas que acarrean tienen un alcance inherentemente internacional y requieren que se instaure la cooperación internacional, así como la asistencia en materia de investigación y se definan disposiciones sustantivas y de procedimiento comunes. Por consiguiente, es importante que los países armonicen sus marcos jurídicos para combatir el ciberdelito, proteger a los niños en línea y facilitar la cooperación internacional[46].

La elaboración de una legislación nacional adecuada, acompañada de su correspondiente marco jurídico para combatir el ciberdelito y, en esa misma línea, la armonización legislativa a nivel internacional, son requisitos esenciales para que toda estrategia nacional de protección de la infancia en línea tenga éxito. Esto requiere ante todo que se establezcan las necesarias disposiciones de derecho penal sustantivo para tipificar como delito actos como el fraude informático, el acceso ilegal, la interferencia de datos, las violaciones de los derechos de autor y los materiales de tipo MASI, y se vele a la vez por que no se castigue indebidamente a los niños. El hecho de que el código penal contenga disposiciones aplicables a actos similares cometidos en el mundo real no implica que estas se puedan aplicar por analogía a los actos cometidos por Internet. Por consiguiente, es fundamental realizar un análisis exhaustivo de las leyes nacionales en vigor para identificar cualquier posible deficiencia legislativa. El siguiente paso consistiría en identificar y definir el léxico y los materiales de referencia legislativos que pueden ayudar a los países a instaurar normas procesales y leyes armonizadas en materia de ciberdelincuencia. Los países podrían utilizar esos útiles instrumentos para elaborar un marco jurídico sobre ciberseguridad y leyes conexas. La UIT ha estado colaborando a tales efectos con Estados Miembros y partes interesadas pertinentes y está aportando una gran contribución al avance de la armonización mundial de las leyes en materia de ciberdelincuencia.

Dada la rapidez de la innovación tecnológica, la autorregulación y la corregulación se han propuesto como posibles soluciones para la obsolescencia de las normas existentes y el largo

[46] Comisión de la Banda Ancha para el Desarrollo Sostenible (2019).

proceso legislativo. Sin embargo, para que estas soluciones sean eficaces, los organismos reguladores y los encargados de formular políticas deben definir claramente ciertos objetivos y desafíos en materia de protección de la infancia en línea, instaurar un proceso y una metodología de revisión claros para evaluar la eficacia de la autorregulación y la corregulación y, en caso de que estas no consiguieran resolver los problemas identificados, iniciar un proceso legislativo formal para encararlos. Asimismo, en el marco del proceso legislativo se podrían incorporar gradualmente a la legislación en vigor medidas de autorregulación que hayan resultado satisfactorias para que actuasen como mecanismo de protección y evitar así que se retroceda en el cumplimiento de ciertas iniciativas de autorregulación o que estas se dejen de cumplir.

Coordinación

Es probable que algunos de los diversos actores y colectivos interesados ya hayan puesto en práctica actividades y medidas destinadas a proteger a los menores en línea, pero de forma aislada. Comprender estas iniciativas es importante para valorar los esfuerzos ya desplegados con miras a elaborar una estrategia nacional de protección de la infancia en línea. La estrategia permitirá coordinar y dirigir toda esta labor mediante la orquestación de las actividades en curso y de otras nuevas.

4 Recomendaciones relativas a los marcos y su aplicación

Los gobiernos deben combatir todas las manifestaciones de violencia contra niños en el entorno digital. No obstante, las medidas adoptadas para proteger a los niños en dicho entorno no deben restringir indebidamente el ejercicio de otros derechos, como el derecho a la libertad de expresión, el derecho de acceso a la información o el derecho a la libertad de asociación. En lugar de poner coto a la curiosidad innata y al sentido de la innovación de los niños por miedo a que se enfrenten a riesgos en línea, es fundamental aprovechar el ingenio de los niños y mejorar su resiliencia al tiempo que se explora el potencial del entorno digital.

En muchos casos, los actos de violencia contra niños son cometidos por otros niños. En tales situaciones, los gobiernos han de adoptar en la medida de lo posible enfoques restaurativos que reparen el daño causado y, al mismo tiempo, eviten que se penalice a los niños. Los gobiernos deben fomentar la utilización de las TIC para prevenir y hacer frente a la violencia, por ejemplo, alentando el desarrollo de tecnologías y recursos para que los niños accedan a la información, bloqueen el material nocivo y notifiquen los casos de violencia cuando se produzcan[47].

A fin de hacer frente a la situación mundial de la seguridad infantil en línea, los gobiernos deben facilitar la comunicación entre sus organismos pertinentes y cooperar abiertamente para eliminar los daños causados a los niños en línea.

4.1 Recomendaciones relativas a los marcos

4.1.1 Marco jurídico

Los gobiernos deben examinar y, cuando proceda, actualizar su marco jurídico para respaldar la plena efectividad de los derechos del niño en el entorno digital. Un marco jurídico integral debe abordar medidas preventivas; prohibir todas las formas de violencia contra niños en el entorno digital; ofrecer medidas de reparación, recuperación y reintegración eficaces para hacer frente a las violaciones de los derechos del niño; establecer mecanismos de asesoramiento, notificación y reclamación adaptados a los menores; e instaurar mecanismos de rendición de cuentas para luchar contra la impunidad[48].

Siempre que resulte posible, la legislación debe ser tecnológicamente neutra, de manera que su aplicabilidad no se vea menoscabada por avances tecnológicos futuros[49].

Para que la legislación se aplique de manera efectiva, es necesario que los gobiernos adopten medidas complementarias, por ejemplo, iniciativas de sensibilización y movilización social, actividades y campañas educativas y acciones de capacitación de los profesionales que trabajan con y para los niños.

---

47 Representante Especial del Secretario General sobre la Violencia contra los Niños, *Informe anual de la Representante Especial del Secretario General sobre la Violencia contra los Niños al Consejo de Derechos Humanos*, A/HRC/31/20 (enero de 2016), párrs. 103 y 104.

48 Representante Especial del Secretario General sobre la Violencia contra los Niños, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (Nueva York: Naciones Unidas), pág. 55.

49 Representante Especial del Secretario General sobre la Violencia contra los Niños, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (Nueva York: Naciones Unidas), pág. 64.

A fin de elaborar leyes apropiadas, también es importante tener presente que los niños no constituyen un grupo homogéneo. Tal vez se necesiten respuestas diferentes para los niños de diferentes grupos de edades, los que tengan necesidades específicas o los que corran un riesgo más elevado de sufrir daños en el entorno digital o a través de este.

Los gobiernos deben crear un entorno jurídico y reglamentario claro y previsible que ayude a las empresas y demás terceros a cumplir sus responsabilidades relativas a la protección de los derechos del niño en el marco de sus actividades, tanto en su país como en el extranjero[50].

A continuación se exponen diversos aspectos que los encargados de formular políticas considerarán útiles para revisar el alcance de sus marcos jurídicos y las garantías ofrecidas en ellos:

- la seducción u otras formas de instigación, extorsión o coacción a distancia de menores para que establezcan contactos sexuales o realicen actividades sexuales de manera inapropiada;
- la posesión, producción y distribución de materiales de tipo MASI, con independencia de la intención de distribuirlos;
- el acoso, la intimidación, el abuso o el discurso de odio en línea;
- el material de naturaleza terrorista en línea;
- la ciberseguridad;
- la consideración de que todo lo que es ilegal fuera de línea también lo es en línea.

4.1.2 Marcos institucionales y de políticas

Para garantizar la efectividad de los derechos del niño en el entorno digital, es necesario que los gobiernos logren un equilibrio entre el aprovechamiento al máximo de las ventajas que presenta la utilización de las TIC por los niños y la reducción al mínimo de los riesgos asociados a dicha utilización. Este equilibrio se puede conseguir incluyendo en los planes nacionales de banda ancha medidas para proteger a los niños en línea[51] y elaborando una estrategia de protección de la infancia en línea independiente y polifacética. Ese tipo de agenda se debe integrar plenamente en todos los marcos de política en vigor que guarden relación con los derechos o la protección del niño y además debe completar las políticas nacionales de protección de la infancia ofreciendo un marco específico que cubra todos los riesgos y posibles daños para los niños con miras a crear un entorno digital seguro, inclusivo y capacitador[52].

Los gobiernos deben instaurar un marco de coordinación nacional con un mandato claro y suficientes facultades para coordinar todas las actividades relacionadas con los derechos del niño y los medios digitales y las TIC en todos los sectores y en los planos nacional, regional y local. Los gobiernos han de incluir en el marco objetivos sujetos a plazos y un proceso transparente para evaluar y supervisar los progresos realizados y deben velar por que se pongan a disposición todos los recursos humanos, técnicos y financieros necesarios para el funcionamiento eficaz de dicho marco[53].

---

50 Comité de los Derechos del Niño de las Naciones Unidas, *Observación general núm. 16,* párr. 53.

51 *The State of the Broadband 2019*, Recomendación 5.6, pág. 78. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

52 Véase el Capítulo 10 del Informe sobre la seguridad de la infancia en línea para consultar las disposiciones modelo sobre la protección de la infancia para los planes nacionales de banda ancha.

53 Representante Especial del Secretario General sobre la Violencia contra los Niños, *Informe anual de la Representante Especial del Secretario General sobre la Violencia contra los Niños* (diciembre de 2014) A/HRC/28/55 y *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children*, 2014 (Nueva York: Naciones Unidas), párr. 55. 88.

Los gobiernos deben establecer una plataforma multipartita para dirigir la elaboración, la aplicación y la supervisión de la agenda digital nacional para los niños. Esta plataforma debería reunir a los representantes de los grupos más importantes, por ejemplo: los niños y jóvenes; las asociaciones de padres/cuidadores; las secciones pertinentes del gobierno; los sectores de la educación, la justicia, la salud y la atención social; las instituciones nacionales de derechos humanos y los organismos reguladores pertinentes; la sociedad civil; el sector privado; las instituciones académicas; y las asociaciones profesionales pertinentes.

4.1.3 Marco reglamentario

Los gobiernos son responsables de las violaciones de los derechos del niño causadas por empresas o con la contribución de estas, si no han adoptado las medidas apropiadas, razonables y necesarias para impedir o reparar dichas violaciones, o si han tolerado o colaborado de alguna otra forma en su comisión[54].

Los Principios Rectores sobre las empresas y los derechos humanos prevén que las empresas deben proporcionar mecanismos de reparación y reclamación que sean legítimos, accesibles, previsibles, justos, compatibles con los derechos y transparentes, estén basados en el diálogo y el compromiso y constituyan una fuente de aprendizaje continuo. Los mecanismos de reclamación establecidos por las empresas pueden proporcionar soluciones alternativas flexibles y oportunas y, a veces, pueden constituir el medio más conveniente en el interés superior del niño para atender las preocupaciones planteadas en relación con la conducta de una empresa. En todos los casos, se deberá poder recurrir a los tribunales o a la revisión judicial de las medidas de reparación administrativas, así como a otros procedimientos[55]. Se debería analizar la posibilidad de establecer mecanismos que creen servicios seguros y adaptados a la edad de los niños para que los usuarios comuniquen sus preocupaciones.

Sin perjuicio de los mecanismos de reclamación que estén en vigor en cada país, los gobiernos deben establecer mecanismos de supervisión para investigar y reparar las violaciones de los derechos del niño con miras a mejorar la rendición de cuentas de las empresas de TIC y otras empresas pertinentes, y reforzar la responsabilidad de sus organismos reguladores respecto de la elaboración de normas relativas a los derechos del niño y las TIC[56]. Esto es especialmente importante debido a que las demás medidas de reparación de que disponen las personas perjudicadas por la actividad empresarial, como los procedimientos civiles y otras formas de reparación judicial, suelen resultar engorrosas y onerosas[57].

El Comité de los Derechos del Niño de las Naciones Unidas ha subrayado la función que pueden desempeñar las instituciones de derechos humanos en esta esfera, destacando la manera en que podrían recibir, investigar y mediar en relación con las denuncias de violaciones cometidas por entidades del sector privado; realizar investigaciones públicas sobre abusos en gran escala; y examinar las leyes a fin de velar por el cumplimiento de la Convención sobre los Derechos del Niño. El Comité ha indicado que, cuando sea necesario, "los Estados deben ampliar el mandato legislativo de las instituciones nacionales de derechos humanos para dar

[54] Comité de los Derechos del Niño de las Naciones Unidas, *Observación general núm. 16,* párr. 28.
[55] Informe del Representante Especial del Secretario General para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas, A/HRC/17/31 (2011), párr. 71.
[56] Comité de los Derechos del Niño de las Naciones Unidas, *Report of the 2014 Day of General Discussion*, párr. 96.
[57] Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, A/HRC/32/38 (2016), párr. 71.

cabida a las cuestiones relativas a los derechos del niño y las empresas". Es especialmente importante que todo mecanismo de denuncia esté adaptado a los menores, garantice la privacidad y la protección de las víctimas y permita supervisar, realizar un seguimiento y verificar las actividades destinadas a los niños víctimas.

Por ejemplo, los casos de ciberacoso constituyen una esfera en la que las instituciones nacionales de derechos humanos u otros organismos reguladores podrían proporcionar medidas de reparación efectivas a los niños. En esos casos, los mecanismos internos de reparación y reclamación resultan a veces inefectivos porque, aunque el contenido en cuestión cause angustia y daños, no suele estar previsto en la legislación nacional y no existe una base clara para solicitar su supresión a quien lo aloja. El otorgamiento de facultades a una autoridad pública para que reciba denuncias relativas a casos de ciberacoso e intermedie con quienes alojan el material correspondiente para lograr su supresión ofrecería importantes garantías a los niños[58]. Esto tendría la ventaja de ofrecer una respuesta rápida, cuya importancia es capital en el caso del ciberacoso, así como una base jurídica clara para abordar la supresión del material a que se refiere a dicho acto.

Al preparar su enfoque sobre la reglamentación del entorno digital, los gobiernos también han de tener en cuenta la repercusión de dicha reglamentación en el disfrute de todos los derechos humanos, en particular la libertad de expresión[59].

Los gobiernos deben obligar a las empresas a que procedan con la diligencia debida en lo que respecta a los derechos del niño. Esto garantizaría que las empresas identificasen, previniesen y mitigasen el impacto de sus operaciones en los derechos del niño, por ejemplo, en sus relaciones comerciales y en las operaciones mundiales[60].

Además, los gobiernos deberían estudiar la posibilidad de adoptar medidas complementarias, por ejemplo, garantizar que las entidades del sector privado cuyas actividades puedan repercutir en los derechos del niño en el entorno digital cumplan las normas más estrictas en materia de prevención y respuesta a posibles violaciones de derechos para poder obtener financiación o suscribir contratos.

4.2 Recomendaciones relativas a la aplicación

Los gobiernos deben garantizar que los niños cuyos derechos se han vulnerado puedan acceder a medidas de reparación efectivas y, en particular, reciban ayuda para obtener una reparación rápida y apropiada del daño sufrido mediante una indemnización, cuando proceda. Asimismo, los gobiernos deben brindar apoyo y asistencia adecuados a los niños que han sufrido violaciones relacionadas con los medios digitales y las TIC, entre otras cosas prestando servicios integrales para garantizar la plena recuperación y reintegración del niño y evitar que se vuelvan a cometer dichas violaciones en su contra[61].

En la ley se deben establecer mecanismos de asesoramiento, notificación y presentación de denuncias seguros, adaptados a los niños y de fácil acceso, como las líneas de ayuda, y dichos

[58] Bertrand de Crombrugghe, Informe del Consejo de Derechos Humanos sobre su trigésimo primer periodo de sesiones (Consejo de Derechos Humanos de las Naciones Unidas, 2016).
[59] Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, A/HRC/32/38 (2016), párr. 45.
[60] Comité de los Derechos del Niño de las Naciones Unidas, *Observación general núm. 16*, párr. 62.
[61] Comité de los Derechos del Niño de las Naciones Unidas, *Report of the 2014 Day of General Discussion*, párr. 106.

mecanismos deben formar parte del sistema nacional de protección del menor. Es importante velar por que estos servicios estén vinculados con los servicios reglamentarios a fin de agilizar las interacciones entre el menor y los organismos institucionales en un momento en que puede estar atravesando un periodo de sufrimiento. Las líneas de ayuda son especialmente útiles en los casos sumamente delicados, como los de abuso sexual, que a los niños les puede costar abordar con sus compañeros, padres, cuidadores o profesores. Las líneas de ayuda también desempeñan una función capital para dirigir a los niños hacia servicios como los de asesoría jurídica, los albergues, los organismos encargados de hacer cumplir la ley o los centros de rehabilitación[62].

Asimismo, los gobiernos deben entender y realizar un seguimiento de la conducta de los agresores a fin de mejorar los índices de detección de estos y reducir el riesgo de reincidencia de los que hayan sido condenados. Se podrían establecer líneas de ayuda que ofrezcan asesoramiento y apoyo gratuito y anónimo por teléfono o chat a quienes tengan sentimientos o pensamientos sexuales en relación con menores (posibles agresores). La ayuda que se preste a los agresores para cambiar su conducta reduce al mínimo el riesgo de reincidencia.

Los mecanismos de tramitación de denuncias establecidos por la ley también constituyen un elemento fundamental del marco para lograr medidas de reparación eficaces.

Los organismos reguladores deben llevar a cabo mediciones y estudios independientes a fin de evaluar la manera en que las plataformas comunican y tratan los problemas relativos a la protección de menores. Hay tecnologías que permiten a estos organismos supervisar las plataformas de manera independiente. Se debe dar apoyo a los proveedores privados para que publiquen informes de transparencia.

Junto con la comunidad internacional y el sector privado, los gobiernos deben desarrollar un conjunto universal de parámetros que las partes interesadas puedan utilizar para medir todos los aspectos pertinentes de la seguridad de la infancia en línea.

4.2.1 Explotación sexual

Los encargados de formular políticas han de tener en cuenta determinados aspectos al examinar las amenazas de daño a que se exponen los niños, en especial el material de abuso sexual infantil, el contenido autogenerado, la seducción y el chantaje sexual, así como otros riesgos en línea. Entre otras cosas podrían:

- Tomar medidas para interrumpir y reducir el tráfico de materiales de tipo MASI, por ejemplo, mediante el establecimiento de una línea de ayuda nacional o un portal de notificaciones a la IWF, y la implementación de soluciones para bloquear el acceso al contenido en línea respecto del que se sabe que contiene o publicita la disponibilidad de materiales de tipo MASI.
- Velar por que haya procesos nacionales para garantizar que todos los materiales de tipo MASI encontrados en un país se transmitan a un sistema nacional centralizado dotado de facultades legislativas para ordenar a las empresas a retirar dichos contenidos.
- Elaborar estrategias para combatir la demanda de materiales de tipo MASI, en particular entre quienes han sido condenados por ese tipo de delito. Es importante hacer tomar conciencia de que no se trata de un delito sin víctimas: se abusa de menores para producir el material visualizado, y al mirar o descargar material de tipo MASI de forma deliberada

[62] Representante Especial del Secretario General sobre la Violencia contra los Niños, *Releasing children's potential and minimizing risks*, págs. 51 y 65.

se contribuye directamente al abuso del menor en cuestión y se alienta el abuso de otros niños para generar más imágenes.

- Promover la conciencia de que los niños nunca pueden consentir ser objeto de abuso sexual, ya sea para la producción de materiales de tipo MASI, o para cualquier otro fin. Alentar a las personas que utilizan materiales de tipo MASI a buscar ayuda e informarles de que serán penalmente responsables de la actividad ilícita en la que participan o han participado.
- Elaborar otras estrategias para hacer frente a la demanda de materiales de tipo MASI. Por ejemplo, algunos países mantienen un registro de delincuentes sexuales condenados. Los tribunales han emitido órdenes judiciales a tenor de las cuales se prohíbe a esos delincuentes utilizar Internet, ya sea completamente o solo respecto de las partes que los niños o jóvenes utilizan frecuentemente. Hasta la fecha, el problema con estas órdenes ha sido su inobservancia. Sin embargo, en algunos países se está considerando la posibilidad de integrar la lista de delincuentes sexuales conocidos en una lista general de bloqueo que impedirá a los que figuren en ella consultar ciertos sitios web o formar parte de sus miembros, por ejemplo, los sitios a los que se sabe que recurren grandes cantidades de niños y jóvenes. Por supuesto, si el delincuente acude a un sitio web utilizando otro nombre o un inicio de sesión falso, estas medidas perderán en gran medida su eficacia, pero la penalización de esta conducta puede representar otro factor disuasivo.
- Proporcionar a las víctimas un apoyo adecuado a largo plazo. Cuando los niños o jóvenes son víctimas en línea como, por ejemplo, si ha aparecido una imagen ilícita de ellos en Internet, es natural que sientan gran preocupación por la posible visualización de dicha imagen y las repercusiones que tendrá en sus vidas. Esto podría dejar en los niños o jóvenes un sentimiento de vulnerabilidad a los actos de intimidación o a nuevos actos de abuso y explotación sexual. En ese contexto, es importante disponer de servicios de apoyo profesionales que ayuden a los niños y jóvenes que se encuentren en tales circunstancias. Podría ser necesario prestar este tipo de apoyo a largo plazo.
- Velar por que se establezca y promueva ampliamente un mecanismo destinado a ofrecer un medio rápido y fácilmente comprensible para notificar contenidos ilícitos o conductas en línea ilegales o preocupantes, por ejemplo, un sistema similar al establecido por el Grupo de Trabajo Global Virtual y la INHOPE. Se debería alentar la utilización del sistema i24/7 de INTERPOL.
- Velar por que se imparta una formación adecuada en materia de investigación en Internet y delincuencia informática a un número suficiente de funcionarios encargados de hacer cumplir la ley y por que estos tengan acceso a instalaciones forenses apropiadas que les permitan extraer e interpretar datos digitales pertinentes.
- Invertir en la formación de quienes conforman las autoridades judiciales, fiscales y las encargadas de hacer cumplir la ley, sobre los métodos utilizados por los delincuentes en línea para cometer dichos delitos. También será preciso destinar inversiones a la adquisición y mantenimiento de los medios necesarios para obtener e interpretar pruebas forenses procedentes de dispositivos digitales. Además, será importante establecer una colaboración bilateral y multilateral e intercambiar información con las correspondientes autoridades encargadas de hacer cumplir la ley y los organismos de investigación de otros países.

4.2.2 Educación

La educación de los niños en materia de alfabetización digital forma parte de una estrategia destinada a garantizar que puedan beneficiarse de la tecnología, sin sufrir ningún daño. Esto permitirá que los niños desarrollen su capacidad de pensamiento crítico, lo cual les ayudará a identificar y entender los aspectos positivos y negativos de su conducta en el espacio digital. Si bien es importante enseñar a los niños los daños que se pueden producir en línea, esta labor solo será eficaz si se integra en un programa de alfabetización digital más amplio que deberá adaptarse a la edad de los destinatarios y centrarse en sus habilidades y competencias. Es importante que la educación en materia de seguridad en línea abarque conceptos sobre el

aprendizaje social y emocional, ya que estos ayudarán a los alumnos a entender y gestionar sus emociones para tener relaciones sanas y respetuosas, tanto en línea como fuera de línea.

Los niños deben disponer de herramientas y conocimientos apropiados para abordar Internet, ya que esta es una de las mejores maneras de garantizar su seguridad. La incorporación de la alfabetización digital en los programas escolares es una vía para lograr dicho objetivo. Otra consiste en crear recursos pedagógicos fuera del programa escolar.

Quienes trabajan con niños deben tener conocimientos y aptitudes adecuadas a fin de ayudarlos con confianza a responder y resolver las cuestiones relativas a la protección de la infancia en línea, y a desarrollar en ellos las habilidades digitales necesarias para que se beneficien de la tecnología de manera satisfactoria.

4.2.3 Sector privado

Los actores del sector privado en los planos nacional e internacional deben llevar a cabo una labor de sensibilización sobre las cuestiones relativas a la seguridad de la infancia en línea y ayudar a todos los adultos responsables del bienestar de los niños (entre otros, los padres y cuidadores, las escuelas y las organizaciones y comunidades de ayuda a la juventud) a desarrollar los conocimientos y las habilidades que necesitan para mantener la seguridad de los menores. El sector privado debe adoptar el enfoque de la seguridad desde el diseño en relación con sus productos, servicios y plataformas, y reconocer al mismo tiempo la seguridad entre sus principales objetivos. A tales efectos, debería llevar a cabo las siguientes medidas:

- Proporcionar herramientas aptas para las familias y adaptadas a la edad a fin de ayudar a sus usuarios a gestionar mejor la protección de sus familias en línea.
- Ofrecer mecanismos de notificación adecuados para que sus usuarios notifiquen sus problemas y preocupaciones. Cabría esperar que los usuarios recibiesen respuestas oportunas a dichas notificaciones, con información sobre las medidas adoptadas y, en su caso, orientación sobre la manera en que pueden recibir ayuda adicional.
- Informar también de manera proactiva sobre los abusos contra niños a fin de detectar y combatir todo tipo de abuso (tipificado como actividad delictiva) contra menores. Esta práctica ha demostrado que si todas las partes interesadas contribuyen a la detección, bloqueo y notificación de abusos, sería posible imaginar una Internet más limpia y segura para todos. El sector privado debería considerar la posibilidad de servirse de todos los instrumentos pertinentes para prevenir la explotación de sus plataformas, por ejemplo, los servicios de la IWF.

Es fundamental que todos los actores pertinentes del ecosistema participen y sean conscientes de los riesgos y daños en línea a fin de evitar que los niños se expongan a riesgos innecesarios.

Asimismo, se deben elaborar parámetros comunes para la seguridad infantil en línea a fin de medir todos los aspectos pertinentes en la materia. El establecimiento de normas y parámetros comunes es la única vía que permite realizar un seguimiento de los avances logrados en los países y determinar el éxito de los proyectos y actividades que se han llevado a cabo para eliminar todo tipo de violencia contra menores y confirmar la solidez del ecosistema de la seguridad de la infancia en línea.

5 Elaboración de una estrategia nacional de protección de la infancia en línea

5.1 Actividades que se han de llevar a cabo a nivel nacional

Con miras a elaborar una estrategia nacional centrada en la seguridad de los menores en línea, es preciso que los encargados de formular políticas consideren toda una serie de estrategias. En el Cuadro 1 se establecen los ámbitos esenciales que se han de tener en cuenta.

Cuadro 1: Ámbitos esenciales que se han de tener en cuenta

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Marco jurídico	1	Analizar el marco jurídico en vigor a fin de determinar que se otorgan todas las facultades jurídicas necesarias para que los encargados de hacer cumplir la ley y otros organismos pertinentes protejan a los menores de 18 años en línea en todas las plataformas de Internet.	En general será necesario que exista un conjunto de leyes en que se establezca claramente que todos y cada uno de los delitos que se pueden cometer contra un niño en el mundo real también se pueden cometer, *mutatis mutandis*, por Internet o cualquier otra red electrónica. Asimismo, podría ser necesario elaborar nuevas leyes o adaptar las existentes para proscribir ciertos tipos de conductas que solo pueden tener lugar por Internet, como por ejemplo, incitar a distancia a niños para que realicen u observen actos sexuales, o seducir a niños para reunirse con ellos en el mundo real con fines sexuales. Además de los fines antes anunciados, en general también será necesario contar con un marco jurídico en el que se proscriba la utilización indebida de ordenadores con fines delictivos, así como la piratería u otras modalidades de utilización maliciosas o no consensuadas de códigos informáticos, y se dictamine que Internet es un lugar en el que se pueden cometer delitos.
	2	Determinar, *mutatis mutandis*, que todo acto contra un niño que sea ilegal en el mundo real también lo es en línea y confirmar también la adecuación de las normas en materia de protección y privacidad de datos en línea relativas a los niños.	

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Marco reglamentario	3	Considerar la posibilidad de elaborar una política reglamentaria. Esta labor puede consistir en desarrollar políticas de autorregulación o corregulación, así como un marco reglamentario completo. El modelo de autorregulación o corregulación podría incluir la formulación y publicación de códigos de buenas prácticas o expectativas básicas en materia de seguridad en línea, tanto en relación con la ayuda encaminada a propiciar, coordinar u orquestar y mantener la participación de todos los interesados pertinentes, como en lo relativo a la aceleración del ritmo en que se pueden formular y llevar a la práctica respuestas apropiadas a los cambios tecnológicos. Un modelo reglamentario podría definir las expectativas y obligaciones respectivas de las partes interesadas e incorporarse en un contexto jurídico. También se podría contemplar la posibilidad de establecer sanciones por el incumplimiento de tales políticas.	Algunos países han establecido un modelo de autorregulación o corregulación en relación con la elaboración de políticas en esta esfera, y con base en esos modelos han publicado, por ejemplo, códigos de buenas prácticas para orientar al sector de Internet sobre las medidas que podrían dar mejor resultado para mantener la seguridad de los niños y jóvenes en línea. Por ejemplo, en la Unión Europea se han publicado códigos aplicables a nivel comunitario tanto a los sitios de redes sociales como a las redes de telefonía móvil en relación con el suministro de contenidos y servicios a niños y jóvenes a través de sus redes. La autorregulación y la corregulación pueden resultar más eficaces para acelerar el ritmo en que se formulan y llevan a la práctica medidas de respuesta apropiadas para los cambios tecnológicos. Más recientemente, varios países han elaborado y/o instaurado un marco reglamentario. En estos ejemplos, el marco reglamentario surgió a raíz de modelos de autorregulación o corregulación y en él se definen las obligaciones de las partes interesadas, en particular los proveedores del sector, y lo que se espera de ellos, para mejorar la protección de sus usuarios.

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Notificaciones – contenido ilícito	4	Garantizar que se dispone y promueve ampliamente la utilización de un mecanismo a fin de ofrecer un medio fácilmente comprensible para notificar los diversos contenidos ilícitos encontrados en Internet, por ejemplo, una línea de ayuda nacional que pueda responder inmediatamente y lograr que se supriman el material ilícito o que no se pueda acceder a él. El sector privado debe disponer de mecanismos para identificar, bloquear y eliminar el abuso de menores en línea, sirviéndose de todos los servicios pertinentes de sus organizaciones.	Se deberían publicitar y promover de manera generalizada, tanto en Internet como en otros medios de comunicación, mecanismos concebidos para notificar abusos de un servicio en línea o denunciar un comportamiento censurable o ilícito en línea, por ejemplo, a través de una línea de ayuda nacional. Si no se dispone de ninguna línea de ayuda nacional, la IWF ofrece la solución de utilizar los Portales de notificaciones. Se deberían exponer de manera destacada enlaces hacia mecanismos de notificación de abusos en las partes correspondientes de cualquier sitio web que autorice la aparición de contenidos generados por el usuario. Asimismo, debería ser posible que las personas que de algún modo se sientan amenazadas o hayan sido testigos de actividades preocupantes en Internet, puedan informar a la mayor brevedad posible a los correspondientes organismos encargados de hacer cumplir la ley, que a su vez deberán estar capacitados y en condiciones de responder a tales actos. El Grupo de Trabajo Global Virtual es un organismo responsable de la observancia de la ley que ofrece un mecanismo que funciona las 24 horas los 7 días de la semana para recibir notificaciones de contenidos o comportamientos ilícitos emitidas por personas situadas en los Estados Unidos de América, Canadá, Australia e Italia, a los que se espera que se sumen próximamente otros países. Véase www.virtualglobaltaskforce.com. Véase también la INHOPE.

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Notificaciones – preocupaciones de los usuarios	5	El sector privado debería brindar a los usuarios la oportunidad de comunicar sus preocupaciones y problemas y responder en consecuencia.	Se debería obligar a los proveedores a ofrecer e indicar claramente a sus usuarios la posibilidad de notificar los problemas y preocupaciones que tengan en relación con sus servicios. Esta posibilidad debería ofrecerse de manera inmediata y adaptada a los niños.
Actores y partes interesadas	6	Hacer que participen todas las correspondientes partes interesadas en la protección de la infancia en línea, y en particular: • los organismos gubernamentales; • los organismos responsables de hacer cumplir la ley; • las organizaciones de servicios sociales; • los proveedores de servicios Internet (PSI) y otros proveedores de servicios electrónicos (PSE); • los proveedores de redes de telefonía móvil; • los proveedores de Wi-Fi públicos; • otras empresas pertinentes de alta tecnología; • las organizaciones de profesores; • las organizaciones de padres; • los niños y jóvenes; • las organizaciones dedicadas a la protección de la infancia y otras ONG pertinentes; • las instituciones académicas y la comunidad científica; • los propietarios de cibercafés y otros proveedores de acceso público, por ejemplo, las bibliotecas, los telecentros, los PC Bangs[63] y los centros de juegos en línea, etc.	Varios gobiernos nacionales han considerado útil reunir a todos los principales interesados y actores para centrarse en el desarrollo e implementación de una iniciativa nacional destinada a transformar a Internet en un lugar más seguro para niños y jóvenes, y en la sensibilización sobre los problemas que esta entraña y el modo de hacer a ellos de una manera muy práctica. En el marco de esta estrategia, será importante reconocer el gran número de personas que se conectan constantemente y desde cualquier parte del mundo a Internet por varios tipos de dispositivos diferentes. Es necesario que en ella participen los operadores de banda ancha, telefonía móvil y Wi-Fi. Además, en numerosos países la red de bibliotecas públicas, telecentros y cibercafés pueden ser importantes fuentes de acceso a Internet, en particular para niños y jóvenes.

[63] *PC Bang* es un término que se utiliza normalmente en la República de Corea y otros países para describir una gran sala en que se ofrecen prestaciones LAN para juegos en gran escala, ya sea en línea o entre los jugadores de la sala.

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Investigación	7	Realizar investigaciones relativas a los diversos actores y colectivos interesados de ámbito nacional para conocer sus opiniones, experiencias, preocupaciones y oportunidades en relación con la protección de la infancia en línea. En este proceso también se debe valorar el grado de toda responsabilidad junto con las actividades actuales y previstas para la protección de la infancia en línea.	

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Educación en materia de alfabetización y competencias digitales	8	El desarrollo de la alfabetización digital forma parte de cualquier programa escolar nacional que sea apropiado para la edad y aplicable a todos los niños.	Las escuelas y el sistema educativo constituirán por lo general la base de la educación y la alfabetización digital de una estrategia nacional de protección de la infancia en línea. Todo programa escolar nacional debe incluir aspectos relativos a la protección de los niños en línea y tener por objeto proporcionar a los niños de todas las edades las habilidades apropiadas tanto para aprovechar y utilizar con éxito la tecnología como para concienciarse de las amenazas y peligros que entraña para poder evitarlos. En él se deben reconocer y recompensar las conductas positivas y constructivas. En toda campaña de concienciación y educación será importante lograr el equilibrio adecuado. A la vez que deben evitarse los mensajes basados en el miedo, hay que dar la debida importancia a los numerosos aspectos positivos y recreativos de las nuevas tecnologías. Internet encierra enormes posibilidades como un medio de capacitación de niños y jóvenes para que estos descubran nuevos mundos. Un objetivo capital de los programas de educación y concienciación debe ser enseñar formas positivas y responsables de comportamiento en línea. Quienes trabajan con niños, especialmente los profesores, deben recibir la formación y los equipos adecuados para educar y proporcionar a los niños estas habilidades de manera satisfactoria. Deben entender las amenazas y peligros en línea y ser capaces de reconocer con certeza los indicios de abusos y daños y reaccionar ante estas preocupaciones, así como notificarlas, a fin de proteger a los niños.

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Recursos educativos	9	Aprovechar los conocimientos y la experiencia de todos los interesados y elaborar materiales y mensajes sobre la seguridad en Internet que reflejen las leyes y normas culturales locales, y velar por que se distribuyan con eficacia y se presenten adecuadamente a todos los destinatarios clave. Considerar la posibilidad de obtener la ayuda de los medios de comunicación masivos para promover los mensajes de sensibilización. Elaborar materiales que hagan hincapié en los aspectos positivos y capacitantes de Internet para los niños y los jóvenes y evitar los mensajes basados en el miedo. Promover formas positivas y responsables de comportamiento en línea. Considerar la posibilidad de elaborar recursos para ayudar a los padres a evaluar la seguridad en línea de sus propios hijos y a aprender cómo reducir al mínimo los riesgos y aprovechar al máximo el potencial para su propia familia a través de iniciativas educativas concretas.	Al producir materiales didácticos, es importante tener en cuenta que muchas personas que no conocen la tecnología no se sentirán muy cómodas al utilizarla. Por ello, es importante velar por que se pongan a disposición materiales en materia de seguridad, ya sea en la forma escrita o utilizando otros medios con los que los novatos se sientan más familiarizados, como por ejemplo el vídeo. Muchas de las principales empresas de Internet crean sitios web que contienen gran cantidad de información sobre cuestiones en línea para niños y jóvenes. Sin embargo, muy a menudo estos materiales sólo están disponibles en inglés o en un número muy reducido de idiomas. Por lo tanto, es importante que se produzcan materiales a escala local en los que se reflejen las leyes locales así como las normas culturales locales. Este aspecto será esencial para cualquier campaña sobre la seguridad en Internet o cualesquiera materiales de capacitación que se elaboren.
Protección de la infancia	10	Velar por que existan mecanismos de protección infantil universales y sistemáticos que obliguen a todas las personas que trabajan con menores (en el ámbito social, sanitario, escolar, etc.) a identificar, tratar y denunciar los incidentes de abuso y daño que se producen en línea.	Debe haber un sistema de protección infantil universal aplicable a todos los que trabajan con menores, que les obligue a denunciar los casos de abuso o daño de menores para que se puedan investigar y resolver las correspondientes situaciones.

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Sensibilización nacional	11	Organizar campañas nacionales de sensibilización para propiciar que se pongan de relieve a escala universal las cuestiones relativas a la protección de la infancia en línea. Para preparar dichas campañas, puede resultar beneficioso aprovechar las que se celebran a nivel mundial como el Día de la Internet Segura.	Los padres, tutores y profesionales como los profesores deben desempeñar un papel cardinal a la hora de ayudar a mantener la seguridad de los niños y jóvenes en línea. Se deberían elaborar programas de apoyo que ayuden a tomar conciencia de las cuestiones en juego y a formular estrategias para hacer frente a ellas. Asimismo, se debería considerar la posibilidad de obtener la ayuda de los medios de comunicación masivos para la promoción de mensajes y campañas de sensibilización. Algunos eventos como el Día de la Internet Segura serán útiles para estimular y alentar el diálogo nacional sobre la protección de la infancia en línea. Muchos países han creado con éxito campañas de sensibilización nacionales en torno a este día y han conseguido que todos los diversos actores y partes interesadas participen en la difusión de mensajes universales a través de los medios sociales y de comunicación.

	#	Ámbitos esenciales que se han de tener en cuenta	Información adicional
Herramientas, servicios y ajustes	12	Tomar en consideración la importancia de los ajustes de los dispositivos, las herramientas técnicas (como los programas de filtrado) y las aplicaciones y los ajustes de protección de la infancia que pueden ser de utilidad. Alentar a los usuarios a que sean responsables con sus dispositivos, fomentando la realización de actualizaciones de los sistemas operativos y la utilización de aplicaciones y programas informáticos de seguridad adecuados.	Hay varios servicios disponibles que pueden ayudar a excluir materiales no deseados o bloquear contactos no deseados. Algunos de estos programas de seguridad infantil y filtrado pueden ser básicamente gratuitos, puesto que forman parte del sistema operativo del ordenador o se proporcionan como parte de un conjunto de servicios prestados por un PSI o PSE. Los fabricantes de algunas consolas de juegos también proporcionan instrumentos similares si el dispositivo funciona con Internet. Estos programas no ofrecen una garantía a toda prueba, pero pueden proporcionar un valioso apoyo, sobre todo a familias con niños pequeños. La mayoría de los dispositivos vienen con ajustes que ayudan a proteger a los niños y también fomentar su utilización sana y equilibrada. Esto se aplica también a los mecanismos que permiten a los padres administrar los dispositivos de sus hijos, asignándoles el tiempo de uso, las aplicaciones y los servicios que pueden utilizar, así como gestionar sus compras. Más recientemente se han elaborado informes y ajustes que permiten a los usuarios y los padres entender y administrar mejor el tiempo de pantalla y el acceso a los dispositivos. Estas herramientas técnicas se deberían utilizar como parte de un arsenal más amplio. Es indispensable la participación de los padres y/o tutores. A medida que los niños comienzan a crecer un poco aspiran a una mayor privacidad y también sienten un deseo más fuerte de comenzar a explorar por sus propios medios. Además, cuando existe una relación de facturación entre el vendedor y el cliente, los procedimientos de verificación de la edad pueden desempeñar un papel muy útil para ayudar a los

5.2 Ejemplos de preguntas

Una vez que se han identificado los interesados y actores en el plano nacional, se les pueden enviar las siguientes preguntas e invitarlos a remitir sus correspondientes respuestas. Estas respuestas ayudarán a determinar qué cubren las políticas, los puntos fuertes y las esferas prioritarias de la lista de actividades que se han de llevar a cabo a nivel nacional.

- ¿Cuál es su grado de responsabilidad respecto de la seguridad en línea y los derechos del niño?
- ¿De qué manera están integrados estos aspectos en sus políticas y procesos en vigor?
- ¿Hasta qué punto cubre la legislación en vigor la seguridad en línea?
- ¿Cuáles son sus prioridades en materia de seguridad en línea?
- ¿Qué actividades realiza para apoyar la seguridad en línea?
- ¿De qué manera colabora con otros organismos y organizaciones para lograr mejoras o avances en la esfera de la seguridad en línea?
- ¿Tienen los niños/padres la posibilidad de notificarle preocupaciones o problemas de seguridad en línea?
- ¿Cuáles son sus tres desafíos principales en el mundo en línea?
- ¿Cuáles son sus tres oportunidades principales en el mundo en línea?

También sería útil realizar una investigación y entender la percepción y las experiencias de los niños y sus padres respecto de la protección infantil en línea.

6 Material de referencia

La seguridad de la infancia en línea: Principales documentos y publicaciones

2020

- ECPAT International, *Sexual Exploitation Of Children In The Middle East And North Africa*, 2020
- DQ Institute, 2020 Child Online Safety Report, 2020
- EU Kids Online, *EU Kids Online 2020: Survey results from 19 countries*, 2020

2019

- Internet Watch Foundation (IWF), *Annual Report*, 2019
- Alianza Mundial WeProtect, *Global Threat Assessment*, 2019
- Comisión de la Banda Ancha para el Desarrollo Sostenible de la UIT y la UNESCO, *Child Online Universal Declaration*, 2019
- Comisión de la Banda Ancha para el Desarrollo Sostenible de la UIT y la UNESCO, *Child Safety Online: Minimizing the Risk of Violence, Abuse and Exploitation Online*, 2019
- Global Kids Online, *Growing up in a connected world*, 2019
- *Rethinking the Detection of Child Sexual Abuse Imagery on the Internet*, en *Proceedings of the 2019 World Wide Web Conference,* 13 a 17 de mayo de 2019, San Francisco (Estados Unidos de América), 2019
- Ministerio del Interior del Reino Unido, *Online Harms White Paper* (solo en el Reino Unido), 2019
- PA Consulting, *A tangled web: rethinking the approach to online CSEA*, 2019
- Oficina del Comisionado de Información del Reino Unido, *Consultation on Code of Practice to help protect children online* (solo en el Reino Unido), 2019
- Global Fund to End Violence against Children, *Disrupting Harm: evidence to understand online child sexual exploitation and abuse*, 2019
- Global Partnership to End Violence against Children, *Safe to Learn,* Un Llamado a la Acción, Manifiesto de la Juventud, 2019
- UNESCO, *Behind the numbers: Ending school violence and bullying*, 2019 (incluye datos sobre las conductas perniciosas en línea y el ciberacoso)
- Oficina del Alto Comisionado para los Derechos Humanos, *Los derechos del niño en relación con el entorno digital*, 2019
- Comisionado de Ciberseguridad de Australia, *Safety by Design Overview*, 2019
- UNICEF, *Why businesses should invest in digital child safety*, 2019
- Departamento de Estado de los Estados Unidos, *Trafficking in Persons report*, 2019

2018

- Alianza Mundial WeProtect, *Global Threat Assessment*, 2018
- *Child Dignity on the Digital World*, *Technical Working Group Report*, 2018, Consejo de Europa, Recomendación CM/Rec(2018)7 del Comité de Ministros a los Estados miembros sobre las Directrices para respetar, proteger y hacer efectivos los derechos del niño en el entorno digital, 2018
- Global Fund to End Violence against Children, *Two years of supporting solutions: results from the Fund's investments*, 2018
- Alianza Mundial WeProtect, *Working examples of Model of National Response capabilities and implementation*, 2018
- INTERPOL y ECPAT International, *Hacia un indicador mundial de las víctimas no identificadas en material de explotación sexual de niñas, niños y adolescentes*, 2018

- EUROPOL, *Internet Organized Crime Threat Assessment* (IOCTA), 2018
- NetClean, *Report about Child Sexual Abuse Cybercrime*, 2018
- Centro Internacional para Niños Desaparecidos y Explotados (ICMEC), *Material sobre abuso sexual infantil: Legislación modelo y revisión global*, novena edición, 2018
- Centro Internacional para Niños Desaparecidos y Explotados (ICMEC), *Studies in Child Protection: Sexual Extortion and Non-Consensual Pornography*, 2018
- International Association of Internet Hotlines, *INHOPE Report*, 2018
- Internet Watch Foundation (IWF), *Annual Report*, 2018
- Thorn, Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims, 2018
- UIT, *Global Cybersecurity Index*, 2018
- Centre of Expertise on child sexual abuse (CSA), Interventions for perpetrators of online child sexual exploitation – a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of Online-facilitated CSEA – a rapid evidence assessment, 2018
- UNICEF, *Policy guide on children and digital connectivity*, 2018

2017

- The National Center for Missing & Exploited Children (NCMEC), *The online enticement of children: an in-depth analysis of CyberTipline Reports*, 2017
- 5Rights Foundation, *Digital Childhood, Addressing Childhood Development Milestones in the Digital Environment,* 2017
- Childnet*, DeShame Report*, 2017
- Canadian Centre for Child Protection, *Survivors' survey*, 2017
- Internet Watch Foundation (IWF), *Annual Report*, 2017
- Centro Internacional para Niños Desaparecidos y Explotados (ICMEC), *Annual Report*
- Centro Internacional para Niños Desaparecidos y Explotados (ICMEC), Grooming por Internet de niños, niñas, y adolescentes con fines sexuales: Legislación modelo y revisión global, 2017
- Thorn, *Sextortion online survey with 2,097 victims of sextortion ages 13 to 25*, 2017
- UNICEF, *Niños en un mundo digital*, 2017
- Western Sydney University, *Young and Online: Children's Perspectives on Life in Digital Age,* 2017
- ECPAT International, *Sexual Exploitation of Children in South East Asia*, 2017

2016

- UNICEF, *Perils and possibilities: growing up online,* 2016
- UNICEF, *Child protection in the digital age: National responses to online CSEA in ASEAN*, 2016
- Centre for Justice and Crime Prevention, *Child Online Protection in the MENA Region*, 2016
- ECPAT International, Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes, *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales* (Orientaciones de Luxemburgo), 2016

2015

- Alianza Mundial WeProtect, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*, 2015
- National Center for Missing and Exploited Children (NCMEC), *A Global Landscape of Hotlines Combating CSAM,* 2015
- UIT y UNICEF, Directrices de protección de la infancia en línea para la Industria, 2015

Documentos relacionados con los derechos humanos en un mundo digital

- Consejo de Europa, *Directrices para respetar, proteger y hacer efectivos los derechos del niño en el entorno digital*, 2018
- UNESCO, *Indicadores universales de Internet*, 2019
- Ranking Digital Rights (RDR), *Índice de responsabilidad corporativa 2019*, 2019
- Comisión de la Banda Ancha para el Desarrollo Sostenible, *The State of the Broadband*, 2019
- UIT, *Measuring Digital Development*, 2019
- UIT, *Measuring Information Society Report*, 2018
- UNICEF, Children and Digital Marketing – Industry Toolkit, 2018
- Comisión de la Banda Ancha para el Desarrollo Sostenible, *Digital health,* 2017
- Comisión de la Banda Ancha para el Desarrollo Sostenible*, Digital Skills for life and work*, 2017
- Comisión de la Banda Ancha para el Desarrollo Sostenible, *Digital gender divide,* 2017
- UNICEF, Privacy, protection of personal information and reputation, 2017
- UNICEF, Freedom of expression, association, access to information and participation, 2017
- UNICEF, Access to the Internet and digital literacy, 2017
- Convención de las Naciones Unidas sobre los Derechos del Niño, *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*, 2019

Si desea consultar otros recursos, remítase a la lista de recursos adicionales que figura en **www.itu-cop-guidelines.com**.

Anexo 1: Terminología

Las definiciones que figuran a continuación se basan principalmente en la terminología existente, elaborada en el marco de la Convención sobre los Derechos del Niño, de 1989, así como por el Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes, en sus Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, de 2016[64] (Orientaciones de Luxemburgo), por el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, de 2012[65], así como por el Informe de Global Kids Online, de 2019[66].

Adolescente

Es adolescente toda persona de entre 10 y 19 años de edad. Es importante señalar que, con arreglo al derecho internacional, el término adolescente no es vinculante y que las personas menores de 18 años de edad se consideran niños, mientras que las de 19 años de edad son adultos salvo que, en virtud de la ley que les sea aplicable, hayan alcanzado antes la mayoría de edad[67].

Inteligencia artificial (IA)

En el sentido más amplio, el término se refiere indistintamente a los sistemas que son pura ciencia ficción (los llamados IA "fuertes" que son autoconscientes) y a los sistemas que ya están en funcionamiento y son capaces de realizar tareas muy complejas (reconocimiento facial o de voz, conducción de vehículos – estos sistemas se describen como IA "débiles" o "moderados")[68].

Sistemas de IA

Un sistema de IA es un sistema basado en una máquina que, para un determinado conjunto de objetivos definidos por el ser humano, puede hacer predicciones o recomendaciones y tomar decisiones que influyen en entornos reales o virtuales, y está diseñado para funcionar con diversos niveles de autonomía[69].

Interés superior del niño

Describe todos los factores necesarios para tomar una decisión en un caso específico para un niño en particular o un grupo de niños[70].

---

64 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales,* 2016, pág. 114, http://luxembourgguidelines.org/es/.

65 Consejo de Europa, *Protection of Children against Sexual Exploitation and Sexual Abuse* (Estrasburgo: Publicaciones del Consejo de Europa, 2012), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf.

66 Globalkidsonline.net, *Done Right, Internet Use Can Increase Learning and Skills,* noviembre de 2019, http://globalkidsonline.net/synthesis-report-2019/.

67 UNICEF y UIT (2015), *Directrices de protección de la infancia en línea para la Industria* – itu.int/cop, 2015, https://www.itu.int/en/cop/Documents/COP%20Guidelines_Spanish.pdf.

68 Consejo de Europa, *What's AI?*, coe.int, inteligencia artificial, consultado el 16 de enero de 2020, https://www.coe.int/en/web/artificial-intelligence/what-is-ai.

69 OCDE, *Recommendation of the Council on Artificial Intelligence* (OCDE, 2019), https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari.

70 ACNUDH, *Convención sobre los Derechos del Niño*, consultado el 16 de enero de 2020, https://www.ohchr.org/SP/ProfessionalInterest/Pages/CRC.aspx.

Niño, niña y adolescente

De acuerdo con el Artículo 1 de la Convención sobre los Derechos del Niño, "niño" es todo ser humano menor de 18 años de edad salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad[71].

Explotación y abuso sexual infantil (EASI)

Describe todas las formas de explotación y abuso sexuales (Convención sobre los Derechos del Niño, 1989, Art. 34), por ejemplo "a) la incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal; b) la explotación del niño en la prostitución u otras prácticas sexuales ilegales; c) la explotación del niño en espectáculos o materiales pornográficos" así como el "contacto sexual que normalmente implica el uso de la fuerza sobre una persona sin consentimiento". La explotación y abuso sexuales de niños sucede cada vez más por Internet, o guarda cierta relación con el entorno en línea[72].

Material de abuso (y explotación) sexual infantil (MASI)

La rápida evolución de las TIC ha creado nuevas formas de explotación y abuso sexual de niños en línea, que suceden virtualmente y no tienen por qué incluir el encuentro físico con el niño[73]. Si bien en muchas jurisdicciones todavía se clasifican las imágenes y vídeos de abuso sexual infantil como "pornografía infantil" o "imágenes indecentes de niños", en estas directrices englobamos ambos conceptos en el término material de abuso sexual infantil (en adelante, MASI). Esta definición está en consonancia con las Directrices de la Comisión de la Banda Ancha y el Modelo de Respuesta Nacional de la Alianza Mundial WePROTECT[74]. Este término describe con mayor precisión el contenido. La pornografía se refiere a una industria legítima y comercializada y, tal como establecen las Orientaciones de Luxemburgo, el uso del término:

"puede (de forma involuntaria o voluntaria) contribuir a disminuir la gravedad, normalizar, o incluso legitimar lo que en realidad es abuso sexual de niñas, niños y adolescentes […] el término 'pornografía infantil' corre el riesgo de insinuar que estos actos son llevados a cabo con el consentimiento de la niña, el niño o el adolescente y es material sexual legal"[75].

El término MASI se refiere al material que representa actos de explotación o abuso sexual de un niño. Comprende, entre otras cosas, grabaciones de abuso sexual de niños por adultos; imágenes de niños en actos sexuales explícitos; imágenes de órganos sexuales de niños producidas o utilizadas con fines principalmente sexuales.

Niños y jóvenes

---

71 ACNUDH; UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria.*

72 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.*

73 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales;* UNICEF, *Global Kids Online Comparative Report (2019).*

74 Alianza Mundial WeProtect, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response,* 2016, https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf; Comisión de la Banda Ancha, *Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online* (2019).

75 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.*

Toda persona menor de 18 años, siendo los niños, también llamados niños pequeños en estas directrices, los menores de 15 años y jóvenes los que tienen entre 15 y 18 años.

Juguetes conectados

Los juguetes conectados se conectan a Internet mediante tecnologías como Wi-Fi y Bluetooth, y suelen funcionar junto con aplicaciones que permiten el juego interactivo de los niños. Según Juniper Research, en 2015 el mercado de los juguetes conectados se cifró en 2 800 millones de dólares y se prevé que alcance los 11 000 millones de dólares en 2020. Estos juguetes recogen y almacenan información personal de los niños, como su nombre, geolocalización, direcciones, fotografías, grabaciones de audio y vídeo[76].

Ciberacoso, también denominado acoso en línea

La definición del ciberacoso no está recogida en el derecho internacional. A los efectos del presente documento, el ciberacoso describe una agresión deliberada y reiterada por una persona o grupo, utilizando la tecnología digital, contra una víctima que no puede defenderse fácilmente[77]. Suele consistir en "utilizar la tecnología digital e Internet para publicar información dañina sobre alguien, compartir deliberadamente información privada, fotografías o vídeos con fines lesivos, enviar amenazas o insultos (por correo electrónico, mensajería instantánea, chat, mensajes de texto), difundir rumores e información falsa sobre la víctima o excluirla a propósito de las comunicaciones en línea"[78]. Puede tratarse de comunicaciones directas (como el envío de mensajes por chat o de texto), semipúblicas (como la publicación de mensajes en una lista de correo electrónico) o públicas (como la creación de un sitio web dedicado a burlarse de la víctima).

Odio cibernético, discriminación y extremismo violento

"El odio cibernético, la discriminación y el extremismo violento son un tipo distinto de violencia cibernética, que se dirige contra una identidad colectiva, en lugar de individuos [...] a menudo por motivos de raza, orientación sexual, religión, nacionalidad o situación migratoria, sexo/género y política"[79].

Civismo digital

Por civismo digital se entiende la capacidad de participar de manera positiva, crítica y competente en el entorno digital, aprovechando las aptitudes de comunicación y creación efectivas, a fin de entablar la participación social respetando derechos humanos y la dignidad mediante el uso responsable de la tecnología[80].

---

76 Jeremy Greenberg, *Dangerous Games: Connected Toys, COPPA, and Bad Security*, Georgetown Law Technology Review, 4 de diciembre de 2017, https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/.

77 Anna Costanza Baldry, Anna Sorrentino, y David P. Farrington, *Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities,* Children and Youth Services Review 96 (enero de 2019): 302–7, https://doi.org/10.1016/j.childyouth.2018.11.058.

78 UNICEF, *Global Kids Online Comparative Report* (2019); *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.*

79 UNICEF, *Global Kids Online Comparative Report* (2019).

80 Consejo de Europa, *Digital Citizenship Education,* consultado el 16 de enero de 2020, https://www.coe.int/en/web/digital-citizenship-education/home.

Alfabetización digital

Por alfabetización digital se entiende disponer de las aptitudes necesarias para vivir, aprender y trabajar en una sociedad en la que la comunicación y el acceso a la información se realiza cada vez más a través de tecnologías digitales como las plataformas de Internet, los medios sociales y los dispositivos móviles[81]. Comprende la comunicación clara, conocimientos técnicos y pensamiento crítico.

Resiliencia digital

Este término se refiere a la capacidad del niño para afrontar emocionalmente los peligros a los que se expone en Internet. Incluye los recursos emocionales que el niño debe tener para comprender cuándo está en situación de riesgo en línea, saber qué hacer para buscar ayuda, aprender de la experiencia y recuperarse cuando las cosas salen mal[82].

Educadores

Un educador es una persona que trabaja sistemáticamente para mejorar los conocimientos de otra persona sobre un determinado tema. Comprende tanto a quienes enseñan en las aulas como a otros que, de manera más informal, por ejemplo, utilizan las plataformas y servicios de redes sociales para informar acerca de la seguridad en línea o imparten cursos comunitarios o escolares para garantizar la seguridad de los niños y jóvenes en línea.

La labor de los educadores depende del contexto en el que trabajan y de la edad de los niños y jóvenes (o adultos) de los que se ocupan.

Seducción/seducción en línea

La seducción (*grooming*) o seducción en línea, tal como se define en las Orientaciones de Luxemburgo, hace referencia al proceso por el que una persona establece/entabla una relación con una niña, un niño o un adolescente, ya sea en persona o mediante el uso de Internet u otras tecnologías digitales, para facilitar el contacto sexual del menor, en línea o fuera de línea, con esa persona que lo convence de que tenga una relación sexual con ella[83]. Es un proceso destinado a engatusar a los niños para que adopten un comportamiento o entablen conversaciones de carácter sexual, con o sin su conocimiento, o un proceso caracterizado por la comunicación y la socialización entre el agresor y el niño a fin de conseguir que este último sea más vulnerable al abuso sexual. En el derecho internacional no se establece la definición del concepto de *grooming* (seducción); algunos países, como Canadá, utilizan el término *luring* (engatusamiento).

Tecnologías de la información y la comunicación (TIC)

Por tecnologías de la información y la comunicación se entiende todas las tecnologías de la información centradas en la comunicación. Quedan comprendidos los servicios y dispositivos de conexión a Internet, como los ordenadores, portátiles, tabletas, teléfonos inteligentes,

81 Universidad de Western Sydney, Claire Urbach, *What is digital literacy?,* consultado el 16 de enero de 2020, https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.

82 Dr. Andrew K. Przybylski, y otros, *A Shared Responsibility. Building Children's Online Resilience* (ParentZone, Universidad de Oxford y Virgin Media, 2014), https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf.

83 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.*

consolas de juego, televisores y relojes[84]. También incluye otros servicios como la radio, la banda ancha, los equipos de red y los sistemas de satélite.

Internet y otras tecnologías conexas

Hoy en día es posible conectarse a Internet mediante diversos dispositivos como los teléfonos inteligentes, las tabletas, las consolas de juego, los televisores y los ordenadores portátiles y más tradicionales. Por lo tanto, a menos que del contexto se desprenda lo contrario, se entenderá que toda referencia a Internet abarcará todos estos métodos diferentes. Para abarcar todo el vasto y complejo entramado de Internet, se utilizan indistintamente los términos "Internet y otras tecnologías conexas" y "servicios basados en Internet".

Notificación y supresión

Los operadores y proveedores de servicios reciben a veces notificaciones sobre contenidos sospechosos en línea emitidas por clientes, la población, los organismos responsables de hacer cumplir la ley o las organizaciones que gestionan las líneas de ayuda. Por procedimientos de notificación y supresión cabe entender los procesos que aplica una empresa para retirar rápidamente ("supresión") contenido ilícito (cuya definición será la que corresponda a la correspondiente jurisdicción) en cuanto se le informa ("notificación") acerca de la presencia de dicho contenido en sus servicios.

Juegos en línea

Se entiende por "juego en línea" cualquier tipo de juego digital comercial individual o multijugador a través de cualquier dispositivo conectado a Internet, incluidas las consolas de juegos, las computadoras de escritorio, los portátiles, las tabletas y los teléfonos móviles.

El "ecosistema de juegos en línea" comprende ver cómo juegan otros jugadores de videojuegos a través de plataformas de deportes electrónicos, de secuenciación o de publicación de vídeos, que suelen ofrecer a los espectadores la posibilidad de formular comentarios o interactuar con los jugadores y otros miembros del público[85].

Herramientas de control parental

Programas informáticos que permiten a los usuarios, por lo general los padres, controlar algunas o todas las funciones de una computadora u otro dispositivo que puede conectarse a Internet. Habitualmente, estos programas pueden limitar el acceso a determinados tipos o clases de sitios web o servicios en línea. Algunos de estos programas ofrecen asimismo la posibilidad de llevar a cabo una cierta gestión del tiempo, es decir, programar el dispositivo para que solamente se pueda acceder a Internet a determinadas horas. Las versiones más avanzadas de este tipo de programas pueden almacenar todos los mensajes enviados o recibidos en el dispositivo. Normalmente, estos programas están protegidos por una contraseña[86].

Padres, cuidadores y tutores

84 UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria.*

85 UNICEF, *Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry, Discussion paper series: Children's Rights and Business in a Digital World,* 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

86 UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria.*

Varios sitios web se refieren a los padres de manera genérica (por ejemplo, incluyendo una "página para padres" y mencionando los "controles parentales"). Por consiguiente, sería útil definir las personas que, en un mundo ideal, deberían empoderar a los niños para aprovechar al máximo las oportunidades disponibles en línea, velando, a su vez, por que los niños y jóvenes utilicen los sitios Internet de manera segura y responsable y dándoles su consentimiento para acceder a algunos de ellos. En este documento, el término "padres" se refiere a cualquier persona (excluyendo a los educadores) que sea responsable legal del niño. En función de cada país variará el alcance tanto de la responsabilidad como de los derechos parentales.

Información personal

Este término describe la información de identificación personal que se recaba en línea. Esta información comprende el nombre completo, la información de contacto como la dirección postal y de correo electrónico, los números de teléfono, las huellas dactilares o el material de reconocimiento facial, los números de seguro o cualquier otro dato que permite entrar en contacto con una persona de manera física o en línea o localizarla. En este contexto, también se refiere a cualquier información sobre un niño y su entorno, recabada en línea por los proveedores de servicios en línea, en particular los juguetes conectados e Internet de las cosas, así como cualquier otra tecnología conectada.

Privacidad

La privacidad se suele determinar valorando la información personal que se comparte en línea, la tenencia de un perfil público en los medios sociales, la información que se comparte con personas conocidas en línea, la utilización de los parámetros de privacidad y la comunicación de contraseñas a amigos, y preocupándose por la privacidad[87].

Sexteo (sexting)

Por *sexting* se entiende el envío, recepción o intercambio de contenido sexual autoproducido, como imágenes, mensajes o vídeos, a través de teléfonos móviles y/o Internet[88]. En la mayoría de los países, la creación, distribución y posesión de imágenes sexuales de niños es ilegal. Si se revelan imágenes sexuales de niños, los adultos no deben verlas. El hecho de que un adulto comparta imágenes sexuales con un niño es siempre un acto delictivo, y aun cuando se compartan entre niños, puede resultar dañino, por lo que puede resultar necesario informar y tomar medidas para eliminar las imágenes compartidas.

Chantaje sexual (sextorsión) o extorsión sexual de niños

El chantaje sexual (sextorsión) o extorsión sexual (también denominada "coacción y extorsión sexual en línea")[89] es chantajear a "una persona valiéndose para ello de imágenes autogeneradas de esa persona con el fin de obtener favores sexuales, dinero u otros beneficios bajo la amenaza de que se compartirán dichas imágenes, independientemente de que la

---

87 Ley de Protección de la Privacidad en Línea para Niños, Ley Nº 15 del Código de los Estados Unidos, Arts. 6501 a 6505 (1998), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

88 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.*

89 Europol, *Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective* (Centro Europeo contra la Ciberdelincuencia, mayo de 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

persona representada en ellas dé o no su consentimiento (por ejemplo, colgando las imágenes en las redes sociales)"[90].

Internet de las cosas (IoT)

Internet de las cosas constituye la siguiente etapa hacia la digitalización de la sociedad y la economía, en la que los objetos y las personas se interconectan a través de redes de comunicación e informan sobre su estado y/o el entorno que los rodea[91].

URL

Abreviatura para *Uniform Resource Locator* (localizador uniforme de recursos), es decir, la dirección de una página de Internet[92].

Realidad virtual

La realidad virtual es la utilización de la tecnología informática para crear el efecto de un mundo tridimensional interactivo en el que los objetos tienen un sentido de presencia espacial[93].

Wi-Fi

Wi-Fi (*Wireless Fidelity* o fidelidad inalámbrica) es el conjunto de normas técnicas que permiten la transmisión de datos a través de redes inalámbricas[94].

90 *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.*
91 Ntantko, *The Internet of Things,* 1 de octubre de 2013, Digital Single Market – Comisión Europea, https://ec.europa.eu/digital-single-market/en/internet-of-things.
92 UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria.*
93 NASA, *Virtual Reality,* nas.nasa.gov, consultado el 16 de enero de 2020, https://www.nas.nasa.gov/Software/VWT/vr.html.
94 Ley de Protección de la Privacidad en Línea para Niños.

Anexo 2: Contactos delictivos contra niños y jóvenes

Los niños y jóvenes pueden estar expuestos a toda una gama de contactos no deseados o inapropiados en Internet que podrían tener consecuencias desastrosas para ellos. Algunos de esos contactos pueden ser de carácter sexual.

Los estudios han demostrado que un 22% de ellos han sido intimidados[95], acosados o acechados en línea; el 24% ha recibido comentarios sexuales no deseados[96]; el 8% se ha reunido con personas en la vida real que previamente solo habían conocido en línea[97]. Aunque las tasas varían de un país y región a otros, estas cifras demuestran que los riesgos son reales[98]. Un estudio realizado sobre Internet en los Estados Unidos de América[99] reveló que el 32% de los adolescentes en línea han sido abordados por un perfecto extraño, de los cuales el 23% afirmó haber sentido miedo e incomodidad durante ese contacto y el 4% declaró haber recibido propuestas sexuales agresivas.

Los depredadores sexuales utilizan Internet para ponerse en contacto con niños y jóvenes con fines sexuales, a menudo utilizando una técnica conocida como seducción ("grooming") con la que van ganando su confianza al hablarles de sus propios intereses. Con frecuencia introducen temas, fotos y expresiones explícitamente sexuales para desensibilizarlos, despertar su conciencia sexual y ablandar la voluntad de sus jóvenes víctimas. Se utilizan como señuelo regalos, dinero e incluso billetes de transporte para atraer al niño o al joven y persuadirlo de que acuda a un lugar donde el depredador pueda explotarlo sexualmente. Estos encuentros pueden incluso ser fotografiados o filmados en vídeo. Los niños y jóvenes a menudo carecen de madurez emocional y autoestima, lo que los hace susceptibles a la manipulación e intimidación. Estos también son reacios a hablar con adultos de sus encuentros por temor a sentirse avergonzados o a que se les niegue el acceso a Internet. En algunos casos, sus depredadores los amenazan y les dicen que mantengan la relación en secreto. Los depredadores sexuales también aprenden de sus respectivas experiencias en foros de Internet y salas de charla.

95 U-report (2019), http://www.ureport.in/v2/.
96 Proyecto deSHAME (2017), https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf.
97 Lenhardt, A., Anderson, M., Smith, A. (2015), Teens, Technology and Romantic Relationships, https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/.
98 Livingstone, S., Haddon, L., Görzig, A y Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, Londres: EU Kids Online, http://eprints.lse.ac.uk/33731/.
99 Amanda Lenhart y otros, *The Use of Social Media Gains a Greater Foothold in Teen Life as They Embrace the Conversational Nature of Interactive Online Media*, Pew Internet and American Life Project, 2007, 44, https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

Anexo 3: La Alianza Mundial WePROTECT

El Modelo de Respuesta Nacional de WePROTECT

La estrategia de la Alianza Mundial WePROTECT ayuda a los países a elaborar respuestas coordinadas entre múltiples interesados para hacer frente a la explotación sexual infantil en línea, basándose en su Modelo de Respuesta Nacional (MRN). El MRN de la Alianza Mundial WePROTECT actúa como referencia para las actividades llevadas a cabo a nivel nacional. Ofrece a los países un marco en que pueden basarse para combatir la explotación sexual infantil en línea. La finalidad del modelo es ayudar a un país a:

- evaluar su respuesta actual a la explotación sexual infantil en línea e identificar las deficiencias al respecto;
- dar prioridad a las medidas nacionales para solventar las deficiencias;
- mejorar el entendimiento y la cooperación internacional.

El Modelo no pretende imponer actividades ni establecer un único enfoque. Su finalidad radica en describir las capacidades necesarias para lograr una protección de la infancia eficaz y ayudar a los países a ampliar o mejorar sus capacidades existentes. En él también se enumeran una serie de elementos facilitadores que, si se llevan a la práctica y son eficaces, acelerarán el logro y la mejora de resultados. El MRN abarca 21 capacidades, divididas en seis secciones: política y gobernanza, justicia penal, víctimas, capacidad social, sector privado y medios y comunicaciones. La Alianza Mundial WePROTECT considera que si se trabaja en las seis esferas se logrará una respuesta nacional completa para este delito.

El Modelo permitirá a un país, con independencia de la situación de la que parta, identificar las deficiencias de capacidades y empezar a elaborar planes para suplir dichas deficiencias. Si bien los países elaborarán sus propios enfoques individuales, dado que lo harán en el contexto de un marco y un entendimiento de las capacidades establecidos de común acuerdo, se espera que se refuercen aún más la comunicación y la cooperación entre las partes interesadas tanto a nivel nacional como internacional.

La Respuesta Estratégica Global de WePROTECT

La Respuesta Estratégica Global de la Alianza Mundial WePROTECT (REG) es un enfoque coordinado para luchar contra la explotación sexual infantil en línea a fin de adquirir más conocimientos al respecto a nivel mundial, lograr la armonización internacional de los enfoques nacionales y crear soluciones a nivel mundial que se añadan a la respuesta dirigida por cada país. La REG es básicamente el complemento del Modelo de Respuesta Nacional (MRN) ya que, mientras que este se centra en las capacidades que se necesitan para luchar contra la explotación sexual infantil en línea en la esfera nacional, la primera se centra en esferas prioritarias para la colaboración y creación de capacidades a nivel internacional.

La REG incluye seis áreas temáticas a las que se asocian las capacidades que se necesitan y los resultados que se esperan para cada una de ellas, así como los asociados que deberán colaborar para conseguirlos más allá de las fronteras.

Política y legislación

El desarrollo tanto de la voluntad política para actuar como de la legislación para armonizar de manera eficaz el enfoque sobre los delitos hará que en las esferas nacional e internacional se renueve el compromiso de alto nivel de luchar contra la explotación sexual infantil en línea.

Justicia penal

El intercambio de información, incluido el acceso compartido a bases de datos internacionales mediante marcos oficiales de compartición de datos, junto con la presencia de agentes y fiscales dedicados, capacitados y con experiencia en materia de explotación sexual infantil en línea constituyen la mejor vía para identificar, perseguir y detener a agresores, por medios como la realización de investigaciones y la imposición de condenas de manera conjunta y satisfactoria.

Repercusiones para las víctimas y servicios prestados a estas

El apoyo eficaz y oportuno a las víctimas, entre otras cosas protegiendo su identidad y dándoles la palabra, contribuye a garantizar que estas puedan recibir la ayuda que necesitan, cuando la necesitan.

Tecnología

La utilización de soluciones técnicas, incluida la inteligencia artificial, para detectar, bloquear y prevenir el material dañino, la seducción en directo y en línea, que entre otras cosas deberán contar con una adhesión amplia y coherente del sector de las tecnologías, permitirá a esas plataformas evitar su uso con fines de explotación sexual infantil en línea.

Capacidades sociales

Hay una serie de capacidades complementarias que actúan en la sociedad en general con el fin de capacitar a los niños para protegerse de la explotación sexual infantil en línea, con independencia del lugar donde vivan. Si se garantiza que el desarrollo de la cultura digital es más seguro desde el diseño (es decir, que integra aspectos relacionados con la seguridad) y que se aplica un enfoque ético y coherente respecto de la difusión de información en los medios de comunicación, se reducirá la exposición al contenido ilícito en línea. Asimismo, todas las actividades educativas y de divulgación para niños y padres, cuidadores y profesionales, y las intervenciones específicas ante agresores, permitirán prevenir o reducir el número de casos de explotación sexual infantil en línea.

Investigación e información pertinente

Por último, las evaluaciones de amenazas (como la *Global Threat Assessment 2019*), las investigaciones sobre agresores y la labor encaminada a entender los traumas de las víctimas a largo plazo permitirán a los gobiernos, los organismos encargados de hacer cumplir la ley, la sociedad civil, las instituciones académicas y el sector privado entender claramente las amenazas más recientes.

Anexo 4: Ejemplos de respuestas a elementos dañinos en línea

A continuación se expone una serie de ejemplos recopilados por los autores y personas que han contribuido a las directrices de la UIT para los encargados de formular políticas.

Educación de los niños sobre los elementos dañinos en línea

Own IT App: aplicación de la BBC destinada al bienestar de los niños de entre 8 y 13 años que adquieren su primer teléfono inteligente. Al combinar tecnologías vanguardistas de aprendizaje automático para controlar la actividad de los niños en sus teléfonos inteligentes con la posibilidad de que estos comuniquen por sí mismos su estado emocional, la aplicación utiliza dicha información para ofrecer intervenciones y contenidos personalizados a fin de ayudar a los niños a seguir siendo felices y sanos en línea.

Dotada de contenido especialmente encargado por la BBC, la aplicación proporciona material y recursos útiles para ayudar a los jóvenes a aprovechar al máximo su tiempo en línea y adoptar conductas y hábitos en línea sanos, contribuyendo a que tanto estos como sus padres mantengan conversaciones más constructivas sobre sus experiencias en línea. La aplicación no recaba datos personales ni contenidos generados por el usuario, ya que todo el sistema de aprendizaje automático opera sólo en la aplicación/el dispositivo del usuario.

Proyecto Evolve: marco educativo sobre competencias digitales plenamente equipado que determina las habilidades digitales para cada una de las edades del niño a fin de ayudar a los padres y profesores a entender las competencias que deberían tener sus hijos, junto con recursos y actividades que les ofrecerán las habilidades específicas.

360 degree safe: herramienta de autorrevisión destinada a las escuelas para que estas examinen y evalúen el grado de seguridad general en línea total que ofrecen, en la que se brinda orientación y ayuda para alcanzar los niveles definidos.

DQ Institute: entre 2017 y 2019 se recabaron datos de 145 426 niños y adolescentes procedentes de 30 países en el marco de la iniciativa #DQEveryChild, un movimiento mundial de ciudadanía digital promovido por el DQ Institute, que comenzó en Singapur con el apoyo de Singtel y se ha propagado rápidamente con la colaboración del Foro Económico Mundial hasta incluir a más de 100 organizaciones asociadas. Este movimiento tenía por objetivo dotar a los niños de amplias competencias en materia de ciudadanía digital desde el comienzo de sus vidas digitales mediante el programa de educación y evaluación DQ World. Los datos obtenidos en el contexto de este movimiento se utilizaron para crear el Índice de seguridad de la infancia en línea de 2020. En el marco establecido para el Índice de Seguridad de la Infancia en Línea se evalúan y clasifican los niveles de seguridad infantil en línea de 30 países en función de 24 áreas agrupadas en seis pilares que inciden en la seguridad de los niños en línea.

La herramienta Family Readiness Package para familias y la plataforma DQ World para niños brindan a los padres la oportunidad de evaluar la preparación digital de sus hijos y, a través de materiales pedagógicos, permiten mejorar las competencias digitales como la ciudadanía

digital, la administración del tiempo de pantalla, la gestión del ciberacoso y la ciberseguridad, la empatía digital, el control de la huella digital, el pensamiento crítico y la gestión de la privacidad.

El Conjunto de herramientas en materia de ciberseguridad para escuelas de Australia es una serie de recursos diseñados para ayudar a las escuelas a crear entornos en línea más seguros. Este conjunto de herramientas es reflejo de un enfoque polifacético de la educación en materia de la seguridad en línea y se ha dividido en cuatro elementos, con recursos que:

- ayudan a la escuelas a evaluar su grado de preparación para abordar cuestiones relativas a la seguridad en línea y ofrecen sugerencias para mejorar sus prácticas actuales;
- hacen que toda la comunidad se comprometa y participe en la creación de un entorno en línea seguro;
- educan destacando las prácticas idóneas en materia de educación sobre seguridad en línea y ayudando a las escuelas a desarrollar las capacidades de toda la comunidad escolar sobre la seguridad en línea;
- responden de manera eficaz a los incidentes y respaldan al mismo tiempo la seguridad y el bienestar.

La campaña educativa I Click Sensible de la Oficina de Comunicaciones Electrónicas de Polonia (UKE) enseña a los niños y padres a aumentar su seguridad en línea y a reconocer y gestionar los riesgos.

ChildFund Viet Nam creó la iniciativa Swipe Safe. Este programa forma a los niños sobre los posibles riesgos en línea como el fraude, la intimidación o el abuso sexual por Internet y ofrece asesoramiento sobre los métodos para permanecer seguros.

Informe de la Comisión de la Banda Ancha sobre *Technology, Broadband and Education: advancing the education for all agenda*, 2013.

Children's Experiences Online: Building Global Understanding and Action, UNICEF, 2019.

En las investigaciones de Global Kids Online figura una gran cantidad de información sobre las buenas prácticas en materia de respuestas a los elementos dañinos en línea.

Ejemplos de participación del sector privado

El Comisionado de Ciberseguridad de Australia establece sólidas alianzas y colabora con el sector privado a fin de empoderar a todos los australianos con miras a que sus experiencias en línea sean más seguras y positivas. Un ejemplo de dicha colaboración es la labor que realiza este Comisionado en materia de seguridad desde el diseño. Como parte de la iniciativa, el Comisionado llevó a cabo un proceso de consulta con el sector privado, los organismos profesionales y las organizaciones encargadas de proteger a los usuarios, así como los padres, cuidadores y jóvenes. La iniciativa de la Seguridad desde el Diseño fue concebida para alentar y ayudar al sector privado a garantizar la incorporación de la seguridad del usuario en el diseño, la elaboración y el despliegue de servicios y plataformas en línea. El Comisionado también administra tres sistemas de notificación y presentación de denuncias destinados respectivamente a los actos de ciberacoso, abuso basado en imágenes y los contenidos en línea. Asimismo, el Comisionado puede ordenar oficialmente a los proveedores de servicios en línea a retirar contenidos de sus servicios. Si bien los sistemas funcionan de manera general como un modelo cooperativo entre el gobierno y el sector privado, las facultades de que dispone el Comisionado para imponer la supresión de material ofrece una red de seguridad

fundamental y da lugar a que las empresas hagan frente a los elementos dañinos en línea de manera proactiva.

La empresa Telia asume la responsabilidad de entender y gestionar los efectos negativos de la conectividad y su obligación de transparencia y responsabilidad de su Consejo de Administración. También presta especial atención a los niños y jóvenes, al reconocerlos como usuarios activos de sus servicios.

La Oficina de Comunicaciones Electrónicas de Polonia (UKE) hace que en sus campañas de promoción participen la sociedad civil y los niños para que sean conscientes de lo que firman en línea.

La Internet Watch Foundation es una organización colectiva que reúne al sector privado, el gobierno, los organismos responsables de hacer cumplir la ley y las ONG para poner fin al abuso sexual infantil. En 2020, la IWF cuenta con 152 miembros que prestan servicios de plataformas e infraestructura, a los que a su vez ofrece diversos servicios para prevenir la difusión de imágenes delictivas en sus plataformas.

Cobertura de la legislación

Es necesario que se exprese la voluntad política de dar prioridad a la PIeL mediante la firma de la Declaración Universal sobre la Seguridad de la Infancia en Línea (Comisión de la Banda Ancha).

Reglamentación

El índice *Out of the Shadows: shining light on the response to child sexual abuse and exploitation Index* (2019) de la Unidad de Inteligencia de *The Economist* es la única herramienta comparativa que analiza la respuesta de los países a los actos de abuso y explotación sexual de menores, incluso los cometidos en el espacio digital, y la respuesta del sector de las TIC a dichos actos.

Identificación del abuso de menores en línea

A continuación se exponen algunos ejemplos de buenas prácticas en materia de identificación del abuso de menores en línea.

INHOPE: la red INHOPE se constituyó en 1999 a fin de luchar contra el material de abuso sexual infantil en línea con el objetivo común de que Internet estuviera libre de contenidos de este tipo. Durante los 20 años en que ha estado interviniendo, la red INHOPE se ha ampliado para combatir satisfactoriamente el crecimiento, la propagación geográfica y la gravedad de los materiales de abuso sexual infantil en línea. Hoy en día, en cada continente hay líneas de ayuda sobre el terreno, que reciben notificaciones y suprimen rápidamente estos materiales de Internet, compartiendo también información con los organismos responsables de hacer cumplir la ley.

La tecnología **PhotoDNA** de Microsoft crea algoritmos generadores (*hashes*) de imágenes y los coteja con una base de datos de algoritmos generadores sobre los que ya se determinó y confirmó que correspondían a materiales de abuso sexual infantil. Si encuentra una correspondencia, se bloquea la imagen. Sin embargo, esta herramienta no utiliza la tecnología de reconocimiento facial ni tampoco puede identificar a una persona u objeto en la imagen. No obstante, es posible que la situación cambie con la invención de la tecnología PhotoDNA para vídeo.

La tecnología **PhotoDNA para vídeo** descompone el vídeo en fotogramas y básicamente crea algoritmos generadores para esas capturas de imagen. Así como la tecnología PhotoDNA permite identificar una imagen que ha sido modificada para evitar que se detecte al autor, la tecnología PhotoDNA para vídeo puede localizar contenidos sobre explotación sexual infantil que han sido editados o integrados en un vídeo que, de lo contrario, no parecería dañino.

Microsoft ha creado una nueva herramienta para identificar a los predadores de niños que los seducen para abusar de ellos en los chats en línea. El **Proyecto Artemis**, desarrollado en colaboración con Meet Group, Roblox, Kik y Thorn, se basa en la tecnología patentada de Microsoft y se pondrá gratuitamente a disposición de las empresas de servicios en línea que ofrecen funciones de conversación a través de Thorn. El Proyecto Artemis es una herramienta tecnológica que ayuda a advertir a los administradores cuándo es necesario que intervengan en las salas de charla. Esta técnica de detección de los actos de seducción permitirá detectar a los predadores que intentan atraer a los niños con fines sexuales, hacer frente a tales actos y notificarlos.

Thorn ha creado anuncios disuasivos destinados a quienes buscan material de abuso sexual infantil, que se han mostrado millones de veces en cuatro motores de búsqueda durante un periodo de tres años. Además, estos anuncios han tenido una tasa de cliqueo del 3%, consultados por personas que desean recibir ayuda tras haber buscado material relacionado con la explotación.

El programa **Safer**, una herramienta de Thorn que puede implementarse directamente en la plataforma privada de una empresa para detectar, suprimir y notificar materiales de abuso sexual infantil.

Spotlight, un programa informático de Thorn que ofrece a los organismos responsables de hacer cumplir la ley en los 50 estados de los Estados Unidos de América y en Canadá la posibilidad de acelerar el proceso de identificación de víctimas y reducir el tiempo dedicado a la investigación en más de un 60%.

Geebo, un sitio web conocido por su compromiso relativo a la ausencia total de explotación sexual en su plataforma, no ha registrado nunca un caso de explotación sexual infantil. Esto se ha conseguido en parte gracias a su proceso de control previo de los usuarios.

El **Clasificador de Google basado en la IA** se puede utilizar para detectar material de abuso sexual infantil en redes, servicios y plataformas. Esta herramienta se encuentra disponible de manera gratuita a través de **Google Content Safety API**, que es un conjunto de herramientas que aumenta la capacidad para revisar contenidos de una manera que requiere la presencia de un menor número de personas. Esta herramienta ayudaría a los especialistas a revisar el material a una escala aún mayor y a mantenerse al día de las actividades de los agresores, al centrarse en imágenes que no se consideraban previamente material ilícito. La compartición de esta tecnología aceleraría la identificación de imágenes.

En 2015, Google amplió su labor sobre los algoritmos generadores al introducir la primera tecnología de identificación y cotejo para vídeos en **YouTube**, que escanea y detecta los vídeos cargados en esa plataforma que incluyen material conocido de abuso sexual infantil.

En 2019, en el contexto del *Hackathon* para la Seguridad Infantil, **Facebook** anunció que daría a conocer los códigos de dos tecnologías que detectan fotografías y vídeos idénticos y casi idénticos. Estos dos algoritmos se encuentran disponibles en GitHub, que permite que los

sistemas de intercambio de algoritmos generadores comuniquen entre sí, haciendo que los sistemas sean mucho más potentes.

La **línea de ayuda de la IWF** permanece constantemente alerta y no solo realiza el seguimiento de los miles de notificaciones emitidas por particulares, que tal vez hayan tropezado con imágenes de abusos sexuales de niños en línea, sino que también desempeña una función excepcionalmente proactiva de búsqueda de contenido ilícito en Internet. Al otorgar facultades a las líneas de ayuda para que utilicen su información y reorienten sus recursos, se puede identificar y suprimir un mayor número de contenidos. Además, la IWF trabaja continuamente con Google, Microsoft, Facebook y otras empresas que forman parte de sus miembros para ensanchar las fronteras de los conocimientos técnicos. La IWF ofrece la solución del Portal de notificaciones, que permite a los usuarios de Internet situados en países y naciones sin líneas de ayuda notificar directamente a la IWF imágenes y vídeos de actos sospechosos de abuso sexual infantil a través de una página del portal en línea prevista específicamente para tal efecto.

En colaboración con la **Fundación caritativa Marie Collins de ayuda a las víctimas**, la IWF tiene por objeto crear una nueva campaña para alentar a los jóvenes varones a notificar las imágenes o vídeos sexuales autogenerados de menores de 18 años con los que hayan tropezado al navegar por Internet.

Interpol ha creado una Base de Datos Internacional sobre imágenes y vídeos relacionados con la Explotación Sexual de Niños (ICSE), que constituye una herramienta de inteligencia e investigación que permite a investigadores especializados procedentes de más de 50 países compartir información sobre casos de abuso sexual de menores. Al analizar el contenido digital, visual y de audio de las fotografías y vídeos, los expertos en la identificación de víctimas pueden obtener pistas, identificar cualquier solapamiento de casos y aunar sus esfuerzos a fin de localizar a las víctimas de abuso sexual infantil. Actualmente, la Base de Datos Internacional sobre la Explotación Sexual de Niños de Interpol cuenta con más de 1,5 millones de imágenes y vídeos y ha ayudado a identificar a más de 19 400 víctimas en todo el mundo.

NetClean ProActive es un programa informático basado en la correspondencia de firmas y otros algoritmos de detección que detecta automáticamente las imágenes y vídeos de abuso sexual infantil en entornos empresariales.

Griffeye Brain utiliza la inteligencia artificial para escanear contenido que hasta ahora no estaba clasificado, compararlo con los atributos de los materiales conocidos de abuso sexual infantil y notificar elementos sospechosos para que un agente los revise.

RAINN estableció y opera la Línea nacional para víctimas de agresiones sexuales en colaboración con más de 1 000 proveedores locales de servicios de notificación de agresiones sexuales de todo el país y opera también la Línea de ayuda Safe del Departamento de Defensa. RAINN también lleva a cabo programas para prevenir la violencia sexual, ayudar a los supervivientes y velar por que se enjuicie a los autores.

Safehorizon es una organización de ayuda a las víctimas sin ánimo de lucro que desde 1978 lleva apoyando a las víctimas de la violencia y abusos en la ciudad de Nueva York. Safehorizon ofrece servicios de asistencia telefónica a las víctimas de la violencia.

El Proyecto Arachnid es una herramienta innovadora operada por el Centro Canadiense de Protección de la Infancia para combatir la creciente proliferación de materiales de abuso sexual infantil (MASI) en Internet.

[i] http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf

Con el apoyo de:

Unión
Internacional
de Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza

ISBN: 978-92-61-30453-9

Publicado en Suiza
Ginebra, 2020