ITUPublicaciones

Unión Internacional de Telecomunicaciones
Sector de Desarrollo

Directrices sobre la protección de la infancia en línea para la industria

2020

Directrices sobre la protección de la infancia en línea para la industria

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 la EBU, la Alianza Mundial para Erradicar la Violencia contra el Niño, GSMA, la Alianza Internacional de la Discapacidad, la Internet Watch Foundation (IWF), Privately SA y UNICEF. El grupo de trabajo estuvo presidido por Anjan Bose (UNICEF) 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 e-Worldwide Group (e-WWG), Facebook, Tencent Games, Twitter, the Walt Disney Company, así como otros interesados de la industria, 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):

- Giacomo Mazzone (EBU)
- Salma Abbasi (e-WWG)
- David Miles and Caroline Hurst (Facebook)
- Amy Crocker and Serena Tommasino (Alianza Mundial para Acabar con la Violencia contra los Niños)
- Jenny Jones (GSMA)
- Lucy Richardson (Alianza Internacional de la Discapacidad)
- Fanny Rotino (UIT)
- Tess Leyland (IWF)
- Deepak Tewari (Privately SA)
- Adam Liu (Tencent Games)
- Katy Minshall (Twitter)
- Anjan Bose, Daniel Kardefelt Winther, Emma Day, Josianne Galea Baron, Sarah Jacobstein y Steven Edwin Vosloo (UNICEF)
- Amy E. Cunningham (The Walt Disney Company)

ISBN

978-92-61-30083-8 (versión impresa)

978-92-61-30413-3 (versión electrónica)

978-92-61-30073-9 (versión ePub)

978-92-61-30423-2 (versión Mobi)

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

Prefacio

La proliferación de las tecnologías digitales ha creado oportunidades sin precedentes para que los niños y jóvenes se comuniquen, se conecten, compartan, aprendan, accedan a información y manifiesten sus opiniones sobre cuestiones que afectan a sus vidas y a sus comunidades.

Ahora bien, el mayor y más fácil acceso a los servicios en línea conlleva importantes problemas para la seguridad de los niños, tanto en línea como fuera de línea. Hoy en día los niños se enfrentan a abundantes riesgos graves, que van desde cuestiones relacionadas con la privacidad, violencia entre ellos y contenido violento y/o inapropiado para su edad, hasta estafas y delitos por Internet contra los niños, como la seducción (*grooming*) en línea y el abuso y explotación sexuales. Los peligros se multiplican y los perpetradores operan de manera cada vez más coordinada a través de las fronteras, dificultando aún más su rastreo y judicialización.

Por otra parte, a raíz de la pandemia mundial de la COVID-19 ha aumentado repentinamente el número de niños que se incorporaron por primera vez al mundo digital para cursar sus estudios y socializar. 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 éstos accedieran a contenidos inapropiados o fueran blanco de delincuentes que producen material de abuso sexual infantil (MASI).

Los delincuentes se aprovechan de los adelantos tecnológicos, como las aplicaciones y juegos interconectados, el intercambio rápido de archivos, las transmisiones en vivo, las criptodivisas, la Red Oscura y el software de cifrado fuerte. Asimismo, se benefician de la acción a menudo descoordinada y vacilante del sector tecnológico para contrarrestar eficazmente este problema.

La solución puede venir de las tecnologías incipientes, por ejemplo, la base de datos de la Interpol sobre abuso sexual infantil basada en inteligencia artificial que utiliza programas informáticos de comparación de imágenes y vídeos para establecer rápidamente conexiones entre víctimas, abusadores y lugares. Pero la tecnología por sí sola no resolverá el problema.

A fin de reducir los riesgos de la revolución digital y, a su vez, permitir que cada vez más jóvenes saquen provecho de sus ventajas, es fundamental, ahora más que nunca, una respuesta colaborativa y coordinada multipartita. Los gobiernos, la sociedad civil, las comunidades locales, las organizaciones internacionales y los interesados de la industria deben aunar esfuerzos para este fin común.

Habida cuenta de lo anterior, en 2018 los Estados Miembros de la UIT solicitaron una revisión exhaustiva de nuestras directrices sobre protección de la infancia en línea. Estas nuevas directrices de la UIT 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 de esta generación. Además de integrar los nuevos adelantos en las tecnologías y plataformas digitales, esta nueva edición aborda un importante tema pendiente: la situación de los niños con discapacidad, a quienes el mundo en línea les brinda la oportunidad de participar plena y satisfactoriamente en la sociedad.

La industria de la tecnología debe desempeñar un papel fundamental y proactivo a la hora de sentar las bases de la protección y utilización segura de los servicios basados en Internet y otras tecnologías, tanto para los niños de hoy en día como para las futuras generaciones.

Las empresas deben tener más en cuenta el interés del niño en sus actividades, prestando especial atención a proteger la privacidad de los datos personales de los jóvenes usuarios, a preservar su derecho a la libertad de expresión, a combatir el creciente problema del MASI y a garantizar que, cuando se infrinjan los derechos del niño, existan sistemas para actuar con eficacia.

Allá donde las leyes nacionales aún no se hayan adaptado al derecho internacional, las empresas tienen la oportunidad –y la responsabilidad– de ajustar sus propios marcos operativos a las normas más estrictas y a las prácticas idóneas.

Esperamos que, para la industria, estas directrices constituyan una sólida referencia sobre la que elaborar políticas empresariales y soluciones innovadoras. Fiel 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, por cuanto han sido redactadas de consuno por expertos procedentes de una amplia comunidad internacional.

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 de un nuevo programa internacional de la UIT de divulgación destinado a la juventud.

En una época en la que son cada vez más los jóvenes conectados a Internet, estas directrices de la UIT sobre la protección de la infancia en línea resultan más indispensables que nunca. La industria, los gobiernos, los padres y los educadores, así como los propios niños, desempeñan un papel fundamental en la seguridad de la infancia en línea. Agradezco, como siempre, su apoyo y espero con interés continuar nuestra estrecha colaboración en esta cuestión fundamental.

Doreen Bogdan-Martin
Directora
Oficina de Desarrollo de las Telecomunicaciones, UIT

Índice

Cuadros

1 Generalidades

El objetivo del presente documento es servir de orientación a los interesados de la industria de las TIC a fin de que establezcan sus propios recursos de protección de la infancia en línea (PIeL). La finalidad de estas directrices para la industria sobre PIeL es ofrecer un marco útil, flexible y fácil de utilizar tanto en lo relativo a las perspectivas empresariales como en relación con su responsabilidad de proteger al usuario. Tienen por objeto, además, sentar las bases de la protección y utilización segura de los servicios basados en Internet y otras tecnologías conexas, tanto para los niños de hoy en día como para las futuras generaciones

En cuanto a su utilidad, se espera que estas directrices contribuyan a aumentar el éxito empresarial y ayuden a los interesados a crear un modelo comercial atractivo y sostenible para operaciones grandes y pequeñas, permitiendo, a su vez, comprender las responsabilidades jurídicas y morales para con los niños y la sociedad.

En respuesta a los importantes adelantos tecnológicos y a la convergencia, la UIT, UNICEF y los asociados para la protección de la infancia en línea han elaborado y actualizado las directrices para muy diversas empresas que desarrollan, suministran o utilizan las telecomunicaciones o actividades conexas en la prestación de sus productos y servicios.

Las nuevas directrices para la industria sobre la protección de los niños en línea son el resultado de consultas con los miembros de la Iniciativa PIeL y de consultas más amplias con miembros de la sociedad civil, el mundo empresarial, los círculos académicos, los gobiernos, los medios de comunicación, las organizaciones internacionales y los jóvenes.

La finalidad de este documento es:

- establecer un punto de referencia y una orientación comunes para las industrias de las TIC y de Internet y los interesados pertinentes;
- orientar a las empresas para identificar, prevenir y mitigar cualquier efecto negativo que pudieran tener sus productos y servicios sobre los derechos de los niños;
- orientar a las empresas para determinar cómo pueden promover los derechos del niño y el civismo digital responsable entre los niños;
- proponer principios comunes que sirvan de base para adoptar compromisos a escala nacional o regional de todas las industrias afines, reconociendo a su vez que cada tipo de empresa aplicará modelos distintos.

Alcance

La protección de la infancia en línea es un problema complejo que abarca múltiples y diferentes aspectos de gobernanza, políticos, operativos, técnicos y jurídicos. En las presentes directrices se intenta abordar, organizar y priorizar muchas de esas esferas, mediante modelos, marcos y otras referencias existentes y ampliamente reconocidos.

Las directrices se centran en la protección de la infancia en todos los ámbitos y contra todos los riesgos del mundo digital y, en ese sentido, ponen de relieve las buenas prácticas de los interesados de la industria que pueden tomarse en consideración en el proceso de elaboración, desarrollo y gestión de las políticas de la empresa en materia de PIeL. Ofrecen orientación a los agentes industriales sobre la forma de gestionar y frenar las actividades ilícitas en línea contra las que tienen el deber de actuar (como el CSAM en línea) a través de sus servicios y, por añadidura, se centran en ostros aspectos que tal vez no sean delito en todas las jurisdicciones. Entre ellas figuran la violencia entre niños, el ciberacoso y el hostigamiento en línea, así como

cuestiones relacionadas con la privacidad o el bienestar general, el fraude y otros peligros, que sólo son perjudiciales para los niños en determinados contextos.

Con este fin, estas directrices incluyen recomendaciones sobre buenas prácticas para hacer frente a los riesgos a los que se enfrentan los niños en el mundo digital y sobre cómo actuar para crear un entorno seguro para los niños en línea. Estas directrices ofrecen asesoramiento sobre cómo puede actuar la industria para contribuir a garantizar la seguridad de los niños cuando utilizan las TIC, Internet o cualquiera de las tecnologías o dispositivos afines con los que se pueden conectar, en particular teléfonos móviles, consolas de juego, juguetes conectados, relojes, Internet de las cosas y sistemas basados en la inteligencia artificial. Por consiguiente, ofrecen un panorama general de los problemas y retos fundamentales relativos a la protección de la infancia en línea y proponen medidas para las empresas y los interesados destinadas a la creación de políticas locales e internas de protección de los niños. Estas directrices no entran en aspectos tales como el proceso de elaboración real o el texto que podrían incluir las políticas en materia de PIeL para la industria.

Estructura

Sección 1 – Generalidades: En esta sección se describe la finalidad, el alcance y los destinatarios de estas directrices.

Sección 2 – Introducción a la protección de la infancia en línea: En esta sección se presenta el panorama general de la cuestión de la protección de la infancia en línea y se esbozan algunos antecedentes, incluida la situación especial de los niños con discapacidad. Además, se dan ejemplos de los modelos internacionales y nacionales existentes para garantizar la seguridad de los niños en línea, y que dan una idea de las posibles esferas de intervención para los interesados de la industria.

Sección 3 – Principales ámbitos de protección y fomento de los derechos del niño: En esta sección se describen cinco ámbitos fundamentales de actuación de las empresas para garantizar la seguridad y experiencia positivas de los niños en la utilización de las TIC.

Sección 4 – Orientaciones generales: En esta sección se formulan recomendaciones a todos los interesados de la industria sobre la protección de la seguridad de los niños en la utilización de las TIC y el fomento de una utilización positiva de las TIC, incluido el civismo digital responsable entre los niños.

Sección 5 – Lista de prestaciones: En esta sección se destacan recomendaciones específicas para los interesados sobre medidas concretas para respetar y proteger los derechos del niño, con las prestaciones siguientes:

- Prestación A: Conectividad, almacenamiento de datos y servicios de hospedaje
- Prestación B: Ofrecer contenido digital depurado
- Prestación C: Hospedar contenido producido por el usuario y conectar usuarios
- Prestación D: Sistemas basados en inteligencia artificial

Destinatarios

Inspirándose en los Principios rectores de las Naciones Unidas sobre las empresas y los derechos humanos [1], los Derechos del niño y principios empresariales se aboga por que las

[1] Principios Rectores de Naciones Unidas sobre las Empresas y los Derechos Humanos.

empresas cumplan con su responsabilidad de respetar los derechos de los niños evitando las consecuencias negativas de sus operaciones, productos o servicios. Estos Principios también articulan la diferencia entre el respeto (mínimo requerido a las empresas para evitar causar daño a los niños) y el apoyo (por ejemplo, mediante la adopción de medidas voluntarias para promover el cumplimiento de los derechos del niño). Las empresas deben garantizar los derechos del niño tanto en lo relativo a su protección en línea como al acceso a la información y la libertad de expresión, además de promover la utilización positiva de las TIC por los niños.

La tradicional distinción entre las diferentes partes de las industrias de las telecomunicaciones y la telefonía móvil, y entre las empresas de Internet y las emisoras de radio y televisión, está desapareciendo rápidamente y quedando desdibujada. La convergencia está aunando los distintos canales digitales en un único flujo que llega a miles de millones de personas en todos los rincones del mundo. Resulta fundamental la cooperación y la asociación para sentar las bases para la protección y seguridad de Internet y las tecnologías conexas. Los gobiernos, el sector privado, los responsables políticos, los docentes, la sociedad civil, los padres y tutores desempeñan un papel fundamental en el logro de este objetivo. La industria puede actuar en cinco esferas clave, como se describe en la sección 3.

2 Qué es la protección de la infancia en línea

En los últimos 10 años, la utilización y papel de Internet en la vida de las personas ha cambiado considerablemente. La abundancia de teléfonos inteligentes y tabletas, la accesibilidad de la tecnología Wi-Fi y 4G y la evolución de las plataformas y aplicaciones de redes sociales, son cada vez más las personas que acceden a la Internet por razones que van en aumento.

En 2019, más de la mitad de la población mundial utilizaba la Internet. La mayor proporción de usuarios de Internet son personas menores de 44 años, si bien la proporción es igualmente elevada entre los jóvenes de 16 a 24 años y los de 35 a 44 años. A escala mundial, uno de cada tres usuarios de Internet es un niño (de 0 a 18 años) y UNICEF estima que el 71% de los jóvenes ya están conectados[2]. La proliferación de los puntos de acceso a la Internet, la tecnología móvil y la creciente variedad de dispositivos con Internet, junto con los inmensos recursos que se encuentran en el ciberespacio, brindan oportunidades sin precedentes para aprender, compartir y comunicar.

Entre las ventajas de utilizar las TIC figura un acceso más amplio a la información sobre servicios sociales, recursos educativos y asesoramiento sanitario. Dado que los niños, los jóvenes y las familias utilizan la Internet y los teléfonos móviles para buscar información y asistencia, y para denunciar incidentes de abuso, estas tecnologías pueden contribuir a proteger a los niños y jóvenes de la violencia y la explotación. Los proveedores de servicios de protección de la infancia también utilizan las TIC para recabar y transmitir datos, lo que permite facilitar, entre otras cosas, la inscripción de nacimientos, la gestión de casos, la localización de familias, la recopilación de datos y la catalogación de la violencia.

Por otra parte, la Internet ha aumentado el acceso a la información en todos los rincones del planeta, de modo que los niños y jóvenes pueden buscar información sobre prácticamente

[2] OCDE, "New Technologies and 21st Century Children: Recent Trends and Outcomes", Education Working Paper Nº 179.

cualquier tema de su interés, acceder a los medios de comunicación mundiales, perseguir perspectivas profesionales y aprovechar ideas para el futuro. La utilización de las TIC les permite ejercer sus derechos y manifestar sus opiniones, así como conectarse y comunicarse con sus familias y amigos. Las TIC también constituyen un medio privilegiado para el intercambio cultural y el esparcimiento.

A pesar de los profundos beneficios de Internet, la utilización de las TIC también conlleva riesgos para los niños y jóvenes. Pueden verse expuestos a contenidos inapropiados para su edad o a contactos inadecuados, incluso con posibles autores de abusos sexuales. Pueden sufrir daños en su reputación como consecuencia de la publicación en línea de información personal sensible o al "sextear", y a menudo no son conscientes de las consecuencias de sus actos para ellos mismos y para los demás, ni de sus "huellas digitales" a largo plazo. También se enfrentan a riesgos relacionados con la privacidad en línea derivados de la recopilación de datos y el registro y utilización de información de localización.

La Convención sobre los Derechos del Niño, que es el tratado internacional de derechos humanos más ampliamente ratificado[3], establece los derechos civiles, políticos, económicos, sociales y culturales de los niños. Establece que todos los niños y jóvenes tienen derecho a la educación; al esparcimiento, al juego y a la cultura; a una información adecuada; a la libertad de pensamiento y de expresión; a la intimidad y a expresar sus opiniones sobre las cuestiones que les afectan con arreglo a la evolución de sus facultades. La Convención también protege a los niños y jóvenes contra todas las formas de violencia, explotación, abuso y discriminación de cualquier tipo, y establece que el interés superior del niño debe ser la consideración primordial en cualquier asunto que le afecte. Los padres, tutores, educadores y miembros de la comunidad, incluidos los dirigentes comunitarios y los agentes de la sociedad civil, tienen la responsabilidad de cuidar y ayudar a los niños y jóvenes en su paso a la edad adulta. El papel de los gobiernos es fundamental a la hora de garantizar que todos esos interesados cumplan su función.

En lo que respecta a la protección de los derechos del niño en línea, las industrias deben colaborar para lograr un cuidadoso equilibrio entre el derecho del niño a la protección y su derecho al acceso a la información y a la libertad de expresión. Por consiguiente, las empresas deben dar prioridad a las medidas de protección específicas para niños y jóvenes en línea y que no sean indebidamente restrictivas, ni para el niño o para otros usuarios. Además, existe un consenso cada vez mayor acerca de que el fomento del civismo digital entre los niños y jóvenes, y el desarrollo de productos y plataformas que faciliten el uso positivo de las TIC por los niños, deben ser una prioridad para el sector privado.

Si bien las tecnologías en línea presentan muchas oportunidades para que los niños y jóvenes se comuniquen, aprendan nuevas aptitudes, sean creativos y contribuyan a mejorar la sociedad para todos, también conllevan nuevos riesgos para la seguridad de los niños y jóvenes. Estos se ven expuestos a posibles riesgos y peligros relacionados con la privacidad, el contenido ilegal, el hostigamiento, el ciberacoso, el uso indebido de datos personales o la seducción con fines sexuales e incluso abuso y explotación sexual infantil. Otros peligros son los daños a su reputación, incluido el "porno de venganza" que consiste en la publicación de información personal sensible en línea o mediante el "sexteo", es decir, el envío de mensajes, fotografías o imágenes sexualmente explícitas entre usuarios de teléfonos móviles. Asimismo, al utilizar

[3] Convención de las Naciones Unidas sobre los Derechos del Niño. Todos los países, excepto tres (Somalia, Sudán del Sur y Estados Unidos), han ratificado la Convención sobre los Derechos del Niño.

Internet también se enfrentan a riesgos relacionados con la privacidad en línea. Los niños, dada su edad y madurez, son a menudo incapaces de comprender plenamente los riesgos que plantea el mundo en línea y las posibles repercusiones negativas de su comportamiento improcedente para ellos mismos y para los demás.

A pesar de las ventajas, la utilización de tecnologías incipientes y de vanguardia también presenta inconvenientes. Los adelantos en la inteligencia artificial y el aprendizaje automático, la realidad virtual y aumentada, los macrodatos, la robótica e Internet de las cosas van a transformar aún más las actividades de los niños y jóvenes en los medios. Si bien estas tecnologías se están desarrollando predominantemente para ampliar el suministro de servicios y mejorar las prestaciones (mediante, por ejemplo, la asistencia de voz, la accesibilidad y nuevas formas de inmersión digital), algunas de esas tecnologías podrían tener efectos imprevistos e incluso ser utilizadas indebidamente por delincuentes sexuales de menores para sus propios fines. La creación de un entorno en línea seguro y protegido para los niños y jóvenes requiere de la participación efectiva de los gobiernos, el sector privado y todos los interesados. Otro de los principales objetivos es fomentar las aptitudes digitales y la formación de padres y educadores, a cuya consecución la industria puede desempeñar un papel esencial y sostenible.

Es posible que algunos niños sean conscientes de los riesgos en línea y cómo reaccionar a ellos. Sin embargo, no siempre es así, especialmente entre los grupos vulnerables. En virtud de la meta 16.2 de los Objetivos de Desarrollo Sostenible de las Naciones Unidas, que tiene por objeto poner fin al maltrato, la explotación, la trata, la tortura y todas las formas de violencia contra los niños, la protección de la infancia en línea es fundamental.

Desde 2009, la Iniciativa PIeL, una iniciativa internacional multipartita creada por la UIT, ha tenido por objeto concienciar sobre los riesgos para los niños en línea y cómo reaccionar a los mismos. La Iniciativa reúne a asociados de todos los sectores de la comunidad internacional para garantizar que los niños de todo el mundo tengan una experiencia en línea segura. En el marco de esta Iniciativa, la UIT publicó en 2009 un conjunto de directrices de la PIeL para cuatro grupos: los niños; los padres, tutores y educadores; la industria; y los responsables políticos. En esas directrices se entiende que la protección de los niños en línea es un planteamiento integral para responder a todos los posibles peligros y daños que los niños y jóvenes puedan encontrar en línea o por medio de tecnologías en línea. En el presente documento, la protección de la infancia en línea también incluye los daños que se producen fuera de la red pero que están vinculados a violencia y abuso en línea. Además de considerar el comportamiento y las actividades de los niños en línea, la protección de la infancia en línea también se refiere al uso indebido de la tecnología por adultos para explotar a los niños.

Todos los interesados tienen que colaborar para ayudar a los niños y jóvenes a aprovechar las oportunidades que ofrece Internet y a adquirir conocimientos digitales y capacidad de recuperación en relación con su bienestar y protección en línea.

La protección de los niños y jóvenes es responsabilidad de todos los interesados. Por ese motivo, los responsables políticos, la industria, los padres, los tutores, los educadores y otros interesados deben velar por que los niños y jóvenes puedan desarrollar todo su potencial, tanto en línea como fuera de línea.

Si bien no existe una definición universal, por protección de la infancia en línea se entiende que ésta adopta un planteamiento integral para crear espacios digitales seguros, inclusivos, participativos y adecuados para la edad de los niños y jóvenes, caracterizados por:

- respuesta, apoyo y autoayuda frente a las amenazas;
- prevención de daños;
- equilibrio dinámico entre garantizar la protección y brindar oportunidades a los niños para que se conviertan en ciudadanos digitales;
- defensa de los derechos y responsabilidad de niños y la sociedad.

Además, dada la rapidez de los avances tecnológicos y sociales y la naturaleza sin fronteras de Internet, la protección de los niños en línea debe ser dinámica y adaptativa para que resulte eficaz. Con el desarrollo de las innovaciones tecnológicas surgirán nuevos retos que variarán de una región a otra. La mejor manera de hacerles frente es trabajar juntos como una comunidad mundial, ya que es necesario encontrar nuevas soluciones a esos retos.

2.1 Antecedentes

Internet está plenamente integrada en la vida de los niños y los jóvenes, razón por la cual es imposible considerar los mundos digital y físico por separado.

La conectividad ha sido sumamente potenciadora. El mundo en línea permite a los niños y jóvenes superar las desventajas y las discapacidades, y ha proporcionado nuevos ámbitos para el entretenimiento, la educación, la participación y el establecimiento de relaciones. Las plataformas digitales actuales se utilizan para muy diversas actividades y suelen ser experiencias multimedia.

Tener acceso a esta tecnología y aprender a utilizarla y desenvolverse por ella es fundamental para el desarrollo de los jóvenes, que comienzan a utilizar las TIC a una edad temprana. Por consiguiente, es fundamental que todos los agentes sean conscientes de que los niños y jóvenes suelen empezar a utilizar las plataformas y servicios antes de alcanzar la edad mínima que se exige a la industria tecnológica y, por ende, es preciso integrar la educación en todos los servicios en línea utilizados por los niños, junto con medidas de protección.

2.1.1 Niños en el mundo digital

Acceso a Internet

En 2019, más de la mitad de la población mundial utilizaba la Internet (53,6%), estimándose la cifra en unos 4.100 millones de usuarios. A escala mundial, uno de cada tres usuarios de Internet es menor de 18 años[1]. Según el UNICEF, el 71% de los jóvenes del mundo ya están en línea[2]. A pesar de la edad mínima establecida, Ofcom (el organismo regulador de las comunicaciones del Reino Unido) estima que casi el 50% de los niños de 10 a 12 años ya tienen una cuenta en las redes sociales[3]. Los niños y jóvenes tienen ahora una presencia en Internet sustancial, permanente y constante. Internet sirve a otros fines sociales, económicos y políticos y se ha convertido en un producto o servicio para la familia o el consumidor, y ha quedado integrada en la 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 fuertemente vinculado al nivel de ingresos nacionales. El nivel de niños usuarios de Internet suele ser menor en los países de renta baja que en los de renta alta. 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 de 15 a 17 años son los que más tiempo pasan en línea, entre 2,5 y 5,3 horas, según el país.

---

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

2 Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)," *Broadband Commission for Sustainable Development,* October 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

3 BBC, "Under-age social media use 'on the rise', says Ofcom".

Utilización de Internet

El dispositivo más utilizado por los niños y jóvenes para acceder a la Internet es el teléfono móvil, seguido de las computadoras de escritorio y los portátiles. Los niños y jóvenes pasan en promedio dos horas diarias en línea durante la semana y cuatro horas al día el fin de semana. Si bien algunos se sienten permanentemente conectados, muchos otros aún no tienen acceso a la Internet en sus hogares. En la práctica, la mayoría de los niños y jóvenes que utilizan Internet acceden con diversos dispositivos, y los que se conectan al menos una vez por semana llegan a utilizar hasta tres dispositivos diferentes. Los niños de más edad y los de países más ricos suelen emplear más dispositivos, y los varones utilizan un número algo mayor de dispositivos que las niñas en todos los países estudiados.

La actividad más popular, tanto entre las niñas como entre los niños, es ver videoclips. Más de las tres cuartas partes de los niños y jóvenes que utilizan Internet aseguran ver vídeos en línea por lo menos una vez por semana, solos o en compañía de miembros de su familia. Muchos niños y jóvenes pueden considerarse "sociables activos", por cuanto utilizan diversas plataformas de medios sociales como Facebook, Twitter, Tiktok o Instagram. Los niños y los jóvenes también participan en la política en línea y hacen oír su voz en los blogs.

El nivel general de participación de niños y jóvenes en juegos en línea varía según el país y está en consonancia con la facilidad de acceso a Internet. Sin embargo, la disponibilidad y la asequibilidad de los juegos en línea evoluciona rápidamente y los niños y jóvenes comienzan a jugar en línea a una edad cada vez más temprana.

Según una encuesta realizada en un conjunto de países seleccionados, entre el 10% y el 30% de los niños y jóvenes que utilizan la Internet participan semanalmente en actividades creativas en línea[1]. Cada semana, muchos niños y jóvenes de todas las edades utilizan Internet con fines educativos, para hacer sus tareas escolares, o incluso para ponerse al día si han faltado a clases o buscar información sanitaria en línea. Los de mayor edad parecen tener un mayor afán de información que los niños más jóvenes.

[1] Livingstone, S., Kardefelt Winther, D., and Hussein, M. (2019). *Global Kids Online Comparative Report, Innocenti Research Report*. UNICEF Office of Research - Innocenti, Florence, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html.

Explotación y abuso sexual infantil en línea

La explotación y el abuso sexual infantil (EASI) en línea está aumentando a un ritmo alarmante. Hace una década el material de abuso infantil denunciado era inferior a un millón de archivos. En 2019, esa cifra había aumentado a 70 millones, con un incremento de casi el 50% con respecto a las cifras de 2018. Además, por vez primera el número de vídeos de abusos sexuales ha rebasado el número de fotos en las denuncias a las autoridades, lo que demuestra la necesidad de nuevos instrumentos para hacer frente a esta tendencia. Entre las víctimas de EASI en línea se encuentran niños de todas las edades, pero cada vez son más jóvenes. En 2018, la red INHOPE observó un cambio en los perfiles de las víctimas, que pasaron de la pubertad a la prepubertad. Además, las investigaciones realizadas por ECPAT International y la INTERPOL en 2018 revelaron que cuanto más pequeños son los niños, más probabilidades tienen de sufrir abusos graves, como torturas, violaciones violentas o sadismo. También son víctimas los bebés de sólo algunos días, semanas o meses de edad. Si bien las niñas son las más afectadas, en el caso de los niños el abuso puede resultar más grave. En el mismo informe se indica que el 80% de las víctimas mencionadas en los informes eran niñas y el 17% niños. En el 3% de los informes evaluados se mencionaron niños de ambos sexos[1].

Resumen de los datos[2]:

- Uno de cada tres usuarios de Internet es un niño.
- Cada medio segundo, un niño se incorpora al mundo en línea por vez primera.
- 800 millones de niños utilizan las redes sociales.
- En cualquier instante dado, se estima que hay 750 000 personas tratando de contactar en línea a niños con fines sexuales.
- Hay más de 46 millones de imágenes y vídeos diferentes de MASI en los archivos de la Interpol.
- Más del 89% de las víctimas tienen una edad comprendida entre 3 y 13 años.

Para más información sobre la dimensión y respuesta a la EASI, diríjase a WePROTECT Global Alliance.

1 ECPAT and Interpol, "Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: summary report", 2018.
2 End Violence Against Children, "Safe Online".

2.1.2 La incidencia de las diferentes plataformas en las experiencias digitales del niño

Internet y la tecnología digital presentan tanto oportunidades como riesgos para los niños y jóvenes. A continuación, se describen algunos de ellos.

Al utilizar las redes sociales, se abren al niño muchas oportunidades para investigar, aprender, comunicarse y desarrollar habilidades importantes. Los niños consideran que las redes sociales son plataformas que les permiten descubrir su identidad personal en un entorno seguro. Para los jóvenes es fundamental disponer de las aptitudes necesarias y saber cómo sobrellevar las cuestiones relacionadas con la privacidad y la reputación.

"Sé que todo lo que publico en Internet se queda ahí para siempre y puede afectarme en el futuro", niño de 14 años, Chile.

Sin embargo, las encuestas muestran que la mayoría de los niños utilizan las redes sociales antes de la edad mínima de 13 años y que los servicios de verificación de la edad son generalmente insuficientes o inexistentes, de modo que los riesgos que corren los niños podrían ser graves. Además, si bien los niños quieren aprender habilidades digitales, convertirse en ciudadanos digitales y controlar los parámetros de privacidad, tienden a concentrarse en la privacidad para con sus amigos y conocidos –"¿Qué pueden ver mis amigos?"– y se guardan menos de los desconocidos y terceros. Esta situación, junto con la natural curiosidad de los niños y, en general, la menor consciencia de los riesgos los hace más vulnerables a la seducción, la explotación, el acoso u otros tipos de contenidos o contactos perjudiciales.

La popularidad generalizada del intercambio de imágenes y vídeos a través de aplicaciones móviles, y en particular la utilización por los niños de plataformas de transmisión en directo aumenta los peligros y riesgos en materia de privacidad. Algunos niños producen imágenes de carácter sexual de ellos mismos, de sus amigos y hermanos y las comparten en línea. En 2019, casi un tercio (29%) de todas las páginas web clasificadas por la IWF contenían imágenes autogeneradas. De ellas, el 76% mostraba a niñas de 11 a 13 años, la mayoría de ellas en sus dormitorios o en otra habitación de su hogar. Para algunos, en particular los niños de más edad, esta forma de actuar puede considerarse como una búsqueda natural de la sexualidad e identidad sexual, mientras que, para otros, en particular los más pequeños, suele ser el resultado de la coacción por un adulto u otro niño. En cualquier caso, el contenido resultante es ilegal en muchos países, con el consecuente riesgo de enjuiciamiento del niño, o podría ser utilizado para seguir explotando, seduciendo o extorsionando al niño.

Análogamente, los juegos en línea permiten a los niños ejercer su derecho fundamental al jugar, socializar, pasar tiempo con amigos y hacer nuevas amistadas, así como a desarrollar importantes aptitudes. Estas actividades pueden ser sumamente positivas, mas sin la supervisión ni ayuda de un adulto responsable, las plataformas de juego también conllevan riesgos para los niños. Entre los riesgos se cuentan el jugar excesivamente, riesgos financieros relacionados con compras desmedidas en el juego, recopilación y monetización de datos personales del niño por los agentes de la industria, ciberacoso, discurso de odio, violencia y exposición a conductas o contenidos inapropiados, seducción, utilización de imágenes reales, generadas por computadora o incluso de realidad virtual, y vídeos que representan y normalizan el EASI. Estos riesgos no son exclusivos del entorno de los juegos, sino que se aplican a otros contextos digitales donde los niños pasan el tiempo.

Por otra parte, los adelantos tecnológicos han dado lugar a la aparición de la "Internet de las cosas", en la que son cada vez más numerosos y diversos los dispositivos conectados a Internet que se comunican e interconectan por Internet. Entre ellos figuran los juguetes, los monitores de bebés y los dispositivos basados en la inteligencia artificial, que presentan riesgos en materia de privacidad y contactos no deseados.

Buenas prácticas: Búsquedas

En el contexto de la seguridad digital y el ciberacoso, Microsoft ha realizado investigaciones sobre la seguridad digital y el ciberacoso. En 2012, realizó una encuesta a niños de 8 a 17 años de edad en 25 países sobre el comportamiento negativo en línea. Los resultados mostraron que, en promedio, el 54% de los participantes aseguraron sentirse acosados en línea; el 37% se declaró víctima de ciberacoso; y el 24% reveló haber acosado a alguien. La misma encuesta indicaba que menos tres de cada 10 padres habían mantenido conversaciones con sus hijos sobre el acoso en línea. Desde 2016, Microsoft realiza investigaciones periódicas sobre los riesgos en línea y publica informes anuales del Índice de Civismo Digital.

El programa multimedios FACES, producido por NHK Japón y por un consorcio de varias emisoras públicas, publica historias de víctimas de acoso en línea y fuera de línea en todo el mundo. Se trata de una serie de semblanzas de adolescentes en las que los protagonistas explican a la cámara cómo reaccionaron a los ataques a través de la Internet. La serie, producida también en videoclips de dos minutos, ha sido adoptada por Facebook, la UNESCO y el Consejo de Europa, y está disponible en muchos idiomas.

En 2019, UNICEF publicó un artículo sobre los derechos del niño y el juego en línea: retos y oportunidades para los niños y la industria (Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry) en el que se examinaban los retos y oportunidades para los niños en la industria del esparcimiento, que crece a gran velocidad. En el artículo se analizan los siguientes temas:

- El derecho del niño a jugar y a la libertad de expresión (tiempo que pasan jugando y cómo repercute en su salud);
- Participación no discriminatoria y protección contra abusos (interacción e inclusión social, entornos tóxicos, límites de edad y su verificación, protección contra la seducción y el abuso sexual);
- El derecho a la privacidad y a no ser explotado económicamente (modelos comerciales de acceso condicionado al suministro de datos, juegos gratuitos y monetización, falta de transparencia en el contenido comercial).

Buenas prácticas: Tecnología

El Laboratorio de Acción de Realidad Virtual de Google (Virtual Reality Action Lab) investiga cómo puede la realidad virtual instar a los jóvenes a convertirse en paladines contra el acoso en línea y fuera de línea[1].

En septiembre de 2019, la BBC lanzó una aplicación móvil llamada **Own IT**, una aplicación destinada al bienestar de los niños de 8 a 13 años que reciben su primer teléfono inteligente. La aplicación forma parte del compromiso de la BBC de apoyar a los jóvenes en el cambiante entorno mediático actual, tras el exitoso lanzamiento del sitio web de Own IT en 2018. La aplicación integra la tecnología de aprendizaje automático de última generación para hacer un seguimiento de la actividad del niño en su teléfono inteligente, con la opción de que los niños indiquen su estado emocional. Utilizando esa información, ofrece contenido e intervenciones adaptados a los niños, para mantenerlos felices y saludables en línea, ofreciendo consejos amistosos y de apoyo cuando su comportamiento se sale de la norma. Los usuarios pueden acceder a la aplicación cuando buscan ayuda, pero también está disponible para dar consejos y apoyo instantáneos en pantalla cuando lo necesiten, a través de un teclado diseñado especialmente para tal fin. Las características incluyen:

- Recordar a los usuarios que se lo piensen dos veces antes de compartir información personal como el número de móvil en las redes sociales.
- Ayudarles a comprender cómo los mensajes pueden ser percibidos por los demás, antes de pulsar el botón de enviar.
- Seguir su estado de ánimo a lo largo del tiempo y orientarles sobre cómo mejorar la situación, si fuera necesario.
- Proporcionar información sobre temas como el uso de los teléfonos a altas horas de la noche y cómo afecta al bienestar de los usuarios.

La aplicación incluye contenido especialmente encargado por la BBC. Proporciona material y recursos útiles para ayudar a los jóvenes a sacar el máximo provecho de su tiempo en línea y a crear comportamientos y hábitos saludables en la red. Ayuda a los jóvenes y a sus padres a mantener conversaciones más constructivas sobre sus experiencias en línea, pero no proporciona informes o comentarios a los padres, y los datos no salen del dispositivo del usuario. La aplicación no recaba ningún dato personal o contenido generado por el usuario, ya que todo el aprendizaje automático funciona dentro de la aplicación y dentro del dispositivo del usuario. El entrenamiento de las máquinas se efectúa por separado con datos teóricos para garantizar que no se infringe las normas de privacidad.

[1] For more information see, Alexa Hasse et al., "Youth and Cyberbullying: Another Look", Berkman Klein Center for Internet & Society, 2019.

2.1.3 La situación especial de los niños con discapacidad[4]

Los niños y jóvenes con discapacidad se enfrentan a los mismos riesgos en línea que los niños sin discapacidad, pero, además, se enfrentan a riesgos específicos relacionados con sus discapacidades. Uno de los riesgos que corren los niños y jóvenes con discapacidad es la exclusión, la estigmatización y los obstáculos (físicos, económicos, sociales y de actitud) a la hora de participar en sus comunidades. Esas experiencias pueden tener un efecto negativo en un niño con discapacidad y llevarlo a buscar interacciones sociales y amistades en espacios en línea. Si bien esas interacciones pueden ser positivas al ayudar a fomentar la autoestima y crear redes de apoyo, también pueden exponer a esos niños a un mayor riesgo de incidentes de seducción, proposiciones en línea y/o acoso sexual. Las investigaciones demuestran que los niños y jóvenes que experimentan dificultades fuera de la red y los que se ven afectados por dificultades psicosociales corren un mayor riesgo de sufrir incidentes de ese tipo[5].

En general, es probable que los niños que son víctimas fuera de la línea lo sean también en línea. Así, los niños con discapacidades corran un mayor riesgo en línea, pero también tienen mayor necesidad de pasar tiempo en línea. Según las investigaciones, los niños con discapacidad tienen más probabilidades de sufrir abusos de cualquier tipo[6], en particular de carácter sexual.[7] Pueden ser víctimas de acoso, hostigamiento, exclusión y discriminación basadas en la discapacidad real o percibida de un niño o en aspectos relacionados con su discapacidad, como la forma en que se comportan o hablan, o los equipos o los servicios que utilizan.

Entre quienes seducen, hacen proposiciones en línea y/o acosan sexualmente a niños y jóvenes con discapacidad figuran no sólo los delincuentes habituales que persiguen a niños y jóvenes, sino también los que persiguen específicamente a niños y jóvenes con discapacidad. Esos delincuentes pueden ser "obsesos", es decir, personas no discapacitadas que se sienten atraídas sexualmente por personas con discapacidad (por lo general, personas mutiladas o que utilizan prótesis), algunas de las cuales llegan incluso a fingir ser discapacitadas.[8]Las acciones de esas personas van desde descargar fotos y vídeos de niños y jóvenes con discapacidades (que son de naturaleza inocua) hasta compartir dicho material en foros especiales o cuentas de medios sociales. Los instrumentos de denuncia en los foros y medios de comunicación social no cuentan a menudo con un mecanismo adecuado para hacer frente a esas acciones.

Existe la preocupación de que el "sharenting" (padres que comparten en línea información y fotos de sus hijos) pueda vulnerar la privacidad del niño, provocar acoso, avergonzarlo o tener consecuencias negativas más adelante en la vida[9]. Hay padres de niños y jóvenes con discapacidad que comparten información o medios (fotos, vídeos) de su hijo en busca de apoyo o asesoramiento, poniendo así a su hijo en riesgo de que se vulnere su privacidad tanto en el presente como en el futuro. A esto hay que añadir el riesgo de que esos padres sean el blanco de personas desinformadas o sin escrúpulos que ofrecen tratamientos, terapias o

4 See Council of Europe, "Two clicks forward and one click back: report on children with disabilities in the digital environment", 2019.
5 Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content", Berkman Center for Internet & Society, 2008.
6 UNICEF, "State of the World's Children Report: Children with Disabilities", 2013.
7 Katrin Mueller-Johnson et al., "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors", Journal of Interpersonal Violence, 2014.
8 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", *Sexuality and Disability*, 1997.
9 UNICEF y Office of Research-Innocenti (2017), Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

"curas" para la discapacidad de su hijo. Algunos padres de niños y jóvenes con discapacidad pueden ser sobreprotectores debido a que desconocen cómo orientar a sus hijos sobre la utilización de Internet o protegerlos del acoso o el hostigamiento[10].

Algunos niños y jóvenes con discapacidades tienen dificultades para utilizar el entorno en línea, o incluso quedan excluidos porque su diseño no es accesible (por ejemplo, aplicaciones que no permiten aumentar el tamaño del texto), la imposibilidad de realizar ajustes (por ejemplo, programas de lectura de pantalla o control adaptativo del computador), o la falta de ayuda adecuada (por ejemplo, formación en el uso del equipo, ayuda personalizada para desenvolverse en interacciones sociales)[11].

2.2 Modelos nacionales y transnacionales existentes para la protección de la infancia en línea

A nivel mundial, se están adoptando varios modelos para garantizar la seguridad de los niños y jóvenes en línea. Para los interesados de la industria, estos modelos deben servir de orientación en las iniciativas internacionales y como marco para garantizar que no escatimen esfuerzos a la hora de proteger a los niños y jóvenes en línea. La industria de Internet muy diversa e intrincada, integrada por empresas de diversos tamaños y funciones. Es esencial que la protección de los niños se aborde no sólo en las plataformas y servicios basados en contenido, sino también por quienes dan soporte a la infraestructura de Internet.

Cabe señalar que la capacidad de una industria para introducir una política exhaustiva de protección de la infancia se ve limitada por los recursos de que dispone. Por consiguiente, en estas directrices se recomienda que las industrias colaboren para desplegar servicios de protección del usuario. Al compartir recursos y conocimientos técnicos de ingeniería, las industrias podrían crear "espacios seguros" más eficaces para impedir el abuso.

Cooperación industrial

La Technology Coalition es un ejemplo de cooperación industrial exitosa entre interesados para luchar contra la EASI.

Modelos transnacionales

Las industrias deben incluir las directrices internacionales pertinentes en su programa estructural, así como respetar toda la legislación nacional o transnacional pertinente aplicable en los países donde desarrollan su actividad. Las industrias no sólo deben considerar las medidas que deben adoptar en el plano jurídico, sino también las actividades que pueden realizar y, cuando sea posible, tratar de poner en práctica iniciativas a escala mundial. Algunos de los modelos que proporcionan principios para esas iniciativas son los siguientes:

- Five Country Ministerial, Voluntary principles to counter online CSEA (2020);
- Comisión de la Banda Ancha para el Desarrollo Sostenible, Seguridad de los niños en línea: Minimizando el riesgo de la violencia, el abuso y la explotación en línea (2019);
- Alianza Mundial WePROTECT, A Global Strategic Response to Online Child Sexual Exploitation and Abuse (2019);

[10] UNICEF, "Is there a ladder of children's online participation?", Innocenti Research Brief, 2019.

[11] For guidelines on these rights, see the United Nations Convention on the Rights of Persons with Disabilities and Optional Protocol, especially Article 9 on accessibility and Article 21 on freedom of expression and opinion, and access to information.

- Alianza Mundial para Acabar con la Violencia contra los Niños, Safe to Learn: Call to Action;
- La Dignidad Infantil en el Mundo Digital, Child Dignity Alliance: Technology Working Group Report (2018);
- Directiva (EU) 2018/1808 del Parlamento Europeo y del Consejo: Directiva de servicios de comunicación audiovisual;
- Reglamento General de Protección de Datos de la Comisión Europea (2018);
- Recomendación de la OCDE sobre la protección de los niños en línea (2012).

Modelos nacionales

Existen varios modelos nacionales e internacionales que establecen claramente las funciones y responsabilidades de la industria de la tecnología en lo que respecta a la protección de la infancia en línea. Algunos de estos modelos no se han concebido específicamente para niños, pero son también aplicables a éstos en tanto que usuarios de Internet. Ofrecen a la industria directrices generales sobre políticas reglamentarias, normas y colaboración con otros sectores. A los efectos del presente documento, se destacan los principios fundamentales de esos modelos, en la medida en que se aplican a la industria de las TIC.

Código para el diseño adecuado a la edad, Reino Unido

A principios de 2019, la Oficina del Comisionado de Información publicó una serie de propuestas para su código para el diseño adecuado a la edad destinado a la protección de los datos de los niños. El código propuesto se basa en el interés superior del niño, con arreglo a la Convención de las Naciones Unidas sobre los Derechos del Niño, y establece varias expectativas para la industria. El código consta de quince normas, entre las que cabe destacar, que los servicios de localización estén desactivados por defecto para los niños, que la industria reúna y conserve sólo la cantidad mínima de datos personales del niño, que los productos sean privados por diseño y que las explicaciones sean accesibles y adecuadas para la edad.

Ley de comunicaciones digitales perjudiciales, Nueva Zelandia

La Ley de 2015 tipificó el ciberabuso como un delito específico y contempla una amplia gama de daños, desde el ciberacoso hasta la pornografía de venganza. El objetivo es disuadir, prevenir y disminuir la comunicación digital perjudicial, haciendo ilegal la publicación de comunicaciones digital con la intención de causar un grave daño emocional a otra persona, y establece una serie de 10 principios de comunicación. Permite a los usuarios denunciar las agresiones a una organización independiente en caso de que se infrinjan estos principios o recurrir a dictámenes judiciales contra el autor o el anfitrión de la comunicación si el problema no se resuelve.

Comisionado eSafety, Australia

Fundado en 2015, el Comisionado eSafety es el primer organismo gubernamental del mundo dedicado a combatir el abuso en línea y a mantener a sus ciudadanos más seguros en línea. En su calidad de regulador nacional independiente de la seguridad en línea, eSafety tiene una eficaz combinación de funciones. Éstas van desde la prevención mediante la sensibilización, la educación, la investigación y la orientación sobre las mejores prácticas, hasta la intervención temprana y la reparación de daños mediante múltiples mecanismos reglamentarios que facultan a eSafety para eliminar rápidamente el ciberacoso, el abuso basado en imágenes y el contenido ilegal en línea. Este amplio cometido permite a eSafety abordar la seguridad en línea de manera polivalente, integral y proactiva.

En 2018, eSafety creó Seguridad por Diseño (*Safety by Design*, SbD), una iniciativa que sitúa la seguridad y los derechos de los usuarios en el centro del diseño, el desarrollo y el despliegue de productos y servicios en línea. La iniciativa se basa en un conjunto de principios de seguridad por diseño, en el que se establecen medidas realistas, aplicables y viables para que la industria se comprometa a proteger y salvaguardar mejor a los ciudadanos en línea. Los tres principios generales son:

1) **Responsabilidades del proveedor de servicios:** el peso de la seguridad nunca debe recaer exclusivamente en el usuario final. Es posible adoptar medidas preventivas para garantizar que en el diseño y la prestación de servicios en línea se hayan evaluado los daños conocidos y previstos, y tomado las medidas adecuadas, para reducir la probabilidad de que los servicios faciliten, exacerben o fomenten comportamientos ilícitos e impropios.
2) **Empoderamiento y autonomía del usuario:** la dignidad de los usuarios y su interés superior revisten una importancia fundamental. Se debe apoyar, ampliar y reforzar la capacidad de acción humana y la autonomía en el diseño de los servicios, permitiendo a los usuarios un mayor control, gestión y regulación de sus propias experiencias.
3) **Transparencia y responsabilidad:** son los rasgos distintivos de un planteamiento sólido de la seguridad, que ofrece garantías de que los servicios funcionan de acuerdo con los objetivos de seguridad publicados, así como la formación y empoderamiento del usuario sobre las medidas que pueden adoptarse para resolver los problemas de seguridad.

Alianza Mundial WePROTECT

La estrategia de la Alianza Mundial WePROTECT consiste en ayudar a los países para que elaboren respuestas coordinadas multipartitas que permitan hacer frente a la explotación sexual infantil en línea, basándose en su modelo de respuesta nacional, que sirve de modelo para la actuación a escala nacional. Los países pueden basarse en ese marco para luchar contra la explotación sexual infantil en línea. Dentro del Modelo de Respuesta Nacional WePROTECT, existe un claro conjunto de compromisos de las empresas de TIC relacionados con:

- procedimientos de notificación y eliminación;
- denuncias de explotación y abuso sexual infantil en línea (EASI);
- desarrollo de soluciones tecnológicas; e
- inversión en programas preventivos y servicios de respuesta eficaces de PIeL.

Alianza Mundial y Fondo para erradicar la violencia contra el niño

La Alianza Mundial y Fondo para erradicar la violencia contra el niño por el Secretario General de las Naciones Unidas en 2016 con un objetivo, a saber, catalizar y apoyar las medidas para poner fin a todas las formas de violencia contra los niños de aquí a 2030 mediante una colaboración singular de más de 400 asociados de todos los sectores.

La labor se concentra en el rescate y el apoyo a las víctimas, soluciones tecnológicas para detectar y prevenir los delitos, apoyo a las fuerzas de seguridad, reformas legislativas y normativas y generación de datos y pruebas sobre la magnitud y naturaleza de la EASI en línea, así como la comprensión de las perspectivas de los niños[12].

[12] Para más información, véase more information see End Violence Against Children, "Grantees of the End Violence Fund".

3 Ámbitos fundamentales de la protección y promoción de los derechos del niño

En esta sección se describen cinco ámbitos fundamentales en los que las empresas pueden adoptar medidas para proteger la seguridad de los niños y jóvenes cuando utilizan las TIC y promover su utilización positiva.

3.1 Integrar consideraciones relativas a los derechos del niño en todas las políticas corporativas y procesos de gestión pertinentes

Para poder integrar las consideraciones relativas a los derechos del niño es preciso que las empresas adopten medidas adecuadas para determinar, prevenir, mitigar y, si procede, remediar los efectos negativos potenciales y reales sobre los derechos del niño. En los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos se exhorta a todas las empresas e industrias a establecer políticas y procesos adecuados para cumplir con su responsabilidad de respetar los derechos humanos.

Las industrias deben prestar especial atención a los niños y los jóvenes como grupo vulnerable en lo que respecta a la protección de sus datos y la libertad de expresión. La Resolución 68/167 de la Asamblea General de las Naciones Unidas sobre el derecho a la privacidad en la era digital reafirma el derecho a la privacidad y la libertad de expresión sin ser objeto de injerencias ilícitas. Además, en la Resolución 32/13 del Consejo de Derechos Humanos de las Naciones Unidas relativa a la promoción, la protección y el disfrute de los derechos humanos en la Internet, se reconoce el carácter mundial y abierto de Internet como fuerza impulsora para acelerar el desarrollo y se afirma que los mismos derechos que tienen las personas fuera de línea también deben protegerse en línea. En los países en que no existen marcos jurídicos adecuados para la protección de los derechos de los niños y jóvenes a la privacidad y a la libertad de expresión, las empresas deben actuar con la debida diligencia para garantizar que las políticas y prácticas se ajusten al derecho internacional. Con el constante aumento de la participación cívica de jóvenes mediante las comunicaciones en línea, las empresas tienen una mayor responsabilidad de respetar los derechos de los niños y jóvenes, incluso en los casos en los que la legislación nacional todavía no se ha puesto al día con las normas internacionales.

> Las empresas deberían contar con un mecanismo de reclamación operativo en un formato para que las personas afectadas planteen sus inquietudes sobre posibles infracciones. Los mecanismos a nivel operativo deberían ser accesibles a los niños, a sus familias y a quienes representan sus intereses. El principio 31 de los Principios Rectores sobre las Empresas y los Derechos Humanos aclara que esos mecanismos deben ser legítimos, accesibles, previsibles, equitativos, transparentes, compatibles con los derechos, una fuente de aprendizaje continuo y estar basados en el compromiso y el diálogo. Junto con los procesos internos para contrarrestar los efectos negativos, los mecanismos de reclamación deben velar por que las empresas cuenten con marcos para que los niños y jóvenes dispongan de recursos adecuados cuando sus derechos se hayan visto amenazados.

Al adoptar un criterio basado en el cumplimiento de las normas de seguridad de las TIC con arreglo a la legislación nacional o, en su defecto, las pautas internacionales, y evitar las

consecuencias negativas sobre los derechos de los niños y jóvenes, las empresas fomentan proactivamente el desarrollo y bienestar de los niños y jóvenes mediante actuaciones voluntarias propicias para los derechos de los niños y jóvenes al acceso a la información, la libertad de expresión, la participación, la educación y la cultura.

Buenas prácticas: Política y diseño adecuado a la edad

La empresa de desarrollo de aplicaciones Toca Boca fabrica juguetes digitales desde la perspectiva del niño. La política de privacidad de la empresa se ha concebido para compartir qué información recaba la empresa y cómo se utiliza. Toca Boca, Inc es miembro del Programa de Certificación PRIVO Kids Privacy Assured COPPA Safe Harbor.

Otro ejemplo de plataforma de medios sociales segura es LEGO® Life para que los niños menores de 13 años puedan compartir sus creaciones LEGO, se inspiren e interactúen con toda seguridad. A los niños no se les pide ningún tipo de información personal para crear una cuenta, lo que sólo es posible con la dirección de correo electrónico de su padre o tutor. La aplicación ofrece la oportunidad a los niños y sus familias de conversar sobre la seguridad y la privacidad en línea en un entorno positivo.

Entre los ejemplos de diseño apropiado para la edad se incluyen las ofertas específicas de algunos de los principales radiodifusores públicos para ciertos grupos de edad: por ejemplo, la ARD (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland – Das Erste) y la ZDF (Zweites Deutsches Fernsehen) de Alemania se dirigen a un público mayor de 14 años, ofreciendo contenido personalizado a través del canal funk.net. La BBC (British Broadcasting Corporation) publicó CBeebies, que está dirigido a niños menores de 6 años. El contenido del sitio web se adapta específicamente a los respectivos grupos de edad.

Buenas prácticas: Política y tecnología

Twitter no deja de invertir en tecnología patentada, lo que ha contribuido a reducir de manera constante la carga de trabajo de las personas que informan[1]. Concretamente, más del 50% de los tweets, en comparación con el 20% en 2018, que Twitter tramita en respuesta a su carácter abusivo, se detectan actualmente de forma proactiva utilizando tecnología, en lugar de denuncias a Twitter. La nueva tecnología se utiliza para tramitar esferas de contenido normativo relacionado con información privada, medios sensibles, conductas de odio, abuso y suplantación de identidad.

[1] Twitter, "15th Transparency Report: Increase in proactive enforcement on accounts".

3.2 Desarrollar procesos normativos para tratar el material de abuso sexual infantil

En 2019, la IWF intervino en 132.676 páginas web en las que figuraba contenido de abuso sexual infantil[13]. Cualquier URL podría contener cientos, si no miles, de imágenes y vídeos. De las imágenes intervenidas por la IWF, el 45% mostraba niños de 10 años o menos; de éstas 1.609 páginas web eran de niños de 0 a 2 años, de las cuales el 71% contenía abusos sexuales más graves, como violaciones y torturas sexuales. Estos hechos inquietantes ponen de relieve la importancia de la colaboración entre la industria, los gobiernos, las fuerzas de seguridad y la sociedad civil para combatir el material de abuso sexual infantil (MASI).

Pese a que son muchos los gobiernos que luchan contra la difusión y distribución de MASI mediante la promulgación de leyes, la persecución y el enjuiciamiento de los delincuentes, la sensibilización y el apoyo a los niños y jóvenes para que se recuperen del abuso o la explotación, sigue habiendo muchos países que aún no cuentan con sistemas adecuados. En cada país se requieren mecanismos que permitan al ciudadano denunciar contenidos abusivos y de explotación de esta naturaleza. La industria, las fuerzas de seguridad, los gobiernos y la sociedad civil deben colaborar para garantizar que se establezcan marcos jurídicos adecuados de conformidad con las normas internacionales. Esos marcos deben tipificar como delito todas las formas de EASI, MASI inclusive, y proteger a los niños que son víctimas de ese tipo de abuso o explotación. Asimismo, estos marcos deben garantizar que los procesos de denuncia, investigación y eliminación de contenidos sean lo más eficientes posible.

La industria debe proporcionar enlaces a las líneas telefónicas de urgencia nacionales u otras líneas de urgencia disponibles localmente, como los portales de la IWF en algunos países y, en su defecto, proporcionar enlaces a otras líneas de urgencia internacionales que sean pertinentes, como el Centro Nacional para Menores Desaparecidos y Explotados (NCMEC) de Estados Unidos o la Asociación Internacional de Líneas de Denuncia por Internet (INHOPE), en las que se puede utilizar cualquiera de las líneas de urgencia internacionales para efectuar una denuncia.

Las empresas responsables están adoptando una serie de medidas para ayudar a impedir que sus redes y servicios se utilicen para divulgar MASI. Entre estas medidas figura la introducción de texto en los términos y condiciones o códigos de conducta que prohíba explícitamente ese contenido o conducta[14]; la implantación de procesos eficaces de denuncia y eliminación; y el apoyo y la colaboración con las líneas telefónicas directas nacionales.

Por otra parte, algunas empresas despliegan medidas técnicas para evitar el uso indebido de sus servicios o redes para compartir MASI conocido. Por ejemplo, algunos proveedores de servicios de Internet bloquean el acceso a los URL que contienen MASI, confirmado por una autoridad competente, si el sitio web está hospedado en un país en el que no existen procesos para garantizar su rápida eliminación. Otras están desplegando tecnologías de identificación numérica (*hashing*) para detectar y eliminar automáticamente las imágenes de abuso sexual de niños que ya son conocidas por las fuerzas de seguridad o por las líneas telefónicas directas. Los miembros de la industria deben considerar e incorporar todos los servicios pertinentes en sus operaciones para impedir la difusión de los abusos sexuales infantil.

---

13 IWF, "The why. The how. The who. And the results. Annual Report 2019".

14 Cabe señalar que la conducta improcedente del usuario no se limita al MASI y que cualquier tipo de conducta o contenido improcedente debe ser debidamente gestionado por la empresa.

Los agentes de la industria deben comprometerse a asignar recursos proporcionales y seguir desarrollando y compartiendo soluciones tecnológicas, preferiblemente de código abierto, para detectar y eliminar todo MASI.

Buenas prácticas: Tecnología

Microsoft aplica una solución cuádruple para fomentar el uso responsable y seguro de la tecnología, centrándose en la tecnología propiamente dicha, la autogestión, las asociaciones y la educación y divulgación del consumidor. Microsoft también ha incorporado características que ayudan a aprender cómo autogestionar más eficazmente la seguridad en línea. La "seguridad familiar" es una de esas características, que permite a los padres y tutores vigilar el uso de la Internet por sus hijos.

Microsoft aplica políticas contra el acoso en sus plataformas y los usuarios que infringen estas normas se exponen a que se les elimine la cuenta y, en caso de infracciones más graves, a medidas legales.

Microsoft PhotoDNA es una herramienta que crea identificadores numéricos (*hashes*) a partir de imágenes y los compara con una base de datos de *hashes* ya identificados y confirmados como MASI. Cuando encuentra una coincidencia, la imagen se bloquea. Esta herramienta ha permitido a los proveedores de contenido eliminar de Internet millones de fotografías ilícitas, ha ayudado a condenar a depredadores sexuales de niños y, en algunos casos, ha ayudado a las fuerzas de seguridad a rescatar a posibles víctimas antes de que sufrieran daños físicos. Microsoft se ha comprometido desde hace mucho tiempo a proteger a sus clientes del contenido ilícitos en sus productos y servicios, y la aplicación de la tecnología creada por la empresa para combatir este aumento de vídeos ilícitos era el siguiente paso lógico. Sin embargo, esta herramienta no emplea tecnología de reconocimiento facial, ni puede identificar a la persona u objeto en la imagen. Ahora bien, con la invención del PhotoDNA para vídeo, se ha dado un nuevo giro. PhotoDNA para Vídeo descompone un vídeo en cuadros fundamentales y crea *hashes* para esas capturas de pantalla. Asimismo, PhotoDNA puede detectar concordancias con una imagen que ha sido alterada para evitar su detección, PhotoDNA para Vídeo puede encontrar contenido de explotación sexual infantil que ha sido editado o empalmado en un vídeo que de otra manera podría parecer inofensivo.

Además, Microsoft ha lanzado recientemente una nueva herramienta para identificar a depredadores que seducen niños en los chats en línea para abusar de ellos. El Proyecto Artemis, desarrollado en colaboración con The Meet Group, Roblox, Kik y Thorn, se basa en la tecnología patentada de Microsoft y se pondrá a disposición gratuitamente a través de Thorn a las empresas de servicios en línea cualificadas que ofrecen la función de chat. El Proyecto Artemis es una herramienta tecnológica que ayuda a elevar las banderas rojas a los administradores cuando se necesita moderación en las salas de chat. Con esta técnica de detección de depredadores, será posible identificar, localizar y denunciar a los depredadores que intentan engatusar a los niños con fines sexuales.

La Fundación **IWF** ofrece una gama de servicios a los miembros de la industria para proteger a sus usuarios evitando que se topen con MAIS, entre los que cabe destacar:

- Lista de bloqueo dinámico de URL y de calidad garantizada de transmisiones en directo;
- Lista de *hash* de contenido ilícito conocido relacionado con MAIS;
- Lista de de términos crípticos conocidos que se utilizan en el contexto de MAIS;
- Lista de detalles de nombres de dominio que se sabe que hospedan contenido de abuso sexual infantil para permitir la rápida eliminación de los dominios que albergan dicho contenido ilícito.

3.3 Crear un entorno en línea más seguro y apropiado en función de la edad

Muy pocas cosas en la vida pueden considerarse absolutamente seguras y sin riesgos todo el tiempo. Los accidentes siguen ocurriendo pese a que en las ciudades el tráfico está muy regulado y estrechamente controlado. Por la misma razón, el ciberespacio no está exento de riesgos, especialmente para los niños y los jóvenes. Se puede pensar en los niños y los jóvenes como receptores, participantes y actores en su entorno en línea. Los riesgos a los que se enfrentan pueden clasificarse en cuatro categorías[15]:

- *contenido impropio* – Los niños y jóvenes pueden toparse con contenido inadecuado e ilícito al realizar búsquedas y pulsar un enlace aparentemente inocuo en un mensaje instantáneo o en un blog, o al compartir archivos. También pueden buscar y compartir material inapropiado o sensible para su edad. Lo que se considera contenido perjudicial varía de un país a otro; por ejemplo, el contenido que promueve el abuso de estupefacientes, el odio racial, el comportamiento arriesgado, el suicidio, la anorexia o la violencia.
- *conducta improcedente* – Los niños y los adultos pueden utilizar Internet para acosar o incluso explotar a otras personas. A veces los niños pueden formular comentarios ofensivos o publicar imágenes embarazosas, o bien pueden robar contenidos o infringir los derechos de autor.
- *contactos inadecuados* – Adultos y jóvenes pueden utilizar Internet para buscar niños u otros jóvenes vulnerables. Con frecuencia, su objetivo es convencer al niño de que han creado una relación seria, pero su finalidad subyacente es la manipulación. A veces tratan de persuadir al niño de que realice actos sexuales u otros actos abusivos en línea,

[15] Sonia Livingstone et al., "EU Kids Online: Final Report", London school of economics, 2009.

utilizando una cámara web u otro dispositivo de grabación, o bien tratan de encontrarse en persona y tener contacto físico. Este proceso se denomina a menudo "seducción".

- *riesgos comerciales* – Esta categoría se refiere a los riesgos para la privacidad de los datos relacionados con la recopilación y utilización de datos sobre niños, así como con la comercialización digital. La seguridad en línea es un reto para la comunidad y una oportunidad para que la industria, los gobiernos y la sociedad civil colaboren para establecer principios y prácticas en materia de seguridad. La industria puede ofrecer una serie de métodos, instrumentos y servicios técnicos para los padres, niños y jóvenes, y debería ante todo crear productos que sean fáciles de usar, seguros por su diseño y apropiados para la edad de su amplia gama de usuarios. Entre otros métodos cabe citar las herramientas para elaborar sistemas adecuados de verificación de la edad que respeten los derechos del niño a la privacidad y al acceso, impongan a los niños y jóvenes restricciones de acceso a contenidos impropios para su edad, y restrinjan las personas con las que los niños puedan tener contacto, así como los horarios en los que pueden conectarse en línea. Lo más importante es incorporar los marcos de "seguridad por diseño"[16], incluida la privacidad, en los procesos de innovación y diseño de productos. La seguridad del niño y el uso responsable de la tecnología deben tenerse debidamente en cuenta y no tratar de remediarse a posterior.

Algunos programas permiten a los padres supervisar los mensajes de texto y otras comunicaciones que sus hijos y jóvenes envían y reciben. En caso de utilizar programas de este tipo, es importante hablarlo abiertamente con el niño para que no sienta que se le está "espiando", lo que podría socavar la confianza dentro de la familia.

Las políticas relativas al uso aceptable son una forma mediante la cual las empresas pueden fomentar un tipo de comportamiento específico, tanto de adultos como de niños, y definir qué tipos de actividades resultan inaceptables y las consecuencias de incumplir esas políticas. Se debe ofrecer mecanismos de información claros y transparentes a los usuarios que tengan inquietudes sobre el contenido y el comportamiento en línea. Además, se debe dar debido seguimiento a todas las denuncias, suministrando la información oportuna sobre el procedimiento. Aunque la aplicación de los mecanismos de seguimiento puede variar en función del caso, es esencial establecer un plazo claro para las respuestas, comunicar la decisión adoptada en relación con la denuncia y ofrecer un método de seguimiento si el usuario no queda satisfecho con la respuesta.

[16] Comisionado de eSafety, Safety by Design Overview, 2019.

Buenas prácticas: Denuncia

Facebook, en un esfuerzo por frenar el acoso sexual en las plataformas digitales, ha cofinanciado el proyecto deSHAME con la Unión Europea, una colaboración entre Childnet, Save the Children, Kek Vonal y UCLan. Este proyecto tiene por objeto aumentar las denuncias de acoso sexual en línea entre menores y mejorar la cooperación multisectorial para prevenir y responder a este tipo de comportamiento.

Dado que uno de los principales objetivos del proyecto es instar a los usuarios a denunciar el contenido que resulta ofensivo o inapropiado, las Reglas de la Comunidad de Facebook también son pertinentes para saber lo que está y no está permitido en Facebook. También describen los tipos de usuarios a los que no permite publicar. Facebook también ha creado funciones de seguridad como la función "¿Conoces a esta persona?"; una bandeja de entrada "otros" que recoge los nuevos mensajes de personas que el usuario no conoce; y una ventana emergente que aparece en el canal de noticias si parece que un adulto está contactando con un menor que no conoce.

Los proveedores de contenido y servicios en línea también pueden describir la naturaleza del contenido o los servicios que prestan y el grupo de edad al que se dirigen. Estas descripciones deben ajustarse a las normas nacionales e internacionales vigentes, a los reglamentos pertinentes y al criterio de los órganos de clasificación pertinentes en materia de comercialización y publicidad dirigida a los niños. Sin embargo, este proceso se hace más difícil con la creciente gama de servicios interactivos que permiten la publicación de contenido generado por el usuario, por ejemplo, en foros de mensajes, salas de chat y servicios de redes sociales. Cuando las empresas se dirigen específicamente a los niños y jóvenes, y cuando los servicios se dirigen sobre todo a un público más joven, las expectativas en cuanto al contenido y la seguridad en términos de **facilidad de uso, de comprensión y de acceso** serán mucho mayores.

Por otra parte, se insta a las empresas a que adopten las normas de privacidad más estrictas en lo que respecta a la recopilación, procesamiento y almacenamiento de datos sobre niños y jóvenes, u obtenidos de ellos, por cuanto éstos carecen de la madurez necesaria para ser conscientes de las consecuencias sociales y personales más amplias que conlleva revelar o aceptar que se comparta su información personal en línea, o de utilizarla con fines comerciales. Los servicios dirigidos principalmente a niños y jóvenes, o que puedan atraer su atención, deben tener en cuenta los riesgos que les plantea el acceso a la información personal (incluida la localización), o la recopilación y uso de esa información, y garantizar que esos riesgos se tienen debidamente en cuenta y que los usuarios reciben información al respecto. En particular, las empresas deben garantizar que el lenguaje y estilo sean claros y accesibles en todo material o comunicación utilizado para promover servicios y proporcionar acceso a los mismos, o mediante el cual se acceda, recopile y utilice información personal, para ayudar a comprender y gestionar su privacidad de manera clara y sencilla, y para explicar qué es exactamente lo que están consintiendo.

Buenas prácticas: Innovación

En 2018-2019 la Oficina Regional de UNICEF para Asia Oriental y el Pacífico organizó cinco mesas redondas multipartitas para compartir las prácticas prometedoras de la industria en relación con impedir la EASI en línea. Participaron importantes empresas del sector privado, como Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Mongolia) Mobifone+ (Viet Nam), Globe Telecom (Filipinas), True (Tailandia), GSMA y asociados de la sociedad civil, entre ellos INHOPE, ECPAT International y Child Helpline International.

En el marco de este proyecto, UNICEF puso en marcha en febrero de 2020 un grupo de reflexión para acelerar el liderazgo de la industria en la región del Asia oriental y el Pacífico, con el fin de impedir la violencia contra los niños en el mundo en línea. El grupo de reflexión es una incubadora de ideas e innovación, que aprovecha la perspectiva única de los agentes industriales (creación de productos, comercialización, etc.) para elaborar materiales didácticos impactantes e identificar las plataformas para divulgarlos más eficaces, así como para crear un marco de evaluación que permita medir la incidencia de esos materiales didácticos y de los mensajes dirigidos a los niños. El grupo de reflexión está integrado por Facebook, Telenor, expertos académicos, organismos de las Naciones Unidas, como la UIT, la UNESCO y la UNODC, y otros, como el Comisionado de Seguridad Electrónica de Australia, ECPAT International, el ICMEC, la INTERPOL y el Fondo Mundial para Erradicar la Violencia. La reunión inaugural del grupo de reflexión, celebrada con ocasión de la Conferencia Regional de la ASEAN sobre la protección de los niños en línea, congregó a expertos, como Microsoft, para estudiar las posibilidades tecnológicas y de investigación para adaptarse de la mejor manera posible a los cambios en el comportamiento en línea, basándose en la adopción de materiales y mensajes de seguridad en línea.

3.4 Educar a los niños, tutores y educadores sobre la seguridad de los niños y la utilización responsable de las TIC

Las medidas técnicas constituyen una parte importante para garantizar la protección de los niños y jóvenes contra los posibles riesgos en línea, pero sólo son un elemento de la ecuación. Los instrumentos de control parental, la sensibilización y la educación son también componentes fundamentales que ayudarán a empoderar e informar a los niños y jóvenes de todas las edades, así como a los padres, tutores y educadores. Aunque las empresas desempeñan un papel importante a la hora de fomentar la utilización responsable y segura de las TIC por los niños y jóvenes, también es responsabilidad de los padres, las escuelas y los propios niños y jóvenes.

Muchas empresas están invirtiendo en programas educativos destinados a que los usuarios puedan tomar decisiones informadas sobre el contenido y los servicios. Las empresas están ayudando a los padres, tutores y educadores a orientar a los niños y jóvenes hacia experiencias con el móvil y en línea más seguras, responsables y adecuadas. Esto incluye avisos sobre la edad recomendada para el contenido y e información clara sobre aspectos como el precio del contenido, las condiciones de suscripción y cómo cancelarla. Asimismo, fomentar que se cumpla el requisito de edad mínima para participar en redes sociales en todos los países en los que es posible verificar la edad también contribuirá a proteger a los niños, por cuanto

no se les permitirá acceder a los servicios hasta que no tengan una edad adecuada. Otro aspecto importante a tener en cuenta junto con esta recomendación es la recopilación de datos personales adicionales que ello puede entrañar y la necesidad de limitar la recopilación y almacenamiento de esta información, así como su procesamiento.

Por otra parte, es importante proporcionar información directamente a los niños y jóvenes sobre la utilización segura de las TIC y el comportamiento positivo y responsable. Además de sensibilizar sobre la seguridad, las empresas pueden facilitar que los niños y jóvenes tengan experiencias positivas desarrollando contenidos para niños y jóvenes sobre cómo ser respetuosos, amables y abiertos al utilizar las TIC y cómo cuidar de los amigos. También pueden informar sobre las medidas que deben adoptarse en caso de que tengan experiencias negativas, como el acoso o seducción en línea, para facilitar así la denuncia de esos incidentes y ofrecer la opción de no recibir mensajes anónimos.

A veces los padres conocen y comprenden menos de Internet y de los dispositivos móviles que los niños y jóvenes. Además, la convergencia de dispositivos móviles y servicios de Internet dificulta a los padres la tarea de supervisión. La industria puede colaborar con el gobierno y los educadores para reforzar la capacidad de los padres para apoyar a sus hijos a aumentar su resiliencia digital y actuar como ciudadanos digitales responsables. El objetivo no es transferir a los padres la responsabilidad de cómo utilizan las TIC los niños y jóvenes, sino más bien reconocer que los padres están en mejores condiciones de decidir lo que es apropiado para sus hijos y que deben ser conscientes de todos los riesgos para poder proteger mejor a sus hijos y ayudarles a tomar medidas.

La información puede transmitirse en línea y fuera de línea a través de distintos canales de medios, habida cuenta de que hay padres que no utilizan los servicios de Internet. Es importante colaborar con las escuelas para ofrecer programas de formación sobre la seguridad en línea y utilización responsable de las TIC para niños y jóvenes, así como material educativo para los padres. Entre los ejemplos cabe citar la explicación de los tipos de servicios y opciones disponibles para las actividades de vigilancia, las medidas que deben adoptar si un niño experimenta acoso o seducción en línea, cómo evitar el correo basura y de gestionar las configuraciones de privacidad, y la forma de hablar con niños y niñas de diferentes grupos de edad sobre cuestiones delicadas. La comunicación es un proceso bidireccional y muchas empresas ofrecen opciones para que los clientes se pongan en contacto con ellas a fin de informarse o discutir sobre ciertas cuestiones o inquietudes.

A medida que mejoran los servicios y el contenido, los usuarios seguirán recibiendo consejos y recordatorios sobre la naturaleza del servicio que están utilizando y sobre cómo hacerlo de manera segura. Si bien es importante enseñar a los niños a utilizar Internet de manera responsable, sabemos que a los niños les gusta experimentar, correr riesgos, son intrínsecamente curiosos y no siempre toman las mejores decisiones. Darles la oportunidad de actuar por sí mismos contribuye a su crecimiento y es una forma saludable de ayudarles a desarrollar su autonomía y resiliencia, siempre que el golpe no sea demasiado duro. Si bien se debe permitir que los niños asuman algunos riesgos en el entorno en línea, es fundamental que los padres y empresas puedan apoyarlos cuando surge algún problema, por cuanto de esta manera podrán convertir la mala experiencia en una lección útil para el futuro.

Buenas prácticas: Educación

NHK Japón lleva a cabo una campaña de prevención de suicidios para jóvenes en Twitter: En Japón, los suicidios de adolescentes alcanzan su punto máximo cuando vuelven a la escuela después de las vacaciones de verano. Se dice que el regreso a la realidad es la razón de ese aumento. El equipo de producción de NHK Heart Net TV (NHK Japón) produce el programa multimedia #En la noche del 31 de agosto. Se emite simultáneamente por televisión, en transmisión secuencial (streaming) en directo y por los medios sociales, NKH ha creado con éxito un "lugar" donde los adolescentes podían compartir sus sentimientos sin miedo.

Twitter también ha publicado una guía para educadores sobre la formación en el uso de los medios. El manual, elaborado en colaboración con la UNESCO, tiene como principal objetivo ayudar a los educadores a dotar a las generaciones más jóvenes de conocimientos sobre los medios. Otro aspecto de la labor de Twitter en materia de seguridad se refiere a sus operaciones de divulgación de información. Se trata de un archivo de operaciones de información respaldadas por el Estado, que Twitter comparte públicamente. La iniciativa se puso en marcha para facilitar a los círculos académicos y al público la comprensión de las campañas relacionadas con este tema en todo el mundo, y para permitir un control independiente, por parte de terceros, de estas tácticas en la plataforma de Twitter.

El **proyecto deSHAME**, cofinanciado por Facebook y la Unión Europea, también facilita la creación de recursos para muy diversos grupos de edad, en particular para niños de 9 a 13 años. Como parte del proyecto, se ha elaborado un conjunto de instrumentos denominado "Step Up, Speak Up!", en el que se ofrece una serie de cursos, formación y materiales didácticos, así como instrumentos prácticos para estrategias multisectoriales de prevención y respuesta. El proyecto transferirá esos materiales didácticos a otros países europeos y a asociados de todo el mundo a fin de promover los derechos digitales de los jóvenes.

Buenas prácticas: Educación

Google ha desarrollado una serie de iniciativas, recursos y herramientas educativas para ayudar a promover la seguridad en línea de los jóvenes. Una de ellas es la campaña Be Internet Awesome en torno a la ciudadanía digital, creada en colaboración con organizaciones como ConnectSafely, el Family Online Safety Institute y la Internet Keep Safe Coalition. Esta campaña está dirigida a jóvenes de 8 a 11 años de edad. Incluye un juego por la web para jóvenes (Interland) que enseña los rudimentos de la seguridad digital y recursos para educadores, como el programa de civismo digital y seguridad. El Plan de estudios sobre seguridad ofrece cursos sobre las cinco áreas temáticas fundamentales de la campaña, una de las cuales se centra en el ciberacoso. Además, Google ha creado un curso en línea sobre civismo digital y seguridad para educadores de todas las edades, con el fin de fomentar la integración del civismo digital y las actividades sobre seguridad en las escuelas. Google también ofrece varios programas para ayudar a que los jóvenes participen directamente en las actividades de seguridad y civismo digital en línea. La iniciativa mundial Web Rangers es uno de esos programas que enseña a los jóvenes sobre la seguridad en línea y los alienta a diseñar sus propias campañas acerca del uso positivo y seguro de Internet. También hay programas específicos para los jóvenes de cada país, como los programas Ciudadanos de Internet y Leyendas de Internet en el Reino Unido, puestos en marcha por Google.

En la **Central de Noticias para Jóvenes de Eurovisión**, la Unión Europea de Radiodifusión reúne a 15 emisoras de televisión europeas para compartir programas, formatos y soluciones en línea y fuera de línea. En los últimos años, la enseñanza de conocimientos digitales y la alerta de los riesgos en Internet se han convertido en temas centrales de sus programas. Entre las iniciativas más exitosas de los últimos años figuran los anuncios en las redes sociales y los programas de noticias adecuados para los niños producidos por Super y Ultra nytt de NRK, la emisora pública de Noruega.

Buenas prácticas: Alianzas estratégicas

En el marco de un proyecto respaldado por el Fondo para erradicar la violencia contra los niños, Capital Humano y Social Alternativo se asoció en 2008 con Telefónica, el mayor proveedor de servicios Internet, cable y telefonía en Perú, con una cartera de 14,4 millones de clientes, incluidos más de 8 millones de usuarios de Movistar móvil.

En el marco de esta fructífera alianza se llevaron a cabo varias actividades, a saber:

- **Curso virtual sobre la protección de la infancia en línea**, preparado por Telefónica con el apoyo técnico de Capital Humano y Social Alternativo. Este curso ya está disponible en la página web de Telefónica y la compañía está haciendo un seguimiento del número de personas que se inscriben y completan con éxito el curso. El Ministerio de Educación peruano aceptó dar acceso a este curso virtual a través de su página web oficial.
- **Folleto sobre seguridad en Internet,** creado por Capital Humano y Social Alternativo y distribuido por Telefónica en sus más de 300 puntos de venta de telefonía móvil. El objetivo es sensibilizar a los clientes de Telefónica acerca de la seguridad en la red y los riesgos que conlleve la EASI en línea.
- **Juego interactivo sobre la seguridad en Internet,** elaborado por Telefónica con el apoyo técnico de Capital Humano y Social Alternativo, al que los clientes pueden jugar mientras esperan su turno en las tiendas de Telefónica.

Tras el éxito de su alianza con Telefónica, Capital Humano y Social Alternativo se ha asociado con **Econocable**, un proveedor de servicios Internet y cable que desempeña sus actividades en zonas remotas y de renta baja de Perú.

3.5 Promover la tecnología digital como mecanismo para desarrollar el civismo

El Artículo 13 de la Convención de las Naciones Unidas sobre los Derechos del Niño establece que "el niño tiene derecho a la libertad de expresión; este derecho incluirá la libertad de buscar, recibir y difundir informaciones e ideas de todo tipo, sin consideración de fronteras, ya sea oralmente, por escrito o impresas, en forma artística, o por cualquier otro medio elegido por el niño". Las empresas pueden cumplir su obligación de respetar los derechos civiles y políticos de los niños y jóvenes al garantizar que la tecnología y la aplicación de la legislación y las políticas elaboradas para proteger a los niños y jóvenes de los daños en línea no tengan por consecuencia suprimir de manera imprevista su derecho a participación y manifestar su opinión o les impida acceder a información importante para su bienestar. Es fundamental garantizar que los sistemas de verificación de la edad no menoscaben el acceso por determinados grupos de edad a contenidos imprescindibles para su desarrollo.

Por otra parte, las empresas e industrias también pueden promover los derechos de los niños y jóvenes mediante la promoción de mecanismos e instrumentos que faciliten su participación. Pueden hacer hincapié en la capacidad de Internet para propiciar la participación positiva en una vida cívica más amplia, impulsar el progreso social e influir en la sostenibilidad y resiliencia de las comunidades, por ejemplo, participando en campañas sociales y ambientales y haciendo que los responsables rindan cuentas. Con los instrumentos y la información adecuados, los niños y los jóvenes están en mejores condiciones de acceder a las oportunidades de atención sanitaria, educación y empleo, y de manifestar sus opiniones y necesidades en las escuelas,

las comunidades y los países. Se les habilita para acceder a información sobre sus derechos y buscar información sobre cuestiones que les afectan personalmente, como su salud sexual, y sobre la responsabilidad política y gubernamental.

Las empresas también pueden invertir en la creación de experiencias en línea aptas para niños, jóvenes y las familias. Pueden promover el desarrollo de tecnología y contenidos que insten y permitan a los niños y jóvenes aprender, innovar y crear soluciones. Siempre deben tener en cuenta en sus productos la seguridad por diseño.

Por otra parte, las empresas pueden fomentar proactivamente los derechos de los niños y jóvenes mediante esfuerzos destinados a colmar la brecha digital. Para que los niños y jóvenes puedan participar, necesitan disponer de una formación digital, es decir, estar capacitados para comprender e interactuar en el mundo digital. Sin esa capacidad, los ciudadanos no pueden participar en muchas de las funciones sociales que se han digitalizado, como la declaración fiscal, el apoyo a candidatos políticos, la firma de peticiones en línea, la inscripción de un nacimiento o simplemente el acceso a información comercial, sanitaria, educativa o cultural. Si no se adoptan medidas, seguirá aumentando la brecha entre los ciudadanos que pueden acceder a esos foros y los que no, debido a la falta de acceso a la Internet o a la falta de conocimientos informáticos, situando a estos últimos en una situación de considerable desventaja. Las empresas pueden apoyar iniciativas multimedios para fomentar los conocimientos digitales que los niños y jóvenes necesitan para ser ciudadanos seguros, conectados y activamente implicados [17]. En muchos países, la formación digital y en materia de medios, así como los esfuerzos por colmar la brecha digital, ha pasado recientemente a formar parte de la función de los medios públicos. El Parlamento italiano, por ejemplo, ha propuesto que entre las prioridades de la televisión nacional figure la de cerrar la brecha digital y garantizar la protección de los niños, tanto en línea como en el mundo real, ejemplo que podría ser seguido por otros países.

Buenas prácticas: Colaboración interinstitucional

Microsoft se ha unido recientemente a la campaña mundial Power of ZERO, liderada por la organización No Bully, que tiene como objetivo ayudar a los niños pequeños, y a los adultos que los tutelan, a aprender a utilizar correctamente la tecnología digital y a desarrollar la voz, la compasión y la inclusión que son el alma del civismo digital. La iniciativa ofrece a los primeros educadores (la campaña está dirigida a niños de 8 años o menos) y a las familias material didáctico gratuito para ayudar a los niños pequeños a cultivar los "12 poderes para el bien" (los 12 "poderes" o aptitudes prácticas para la vida de *Power of Zero*, para que los niños puedan desenvolverse con éxito tanto en el mundo en línea como fuera de línea, incluida la resiliencia, el respeto, la inclusión y la creatividad) y sentar fundamentos sólidos desde una edad temprana.

[17] Para ejemplos de participación joven desde la comunidad móvil, véase este enlace.

4 Directrices generales para la industria

En el Cuadro 1 se presentan las directrices generales para la industria a fin de determinar, prevenir y mitigar cualquier efecto negativo de los productos y servicios sobre los derechos de los niños y jóvenes, y para promover la utilización positiva de las TIC por los niños y jóvenes.

Obsérvese que no todos los pasos enumerados en el Cuadro 1 resultarán adecuados para todas las empresas y servicios, ni tampoco figuran en ese Cuadro todos los pasos necesarios para cada servicio. Las directrices generales para la industria se complementan con las listas de prestaciones específicas (véase la sección 5) y viceversa. Las listas de prestaciones específicas de los Cuadros 2-5 indican los pasos adicionales más relevantes para cada servicio. Obsérvese que puede haber solapamientos en las listas de prestaciones específicas y que para un mismo servicio puede resultar pertinente varias listas.

Cuadro 1: Directrices generales para el sector

Tener en cuenta los derechos del menor en todas las políticas corporativas y procesos de gestión	Las empresas pueden detectar, prevenir y reducir las consecuencias negativas de las TIC en los derechos de los niños y jóvenes, y descubrir oportunidades para promover esos derechos. Para ello pueden:
	Designar a una persona y/o equipo para que se encargue del proceso y pueda comunicarse con las partes interesadas necesarias, internas o externas. Autorizar a esa persona o equipo a tomar el mando de las actividades destinadas a dar a conocer la cuestión de la protección de la infancia en línea en la empresa.
	Elaborar una política de protección y salvaguarda del menor y/o tener en cuenta los posibles riesgos y oportunidades relativos a los derechos de los niños y jóvenes en los compromisos que se establecen en la política de empresa (por ejemplo, derechos humanos, privacidad, mercadotecnia y códigos relevantes de conducta).
	Incorporar la debida diligencia en cuestiones de Protección de la Infancia en Línea (PIeL) en los vigentes marcos de evaluación de riesgos o de derechos humanos (a nivel corporativo, de producto o tecnología y/o nacional) para determinar si la empresa o el sector, con sus actividades, está causando daños o contribuyendo a que se produzcan daños, o si los daños están directamente vinculados con sus operaciones, productos o servicios, o sus relaciones empresariales.
	Descubrir los daños que se producen en los derechos de niños y jóvenes, en función de los diferentes grupos de edad, como consecuencia de las operaciones empresariales y del diseño, desarrollo e introducción de productos y servicios, y encontrar oportunidades para promover esos derechos.

Tener en cuenta los derechos del menor en todas las políticas corporativas y procesos de gestión (cont.)	Fomentar la educación y el empoderamiento para proteger al menor. Reconocer los derechos de protección de datos del menor, su derecho a la privacidad y su libertad de opinión, al tiempo que se ofrece educación y orientación mediante los servicios de la empresa. Aprovechar la competencia técnica interna y externa y consultar a las partes interesadas clave, incluidos niños y jóvenes, sobre los mecanismos de seguridad en línea con miras a conocer su opinión en todo momento y obtener orientaciones sobre cómo debe actuar la empresa.
	En aquellos países en los que no haya marcos jurídicos adecuados para proteger el derecho de los niños y jóvenes a la privacidad y libertad de opinión, las empresas deberán velar por que se apliquen políticas y prácticas conforme a normas internacionales. Véase la Resolución 68/167 de la Asamblea General de las Naciones Unidas sobre el derecho a la privacidad en la era digital.
	Velar por que haya mecanismos para presentar quejas y denuncias a nivel operacional en relación con cualquier violación de derechos del menor (por ejemplo, pornografía infantil, contenidos o contactos inapropiados o violaciones de la privacidad)
	Nombrar a un gestor de las políticas de protección del menor o a otra persona con la que se pueda contactar para cuestiones relativas a la PIeL. Si existe el riesgo de que un menor sufra algún daño, el gestor de las políticas de protección del menor deberá informar inmediatamente a las autoridades pertinentes. En las directrices editoriales de la BBC de 2019, por ejemplo, se indica que es obligatorio en los medios de comunicación públicos nombrar a un gestor de políticas de protección del menor.
Desarrollar normas del sector para proteger a los niños en línea	Elaborar y aplicar normas de protección de niños y jóvenes para la empresa y el sector, teniendo en cuenta las condiciones propias de este.
Elaborar procesos normalizados para la pornografía infantil	En colaboración con el gobierno, los organismos encargados de hacer cumplir la ley, la sociedad civil y las organizaciones de líneas telefónicas de protección del menor, el sector tiene un papel fundamental en la lucha contra la pornografía infantil. Para ello puede:
	Prohibir subir, publicar, enviar, compartir u ofrecer contenidos que violen los derechos de cualquier persona o que infrinjan cualquier ley local, estatal, nacional o internacional.

	Hacer que los proveedores de servicios de contenidos informen a los organismos nacionales encargados de que se cumpla la ley, o a la(s) línea(s) telefónica(s) nacional(es) de protección del menor, de la existencia de contenidos de pornografía infantil tan pronto como tengan conocimiento de ellos. Velar por que se apliquen procedimientos internos para cumplir la obligación de presentar información en virtud de las leyes locales e internacionales. Si una empresa opera en mercados menos reglamentados y supervisados en lo relativo a esa cuestión, puede remitir a las personas que deseen presentar una denuncia a la International Association of Internet Hotlines (INHOPE), a través de la cual podrán formalizar la denuncia en cualquier línea telefónica del mundo de protección del menor.
Elaborar procesos normalizados para la pornografía infantil **(*cont.*)**	Establecer procedimientos internos para cumplir las leyes locales e internacionales de lucha contra la pornografía infantil. Crear un puesto de rango superior o un equipo con la misión de incorporar esos procedimientos en la organización. A continuación, los miembros del sector deberán informar de las medidas tomadas y los resultados obtenidos por sus equipos en los informes de sostenibilidad e informes corporativos anuales. Cuando los reglamentos nacionales no proporcionen suficiente protección, las empresas deberán ser más escrupulosas que la legislación nacional y aprovechar su posición para abogar por que se produzcan cambios legislativos que permitan al sector luchar contra la pornografía infantil. Deberá crearse un puesto de rango superior o un equipo en la organización para que incorpore esos procedimientos y supervise las operaciones. Todo eso deberá reflejarse de forma transparente en los informes corporativos y de sostenibilidad anuales y estar a disposición del público.
	Indicar que la empresa cooperará plenamente en las posibles investigaciones de los organismos responsables de hacer cumplir la ley que pudieran producirse si se denunciase o descubriese contenido ilegal e informar de las posibles sanciones, como multas o cancelación de privilegios fiscales.
	Utilizar reglamentos para el usuario y/o políticas de uso aceptables en las que se indique claramente la posición de la empresa cuando se utilicen indebidamente sus servicios para almacenar o difundir pornografía infantil y las consecuencias de cualquier tipo de abuso.
	Elaborar procedimientos de notificación y retirada, y de presentación de quejas que permitan a los usuarios denunciar la existencia de pornografía infantil o contenido inapropiado y el lugar/perfil concreto en el que lo han encontrado. Establecer procedimientos de seguimiento de denuncias, acordar con otras partes procesos de recopilación de pruebas y eliminar o bloquear inmediatamente el acceso a pornografía infantil. Velar por que, si fuera necesario, los proveedores de servicio soliciten la opinión de expertos (por ejemplo, organismos de PIeL nacionales) antes de destruir contenido ilegal. Velar por que las terceras partes importantes con las que la empresa tiene una relación contractual apliquen procedimientos de notificación y retirada similares.

	Estar preparado para entregar a las autoridades competentes casos de denuncias y pornografía infantil. Si todavía no se ha establecido una relación con los organismos encargados del cumplimiento de la ley ni con una línea telefónica nacional de protección del menor, es necesario ponerse en contacto con ellos para desarrollar procedimientos conjuntamente.
	Trabajar con funciones internas, como la atención al cliente, la prevención del fraude y la seguridad, para que las empresas puedan presentar informes sobre contenidos sospechosos directamente a los organismos responsables de hacer cumplir la ley y a las líneas telefónicas de protección del menor. Lo ideal sería hacerlo de un modo que no expusiese al personal que atiende a las llamadas a contenidos psicológicamente dañinos para ellos, ni hiciese que el menor tuviese que volver a vivir las experiencias sufridas al ver las imágenes en cuestión. Para las situaciones en las que el personal de la línea telefónica de protección del menor pudiese verse expuesto a imágenes de abusos sexuales, aplicar una política o un programa de apoyo destinado a su seguridad, bienestar y recuperación.
Elaborar procesos normalizados para la pornografía infantil (*cont.*)	Incorporar políticas de preservación y retención de datos para ayudar con pruebas a los organismos responsables de hacer cumplir la ley en caso de investigaciones judiciales. Documentar las prácticas de la empresa relativas al tratamiento de la pornografía infantil, desde la supervisión de los contenidos hasta su transferencia final y destrucción. Incorporar en la documentación una lista de todo el personal encargado de la gestión del material.
	Promover mecanismos para denunciar la pornografía infantil y velar por que los clientes sepan cómo presentar una denuncia si descubren contenido semejante. Si existe una línea telefónica de protección del menor, ofrecer enlaces a esa línea desde el sitio web de la empresa y desde cualquier servicio de contenidos que promocione la empresa.
	Tomar todas las medidas pertinentes sobre servicios y datos para evitar que se difundan contenidos de abusos sexuales a niños en los servicios y plataformas de la empresa.
	Evaluar con diligencia y regularidad todos los contenidos albergados en los servidores de la empresa, incluidos los anuncios (de marcas y de terceras partes). Estudiar la posibilidad de utilizar herramientas como el escaneado de *hashes* de imágenes de abusos sexuales a menores, soportes lógicos para el reconocimiento de imágenes o el bloqueo de URL para luchar contra la pornografía infantil.
Crear un entorno en línea más seguro y apropiado para los diferentes grupos de edad	El sector puede ayudar a crear un entorno digital más seguro y agradable para los niños y jóvenes de todas las edades tomando las siguientes medidas:
	Adoptar principios de seguridad y privacidad por diseño en las tecnologías y servicios de la empresa y priorizar soluciones que reduzcan al mínimo el volumen de datos relativos a los niños.

	Aplicar diseños apropiados para los diferentes grupos de edades en los servicios que se ofrecen. Presentar a los niños la información sobre las normas del sitio de forma detallada pero sencilla y comprensible para su edad. Además de elaborar condiciones de uso sencillas en función de los diferentes grupos de edad, el sector debería comunicar de forma similar información sobre, por ejemplo, normas y políticas fundamentales. En ellas debería subrayarse qué se considera un comportamiento aceptable y un comportamiento inaceptable en relación con el servicio, las consecuencias de infringir cualquier norma, las características del servicio y lo que el usuario acepta al firmar las condiciones de uso. Ese tipo de información deberá dirigirse principalmente a los usuarios jóvenes y a los padres o cuidadores.
	Utilizar condiciones de uso para llamar la atención del usuario sobre los contenidos que ofrece la empresa y que puede que no sean apropiados para todas las edades. Las condiciones también deberían incluir mecanismos claros para informar y tratar las infracciones de esas normas.
Crear un entorno en línea más seguro y apropiado para los diferentes grupos de edad **(cont.)**	Considerar la posibilidad de ofrecer mecanismos tales como programas informáticos de control parental y otras herramientas que permitan a los padres y cuidadores gestionar el acceso de sus hijos menores a los recursos de Internet y, al mismo tiempo, ofrecerles orientación sobre la utilización adecuada de esos recursos con miras a proteger sus derechos. Por ejemplo: listas de bloqueo/permiso, filtros de contenidos, vigilancia de uso, gestión de contactos y límites de tiempo/programa.
	Ofrecer opciones de control parental fáciles de usar que permitan a los padres y cuidadores restringir ciertos servicios y contenidos a los que los niños pueden acceder cuando utilizan dispositivos electrónicos. Esas restricciones pueden ser controles a nivel de red, de dispositivo y de aplicación. Teniendo en cuenta que estas restricciones tienen una enorme implicación en la capacidad de aprendizaje del niño de habilidades digitales y pueden perjudicar sus oportunidades en línea, deberán diseñarse para niños muy pequeños en consonancia con su contexto de desarrollo y con una orientación adecuada para los padres.
	Cuando sea posible, promover servicios nacionales de apoyo para que los padres y cuidadores puedan denunciar infracciones y solicitar apoyo en caso de explotación o abuso infantil.
	Evitar la publicación de contenidos publicitarios dañinos o inapropiados en línea y establecer obligaciones de divulgación de cliente para los proveedores de servicios con contenido destinado a un público adulto y que podría ser dañino para jóvenes y niños. Como publicidad perjudicial también se entiende la publicidad de alimentos y bebidas con alto contenido en grasas, azúcares o sal. Alinear las prácticas comerciales con reglamentos y orientaciones sobre comercialización y publicidad para niños y jóvenes. Vigilar dónde, cuándo y cómo los niños y jóvenes pueden encontrarse con mensajes publicitarios potencialmente perjudiciales destinados a otro segmento del mercado.

	Velar por que las políticas de recopilación de datos cumplan las leyes pertinentes relativas a la privacidad de niños y jóvenes, por ejemplo, teniendo en cuenta si es necesario el consentimiento de los padres antes de que las empresas comerciales puedan recopilar información personal de un niño.
	Adaptar y aplicar parámetros predeterminados de privacidad muy estrictos para la recopilación, procesamiento, almacenamiento, venta y publicación de datos personales, incluida la información relativa a la ubicación y los hábitos de navegación obtenidos de personas menores de 18 años. Esos parámetros y la información sobre la importancia de la privacidad deben ajustarse a la edad de los usuarios y a la naturaleza del servicio.
	Utilizar medidas técnicas, como instrumentos apropiados de control parental, seguridad por diseño, experiencias diferenciadas por edad, contenido protegido por contraseña, listas de bloqueo/permiso, controles de compra/tiempo, funciones de exclusión, filtrado y moderación, para evitar que los menores accedan y se vean expuestos a contenidos o servicios inapropiados. Utilizar tecnologías que permitan determinar la edad de los usuarios para poder presentarles una versión de la aplicación apropiada para su edad. En el caso de contenidos o servicios no aptos para todas las edades, las partes interesadas del sector deberían adoptar medidas para verificar la edad de los usuarios. Cuando sea posible, verificar la edad para limitar el acceso a contenidos o materiales que, ya sea por ley o por política, estén destinados únicamente a personas de una cierta edad. Las empresas también deberían reconocer la posibilidad de que si esas tecnologías se utilizan de forma indebida, podrían limitarse los derechos de los niños y los jóvenes a la libertad de expresión y al acceso a la información o ponerse en peligro su privacidad.
Crear un entorno en línea más seguro y apropiado para los diferentes grupos de edad (*cont.*)	Velar por que el contenido y los servicios que no son apropiados para los usuarios de todas las edades: • se clasifiquen de acuerdo con las normas nacionales y las normas culturales; • estén en consonancia con las normas vigentes en medios equivalentes; • se distingan mediante opciones de visualización claras para controlar el acceso; • se ofrezcan después de verificarse la edad, cuando sea posible, y con condiciones claras sobre la eliminación de cualquier dato de identificación personal obtenido mediante ese proceso de verificación. Por ejemplo, en lo que respecta a las normas relativas a los medios de comunicación, todas las autoridades encargadas de la reglamentación de esos medios deben establecer un conjunto de directrices para los contenidos no aptos para todas las edades, y los proveedores de Internet deben adaptar sus bases de datos y aplicar esas directrices a su oferta de contenidos. Véase, Ofcom en el Reino Unido, CSA en Francia y AGCOM en Italia.
	Ofrecer instrumentos claros de denuncia de contenidos inapropiados, contacto y uso indebido, desarrollar un proceso de seguimiento de esas denuncias y proporcionar información detallada a los usuarios del servicio sobre el proceso de denuncia.

	Preparar la moderación de los espacios interactivos diseñados para niños y jóvenes de manera que en ellos se respeten sus derechos a la privacidad y se fomenten sus capacidades en evolución. Al moderar esos espacios de forma diligente se fomenta un ambiente donde la intimidación y el acoso no son aceptables. Los comportamientos inaceptables pueden ser: • publicar comentarios desagradables o amenazantes en el perfil de alguien; • crear perfiles falsos o sitios de odio para humillar a una víctima; • enviar mensajes en cadena y archivos adjuntos con intenciones dañinas; • piratear la cuenta de alguien para enviar mensajes ofensivos a otros.
	Tomar precauciones especiales con los miembros del personal o los colaboradores que trabajan con niños y jóvenes, para los que puede ser necesario exigir un informe preliminar de posibles antecedentes penales emitido por las autoridades policiales.
	Remitir cualquier sospecha de seducción (*grooming*) rápidamente al equipo de gestión ejecutiva en línea o interactiva encargado de informar a las autoridades competentes. Para ello: • informar de la sospecha de seducción al equipo de dirección ejecutiva y a un gestor de políticas de protección del menor, cuando sea posible; • permitir que los usuarios denuncien directamente a las autoridades cualquier sospechosa de seducción; • ofrecer la posibilidad de contacto directo a través de direcciones de correo electrónico para alertar e informar de una sospecha de seducción.
	Priorizar la seguridad y el bienestar del niño en todo momento. Actuar siempre dentro de los límites profesionales y velar por que cualquier contacto con los niños sea porque es imprescindible para el servicio, programa, evento, actividad o proyecto. Nunca aceptar la responsabilidad exclusiva de cuidar a un niño. Si un niño necesita ayuda, avisar al padre, tutor o acompañante. Escuchar y respetar a los niños en todo momento. Si alguien se comporta de manera inapropiada cerca de un niño, denunciar su comportamiento a la persona encargada de la protección infantil del lugar.
Crear un entorno en línea más seguro y apropiado para los diferentes grupos de edad (cont.)	Establecer un conjunto de normas claras que se publiquen en un lugar destacado y que resuman los puntos clave de las condiciones de servicio y las directrices de uso aceptable. En esas reglas debe definirse de forma sencilla: • la naturaleza del servicio y lo que se espera de sus usuarios; • lo que es y lo que no es aceptable en términos de contenido, comportamiento y lenguaje, así como los usos ilegales; • las consecuencias proporcionales de la infracción, por ejemplo la denuncia a los organismos responsables de hacer cumplir la ley o la suspensión de la cuenta del usuario.
	Poner facilidades a los clientes para que puedan denunciar un uso indebido, mediante procesos estándar y sencillos, como la recepción de comunicaciones no deseadas (por ejemplo, correo basura por SMS).

	Ser transparente y proporcionar a los clientes información clara sobre la naturaleza de los servicios ofrecidos, por ejemplo: • tipo de contenido/servicio y costos; • edad mínima requerida para el acceso; • disponibilidad de controles parentales, describiendo lo que los controles cubren (por ejemplo, la red) o no cubren (por ejemplo, WiFi) y formación sobre cómo usarlos; • tipo de información del usuario recopilada y cómo se utiliza.
	Promover servicios nacionales de apoyo que permitan a los niños y jóvenes denunciar y buscar apoyo en caso de abuso o explotación (véase, por ejemplo, Child Helpline International).
Educar a niños, padres y educadores sobre la seguridad del menor y el uso responsable de las TIC	El sector puede complementar las medidas técnicas con actividades educativas y de empoderamiento del siguiente modo:
	Describir con claridad los contenidos disponibles y los controles parentales correspondientes o los entornos de seguridad familiar. Hacer que el lenguaje y la terminología sean sencillos, visibles, claros y pertinentes para todos los usuarios, incluidos menores, padres y cuidadores, especialmente en relación con las condiciones, los costos que entraña la utilización del contenido y los servicios, las políticas de privacidad, la información sobre la seguridad y los mecanismos de presentación de informes.
	Informar a los clientes sobre el modo de gestionar los posibles problemas que pueden surgir al utilizar Internet, por ejemplo el correo basura, el robo de datos y el contacto inapropiado (intimidación y seducción), y describir las acciones que pueden tomar en ese caso y cómo pueden denunciar cualquier irregularidad.
	Establecer diversos mecanismos apropiados e invitar a los padres a que participen en las actividades de TIC de sus hijos menores, en particular los más pequeños, por ejemplo para que revisen la configuración de privacidad del dispositivo utilizado.
	Colaborar con el gobierno y los educadores para ayudar a los padres a que apoyen a sus hijos menores a ser ciudadanos digitales y usuarios responsables de las TIC.

Educar a niños, padres y educadores sobre la seguridad del menor y el uso responsable de las TIC **(cont.)**	En función del contexto local, proporcionar material educativo a escuelas y hogares para mejorar el uso que hacen los niños y jóvenes de los servicios TIC y fomentarles un pensamiento crítico que les permita comportarse de forma segura y responsable al utilizar esos servicios.
	Apoyar a los clientes proporcionándoles directrices sobre la seguridad de la familia en Internet en las que se alienten a padres y a cuidadores a: • familiarizarse con productos y servicios utilizados por niños y jóvenes; • garantizar que los niños y jóvenes utilizan los dispositivos electrónicos de forma moderada como parte de un estilo de vida saludable y equilibrado; • prestar mucha atención al comportamiento de niños y jóvenes para detectar cambios que podrían indicar ciberacoso o intimidación.
	Proporcionar a los padres la información necesaria para que comprendan cómo sus hijos menores utilizan los servicios TIC, manejen los problemas relacionados con los contenidos y conductas perjudiciales y estén preparados para orientarles en un uso responsable. Eso puede lograrse utilizando herramientas y conversando con los distritos escolares para ofrecer programas de estudio sobre seguridad en línea para menores y materiales educativos para padres.
Utilizar avances tecnológicos para proteger y educar a los niños	La inteligencia artificial (IA) en la que se preserva la privacidad y que es capaz de comprender textos, imágenes, conversaciones y contextos, puede detectar y abordar una serie de daños y amenazas en línea y utilizar esa información para empoderar y educar a los niños ante esos peligros. Cuando se realiza dentro de un entorno de dispositivos inteligentes, puede servir para proteger los datos y la privacidad del menor al tiempo que le apoya en sus capacidades.
	El servicio público y los medios de comunicación nacionales pueden desempeñar un papel esencial mediante sus ofertas de programas (en línea y fuera de línea) para educar a padres y a niños y hacerlos conscientes de los riesgos y oportunidades del mundo en línea.
Promover la tecnología digital como un modo de fomentar la participación cívica	El sector puede alentar y empoderar a los niños y jóvenes apoyando su derecho a participar en el mundo digital mediante las siguientes acciones:
	Proporcionar información sobre un servicio para destacar los beneficios que obtienen los niños al comportarse bien y de forma responsable, por ejemplo utilizando el servicio con fines creativos.
	Establecer por escrito procedimientos para que se apliquen de forma coherente políticas y procesos que protegen la libertad de expresión de todos los usuarios, incluidos niños y jóvenes, y se documente el cumplimiento de esas políticas.
Promover la tecnología digital como un modo de fomentar la participación cívica **(cont.)**	Evitar que el exceso de celo dé como resultado un bloqueo de contenidos legítimos y apropiados para el desarrollo del menor. Con miras a que las solicitudes e instrumentos de filtrado no se utilicen indebidamente para restringir el acceso de los niños y jóvenes a la información, es necesario ser transparentes sobre el contenido bloqueado y establecer un proceso para que los usuarios informen de esos bloqueos involuntarios. Ese proceso debería estar a disposición de todos los consumidores, incluidos los administradores de web. Cualquier proceso de denuncia debe incluir condiciones de servicio claras, serias y legales.

	Crear plataformas en línea en las que se promueva el derecho de los niños y los jóvenes a expresarse, facilitar su participación en la vida pública y fomentar su colaboración, espíritu empresarial y participación cívica.
	Desarrollar contenidos educativos para niños y jóvenes que fomenten el aprendizaje, el pensamiento creativo y la resolución de problemas.
	Promover la alfabetización digital y la creación de capacidades y aptitudes TIC para que los niños y jóvenes, en particular los de las zonas rurales y desatendidas, puedan utilizar los recursos de esas tecnologías y participar plenamente y en condiciones de seguridad en el mundo digital.
	Colaborar con la sociedad civil y el gobierno del lugar en lo relativo a las prioridades nacionales y locales con miras a ampliar el acceso universal y equitativo a las TIC, las plataformas y los dispositivos, y la infraestructura subyacente para apoyar esas tecnologías.
	Informar y hacer participar a los clientes, incluidos padres, cuidadores, niños y jóvenes, sobre los servicios ofrecidos, por ejemplo: • tipo de contenidos y correspondientes controles parentales; • mecanismos de denuncia de casos de abuso, uso indebido y contenido inapropiado o ilegal; • procedimientos de seguimiento de las denuncias; • tipos de servicios que están restringidos por la edad; • uso seguro y responsable de los servicios interactivos de "marca propia".
	Participar en las cuestiones más generales relacionadas con la ciudadanía digital segura y responsable, por ejemplo, la reputación en línea y la huella digital, los contenidos perjudiciales y la seducción. Estudiar la posibilidad de asociarse con expertos locales, como ONG de niños, organizaciones benéficas y grupos de padres, para ayudar a elaborar el mensaje de la empresa y llegar al público destinatario.
	Si la empresa ya trabaja con niños o escuelas, por ejemplo mediante programas de responsabilidad social de las empresas, estudiar la posibilidad de ampliar esa relación para educar y hacer participar a niños y jóvenes, y a **educadores** en los mensajes relativos a la PIeL.
Invertir en investigación	Invertir en investigaciones basadas en pruebas y en analizar a fondo las tecnologías digitales, el efecto de las tecnologías en los niños, la protección del menor y las cuestiones relativas a sus derechos con respecto al entorno digital, con miras a utilizar sistemas de protección en línea en los servicios utilizados por niños y jóvenes y comprender mejor qué tipos de medidas son más eficaces para mejorar las experiencias del menor en línea.

Tipología de las empresas de TIC

Aunque las presentes directrices de la UIT están dirigidas a al sector de las TIC en su conjunto, es importante reconocer que los servicios ofrecidos por las empresas de TIC, las formas en las que operan, los planes de reglamentación con arreglo a los cuales funcionan y el alcance y la escala de sus ofertas son muy diferentes. Toda empresa de tecnología cuyos productos y servicios

estén destinados directa o indirectamente a los niños puede beneficiarse de los principios generales esbozados anteriormente y puede adaptarse a ellos en función de su campo de operaciones concreto. La idea central es apoyar y orientar al sector de las TIC para que adopte medidas adecuadas con las que proteger mejor a los niños del riesgo de sufrir daños cuando están en línea, al tiempo que se les capacita para navegar por Internet de la mejor manera posible. La tipología que figura a continuación ayudará a comprender más claramente algunos de los públicos destinatarios y cómo encajan en las listas de control de la sección siguiente. Cabe señalar que estas son solo algunas categorías de ejemplos concretos, y no todas:

a) Proveedores de servicios de Internet, por ejemplo servicios de banda ancha de línea fija o servicios de datos móviles de operadores de redes móviles: aunque suele tratarse de servicios que se ofrecen a más largo plazo a clientes abonados, también puede hacerse extensivo a empresas con puntos de acceso público a Internet por WiFi gratuitos o de pago.
b) Redes sociales/plataformas de mensajes y plataformas de juegos en línea.
c) Fabricantes de equipos y programas informáticos, como proveedores de dispositivos portátiles, incluidos teléfonos móviles, consolas de juegos, dispositivos domésticos basados en asistencia de voz, Internet de las cosas y juguetes inteligentes conectados a Internet para niños.
d) Empresas proveedoras de medios digitales (creadores de contenidos, empresas que proporcionan acceso a contenidos o que los alojan).
e) Empresas que prestan servicios de transmisión en continuo, incluidos transmisiones en directo.
f) Empresas que ofrecen servicios de almacenamiento de archivos digitales y proveedores de servicios basados en la nube.

5 Listas de control de condiciones concretas

El presente capítulo complementa la anterior lista general de control para el sector y ofrece recomendaciones para las empresas que prestan servicios con condiciones concretas sobre el respeto y el apoyo a los derechos del niño en línea. Las siguientes listas de control de condiciones concretas describen formas de complementar los principios y soluciones comunes presentados en el Cuadro 1, ya que se aplican a diferentes servicios y, por lo tanto, deben considerarse además de los pasos del Cuadro 1.

Las condiciones que se destacan a continuación se aplican a muchos ámbitos por lo que varias listas de control pueden ser relevantes para una misma empresa.

Las siguientes listas de control están organizadas a partir de las mismas áreas clave que las directrices generales de la Tabla 1 y por eso se hace referencia a ellas. Cada una de las listas de control se ha elaborado de la mano de colaboradores clave y, como resultado, puede que haya pequeñas variaciones en los cuadros.

5.1 Condición A: Proporcionar conectividad, almacenamiento de datos y servicios de hospedaje

El acceso a Internet es fundamental para el respeto de los derechos de los niños, y la conectividad puede ofrecerles miles de oportunidades. Los proveedores de conectividad, almacenamiento de datos y servicios de hospedaje tienen muchas oportunidades de incorporar

la seguridad y la privacidad en sus ofertas para niños y jóvenes. Esta condición de los servicios se centra, entre otros, en operadores móviles, proveedores de servicios de Internet, sistemas de almacenamiento de datos y servicios de hospedaje.

Los operadores de telefonía móvil permiten el acceso a Internet y ofrecen una serie de servicios de datos concretos para móviles. Muchos operadores ya han suscrito códigos de prácticas de PIeL y ofrecen diversos instrumentos y recursos de información para apoyar sus compromisos.

La mayoría de los proveedores de servicios de Internet actúan tanto como intermediarios, proporcionando acceso a Internet, y como repositorio de datos, a través de sus servicios de hospedaje, almacenamiento y almacenamiento en caché. Como resultado, su función principal es proteger a los niños en línea.

Acceso a Internet en espacios públicos

Cada vez es más frecuente que los municipios, minoristas, empresas de transporte, cadenas hoteleras y otras empresas y organizaciones ofrezcan acceso a Internet a través de puntos de conexión WiFi. Ese tipo de acceso suele ser gratuito o se ofrece a un costo mínimo, y a veces requiere unos trámites de inscripción mínimos como servicio público o cuando lo ofrece una empresa que desea atraer a clientes a sus locales o intentar que utilicen sus servicios más personas.

Promover el servicio de WiFi es una forma eficaz de que haya Internet en una zona determinada. Ahora bien, hay que tener cuidado cuando ese acceso se proporciona en espacios públicos en los que es habitual que haya niños presentes. Los usuarios deben tener en cuenta que las señales de WiFi pueden estar a disposición de terceros que pueden acceder a sus datos personales. Así, el proveedor de WiFi no siempre podrá gestionar o supervisar el uso de una conexión a Internet suministrada, por lo que los usuarios deberán tomar precauciones para no difundir información confidencial a través de WiFi de acceso público.

En los espacios públicos, los proveedores de WiFi podrían estudiar la posibilidad de aplicar medidas adicionales para proteger a los niños y jóvenes, como por ejemplo:

- Bloquear el acceso a sitios web en los que se sabe que se muestran contenidos inapropiados para un gran público, además de intentar bloquear cualquier acceso a pornografía infantil.
- Incluir en las condiciones de uso cláusulas por las que se prohíba el uso de los servicios WiFi para acceder o mostrar cualquier material que pueda ser inapropiado en un entorno con menores presentes. En esas condiciones también deben mencionarse claramente cuáles son las consecuencias de infringir esas normas.
- Tomar todas las medidas de protección posibles contra los accesos no autorizados que pueden dar lugar a la manipulación o pérdida de datos personales.
- Instalar filtros en el sistema WiFi para reforzar la política sobre materiales inapropiados.
- Proporcionar procedimientos y programas informáticos para indicar y ofrecer la opción de control parental en relación con el acceso de niños y jóvenes a contenidos de Internet.

Buenas prácticas: Los reglamentos de telecomunicaciones de la mayoría de los Estados Miembros de la Unión Europea, por ejemplo, estipulan que el acceso a la red debe ser previa identificación, mediante tarjetas SIM individuales u otras herramientas de identificación.

En el Cuadro 2 se ofrece orientación a los proveedores de conectividad, almacenamiento de datos y servicios de alojamiento sobre las medidas que pueden adoptar para mejorar la protección de la infancia en línea y la participación de los niños.

Cuadro 2: Lista de control de PIeL para la condición A: Proporcionar conectividad, datos y dispositivos de alojamiento

Tener en cuenta los derechos de los niños en todas las políticas corporativas y procesos de gestión	Los proveedores de conectividad, almacenamiento de datos y servicios de hospedaje pueden detectar, prevenir y reducir las consecuencias negativas de las TIC en los derechos de los niños y jóvenes y descubrir oportunidades para promover esos derechos.
	Consulte las directrices generales en el Cuadro 1.
Elaborar procesos normalizados para hacer frente a la pornografía infantil	En colaboración con el gobierno, los organismos encargados de hacer cumplir la ley, la sociedad civil y las organizaciones de líneas telefónicas de protección del menor, los proveedores de conectividad, almacenamiento de datos y servicios de hospedaje tienen un papel fundamental en la lucha contra la pornografía infantil. Para ello pueden:
	Colaborar con esas entidades para luchar eficazmente contra la pornografía infantil e informar de los casos que se produzcan a las autoridades competentes. Si todavía no se ha establecido una relación con los organismos encargados del cumplimiento de la ley ni con una línea telefónica de protección del menor, es necesario ponerse en contacto con ellos para desarrollar procedimientos conjuntamente. Los proveedores de conectividad, almacenamiento de datos o servicios de alojamiento también pueden impartir formación en materia de TIC a los organismos encargados de hacer cumplir la ley. Si una empresa opera en mercados menos reglamentados y supervisados en lo relativo a esa cuestión, puede remitir a las personas que deseen presentar una denuncia a la International Association of Internet Hotlines (INHOPE), a través de la cual podrán formalizar la denuncia en cualquier línea telefónica del mundo de protección del menor.
	Estudiar la posibilidad de utilizar listas de bloqueo de URL o sitios web reconocidas internacionalmente, creadas por autoridades competentes (por ejemplo, una línea telefónica directa o de aplicación de la ley nacional, Cybertip Canada, Interpol, IWF), para dificultar a los usuarios el acceso contenidos de pornografía infantil.
	Elaborar procesos de notificación y retirada y de denuncia, y vincular las denuncias de abusos a esos procesos mediante un acuerdo de servicio público en el que se especifique el procedimiento de respuesta y los plazos de retirada. Véase, por ejemplo, la Guía de UNICEF y GSMA sobre políticas y prácticas de notificación y retirada.
	Establecer un mecanismo de denuncia con información clara sobre su utilización, por ejemplo con orientaciones sobre contenidos y conductas ilícitas que deben denunciarse y explicando qué materiales no pueden adjuntarse a la denuncia a fin de evitar su ulterior distribución en la web.

Elaborar procesos normalizados para hacer frente a la pornografía infantil (cont.)	Ayudar con pruebas a los organismos responsables de hacer cumplir la ley en caso de investigaciones judiciales. Utilizar condiciones de servicio para prohibir específicamente el uso de servicios de almacenamiento, difusión o distribución de pornografía infantil. Asegurarse de que en esas condiciones se indica claramente que no se tolerará la pornografía infantil. Indicar en las condiciones de uso que la empresa cooperará plenamente en las posibles investigaciones de organismos encargados de hacer cumplir la ley en caso de que se descubra o denuncie un caso de pornografía infantil.
	Actualmente existen dos soluciones de presentación de denuncias por pornografía infantil en línea a nivel nacional: las líneas telefónicas de protección del menor y los portales de denuncias. En INHOPE figura una lista completa y actualizada de todas las líneas telefónicas de protección del menor y de los portales existentes. Líneas telefónicas de protección del menor: Si no hay una línea telefónica de protección del menor, debe estudiarse la posibilidad de establecer una (véase la Guía de líneas telefónicas de protección del menor de GSMA INHOPE para una serie de opciones, incluida la colaboración con INHOPE y la Fundación INHOPE. Existe una versión interactiva de la guía GSMA INHOPE con orientaciones sobre cómo desarrollar procesos internos para que el personal de atención al cliente presente informes de contenido dudoso a las autoridades encargadas de hacer cumplir la ley y a INHOPE. Portales de presentación de denuncias: La IWF tiene un portal en línea para que los usuarios de Internet situados en países y naciones sin líneas telefónicas de protección al menor puedan presentar directamente a la IWF imágenes y vídeos de actos sospechosos de abuso sexual infantil.
	En el caso de los proveedores de conectividad, los servicios de almacenamiento de datos y hospedaje de contenidos (muchos no lo hacen) deben ir vinculados a procesos de notificación y retirada.
Crear un entorno digital más seguro y apropiado para los diferentes grupos de edad	Los proveedores de conectividad, almacenamiento de datos y servicios de hospedaje pueden ayudar a crear un entorno digital más seguro y agradable para los niños de todas las edades tomando las siguientes medidas:
	Los proveedores de servicios de almacenamiento y hospedaje de datos deberían estudiar la posibilidad de presentar la función de presentación de denuncias en todas sus páginas y servicios web, y elaborar y documentar procesos claros para gestionar con rapidez esas denuncias de abusos o de otras infracciones de las condiciones de uso.
	Los proveedores de conexión deberían ofrecer controles técnicos de marca propia o indicar que cuentan con instrumentos de proveedores especializados que son apropiados para los servicios ofrecidos y que los usuarios finales pueden utilizar fácilmente, y deberían ofrecer la posibilidad de bloquear o filtrar el acceso a Internet a través de las redes de las empresas. Proporcionar mecanismos adecuados de verificación de la edad cuando la empresa ofrezca contenidos o servicios (incluidos los servicios de marca propia o de terceros que promueve la empresa), que solo son legales o apropiados para adultos (por ejemplo, ciertos juegos, loterías).

Educar a niños, padres y educadores sobre la seguridad del menor y el uso responsable de las TIC	Los proveedores de conectividad, almacenamiento de datos y servicios de hospedaje deberán incluir los mensajes clave de las condiciones de uso en sus directrices, y deberán hacerlo en un lenguaje fácil de entender a modo de ayuda para menores, padres y cuidadores. Dentro del propio servicio, en el momento de subir contenidos deberán aparecer recordatorios sobre cuestiones como el tipo de contenido que se considera inapropiado.
	Proporcionar a los niños y jóvenes información con miras a utilizar Internet de forma segura. Estudiar la posibilidad de utilizar mensajes clave como los siguientes: "Nunca des a conocer ninguna información de contacto, como tu ubicación física o tu número de teléfono, a alguien que no conozcas personalmente". "Nunca aceptes ver a alguien que hayas conocido por Internet tú solo, sin consultar primero a un adulto. Dile siempre a un amigo de confianza dónde vas a estar". "No respondas a mensajes intimidatorios, obscenos u ofensivos. A pesar de eso, no borres esos mensajes porque servirán de prueba". "Habla con un adulto o amigo de confianza si te sientes incómodo o molesto por algo que ha pasado o por culpa de alguien". "¡Nunca des la contraseña o el nombre de usuario de tu cuenta!". Ten en cuenta que hay personas en Internet que pueden darte información falsa para convencerte de que les des información privada sobre ti".
	Los proveedores de servicios pueden asociarse con organizaciones bien posicionadas en la educación y el apoyo a menores para un uso más seguro de Internet y para cuestiones afines. Véase la guía práctica de Child Helpline International y GSMA para operadores de telefonía móvil y líneas telefónicas de protección del menor destinada a colaborar para proteger los derechos de los niños, por ejemplo.
Promover la tecnología digital como un modo de fomentar la participación cívica	*Consulte las directrices generales en el Cuadro 1.*

5.2 Condición B: Ofrecer contenidos digitales seleccionados

Internet ofrece todo tipo de contenidos y actividades, muchos de los cuales están destinados a niños y jóvenes. Los servicios que ofrecen contenidos seleccionados permiten la creación de un entorno en el que se fomenta la seguridad y la privacidad de niños y jóvenes.

Esta condición del servicio hace referencia tanto a las empresas que están creando sus propios contenidos como a las que permiten el acceso a contenidos digitales. Se refiere, entre otros, a los servicios de noticias y de transmisión multimedia, a la radiodifusión de servicios públicos y nacionales y al sector de los juegos de azar.

En el cuadro 3 se ofrece orientación a los proveedores de servicios que ofrecen contenidos seleccionados sobre las políticas y medidas que pueden adoptar para mejorar la protección y la participación de los menores en línea.

Cuadro 3: Lista de control de PIeL para la condición B: Ofrecer contenidos digitales seleccionados

Tener en cuenta los derechos del menor en todas las políticas corporativas y procesos de gestión	Las empresas que ofrecen contenidos digitales seleccionados pueden detectar, prevenir y reducir las consecuencias negativas de las TIC en los derechos de los niños y jóvenes y descubrir oportunidades para promover esos derechos. Para ello pueden:
	Elaborar políticas que salvaguarden el bienestar de los niños y jóvenes que aportan contenidos en línea, para tener en cuenta el bienestar físico y emocional y la dignidad de los menores que participan en programas, películas, juegos, noticias, etc., independientemente del consentimiento que pudieran haber obtenido de un progenitor u otro adulto.
Elaborar procesos normalizados para hacer frente a la pornografía infantil	En colaboración con el gobierno, los organismos encargados de hacer cumplir la ley, la sociedad civil y las organizaciones de líneas telefónicas de protección, las empresas que ofrecen contenidos digitales seleccionados pueden desempeñar un papel fundamental en la lucha contra la pornografía infantil aplicando las siguientes medidas: Cuando un usuario sube contenidos en los que aparece pornografía infantil mediante las funciones de "comentar" u "opinar", por ejemplo, el personal de la empresa debería ponerse en contacto con el equipo de gestión ejecutiva encargado de denunciar ese material a las autoridades competentes. Además, deberían: • alertar inmediatamente a los organismos nacionales encargados de hacer cumplir la ley; • alertar a su gerente y denunciar el material al responsable de la política de protección de la infancia; • contactar con el servicio de investigación interna por teléfono o correo electrónico con los detalles del incidente y pedir consejo; • esperar la respuesta del organismo pertinente antes de borrar el material, de guardarlo en un espacio compartido o de reenviarlo.

Elaborar procesos normalizados para hacer frente a la pornografía infantil	Si se encuentra algún contenido con pornografía infantil, deberá comunicarse directamente a una organización especializada en la seguridad en Internet con un sistema de denuncia por línea telefónica para el público y con profesionales en tecnología de la información. Por ejemplo, basándose en su política de protección y salvaguardia del menor, la BBC ha publicado orientaciones editoriales sobre la interacción con niños y jóvenes en línea. Además también ha elaborado listas de control y códigos de conducta para trabajar con niños y jóvenes en línea, que también se aplican a subcontratistas y proveedores externos. La política de Ofcom sobre la protección del menor para el Reino Unido aborda los contenidos en línea, los dispositivos móviles y las consolas juegos por separado. Aplicar una estrategia de comunicación con los niveles superiores rápida y eficaz en caso de que se publique pornografía infantil o se sospeche de una conducta ilegal. Para ello: • ofrecer a los usuarios un método sencillo y de fácil acceso para alertar al productor del contenido sobre las posibles infracciones de alguna norma de la comunidad en línea; • eliminar los contenidos que incumplan las normas; • ofrecer a los usuarios un método sencillo y de fácil acceso para alertar al productor del contenido sobre las posibles infracciones de alguna norma de la comunidad en línea; • eliminar los contenidos que incumplan las normas; Antes de subir a una red social contenidos seleccionados para adultos, tener en cuenta las condiciones de uso del sitio. Respetar los requisitos de edad mínima en los diferentes sitios de redes sociales. En las condiciones de cada espacio en Internet deberían aparecer también mecanismos claros de denuncia de las infracciones de esas normas.
Crear un entorno en línea más seguro y apropiado para los diferentes grupos de edad	Las empresas que ofrecen contenidos digitales seleccionados pueden ayudar a crear un entorno digital más seguro y agradable para los niños y jóvenes de todas las edades tomando las siguientes medidas:
	Colaborar con otras empresas del sector para elaborar sistemas de clasificación de contenidos y/o clasificación por edad basados en normas nacionales o internacionales aceptadas y en consonancia con las soluciones adoptadas en medios equivalentes. En la medida de lo posible, las clasificaciones de los contenidos deberían ser coherentes en las distintas plataformas de medios de comunicación; por ejemplo, un tráiler de una película en una sala de cine y en un teléfono inteligente debería tener la misma clasificación.
	Elaborar productos para niños y jóvenes que sean seguros por su diseño y se complementen con un sólido sistema de verificación de la edad.

	Para ayudar a los padres y a otras personas a decidir si los contenidos son apropiados para los niños y jóvenes, desarrollar aplicaciones y servicios en todos los medios de comunicación para que se ajusten a los sistemas de clasificación de contenidos. Adoptar métodos apropiados de verificación de la edad para impedir que niños y jóvenes accedan a contenidos, sitios, productos o servicios interactivos no aptos para su edad. Proporcionar asesoramiento y recordatorios sobre la naturaleza y la clasificación por edades del contenido que están utilizando.
	Una empresa que ofrece servicios audiovisuales y multimedia puede proporcionar un número de identificación personal a los usuarios para acceder a aquellos contenidos que podrían resultar perjudiciales para niños y jóvenes.
	Garantizar la transparencia de precios de productos y servicios, y la información recogida sobre los usuarios. Velar por que las políticas de recopilación de datos cumplan las leyes pertinentes relativas a la privacidad del menor, en particular en lo relativo a si las empresas comerciales requieren un consentimiento de los padres para recopilar información personal de un niño o sobre él.
	Hacer que la publicidad o la comunicación comercial sea claramente reconocible como tal. Supervisar el contenido en Internet y adaptarlo a los grupos de usuarios que probablemente tengan acceso a él, por ejemplo, estableciendo políticas apropiadas para la publicidad en línea dirigida a niños y jóvenes. Si puede interactuarse con el contenido que se ofrece, por ejemplo, mediante comentarios, foros en línea, redes sociales, plataformas de juego, salas de charla o tableros de mensajes, dar a conocer un conjunto claro de "reglas de la casa", en un lenguaje fácil de entender, en las condiciones del servicio y las directrices para el usuario.
	Decidir qué nivel de participación se desea antes de lanzar un servicio en línea. Los servicios destinados a atraer a niños solo deberían presentar contenidos adecuados para un público joven. En caso de duda, puede consultarse a las autoridades nacionales encargadas de la protección de la infancia.
	Proporcionar un etiquetado de contenido claro y fáctico. Hay que tener en cuenta que los usuarios pueden llegar a contenidos inapropiados al seguir enlaces de sitios de terceros que no cuidan sus contenidos.
Educar a niños, padres y educadores sobre la seguridad del menor y el uso responsable de las TIC	Las empresas que ofrecen contenidos digitales seleccionados pueden complementar las medidas técnicas con actividades educativas que empoderen a los niños como:

	Proporcionando a los clientes información específica y clara sobre: el contenido (como el tipo de contenido, las clasificaciones/restricciones por edad, la presencia de lenguaje inapropiado o de violencia) y los correspondientes controles parentales disponibles; el modo de informar sobre un uso indebido o sobre contenidos inapropiados o ilegales, y el modo de manejar los informes. En el mundo interactivo, esta información debería proporcionarse en forma de etiquetas de contenido para cada programa.
	Alentando a los adultos, especialmente a los padres, cuidadores y educadores, a que participen en el uso que hacen los niños y jóvenes de los contenidos en línea, con miras a ayudarlos y orientarlos en la elección correcta de, por ejemplo, una compra, y a que establezcan normas de conducta. Ayudando a los niños (y a los padres y cuidadores) a que aprendan a gestionar bien el tiempo que pasan frente a una pantalla y a que comprendan cómo utilizar la tecnología de una manera que les resulte agradable y cuándo parar y pasar a otra actividad.
	Estableciendo reglas de uso en un lenguaje claro y accesible que aliente a los niños y jóvenes a estar atentos y a ser responsables cuando navegan por Internet.
	Diseñando instrumentos en función de la edad, como tutoriales y centros de ayuda. Trabajando con programas de prevención en línea o presenciales y con centros de ayuda en caso necesario. Por ejemplo, si existe un riesgo de que los niños y jóvenes se enganchen a la tecnología y ello dificulta su desarrollo de relaciones personales o su participación en actividades físicas sanas, los sitios web podrían proporcionar un enlace de contacto para un centro de ayuda o un servicio de asesoramiento. Haciendo que la información sobre seguridad, como los enlaces a consejos, sea visible, fácilmente accesible y clara, cuando sea probable que el contenido en línea atraiga un gran número de niños y jóvenes.
	Ofreciendo herramientas de orientación para padres, como por ejemplo un sistema de bloqueo para controlar el contenido al que puede accederse desde un navegador determinado.

	Cooperando con los padres para garantizar que la información divulgada en Internet sobre los niños no los pone en peligro. La forma en que se detecta a niños en contenidos seleccionados requiere un estudio cuidadoso y varía según el contexto. Obteniendo el consentimiento fundamentado de los menores antes de presentarlos en programas, películas, vídeos, etc., siempre que sea posible, y respetando cualquier negativa a participar.
Promover la tecnología digital como un modo de fomentar la participación cívica	Las empresas que ofrecen contenidos digitales seleccionados pueden alentar y empoderar a los niños y jóvenes apoyando su derecho a la participación a través de las siguientes acciones:
	Elaborar y/u ofrecer a los niños y jóvenes diversos contenidos de alta calidad, educativos, agradables, interesantes, que les supongan un reto intelectual, que sean apropiados para su edad y que les ayuden a dar sentido al mundo en el que viven. Además de ser atractivo y útil, fiable y seguro, esos contenidos pueden contribuir al desarrollo físico, mental y social de los niños y jóvenes al ofrecerles nuevas oportunidades para entretenerse y educarse. Deben alentarse firmemente los contenidos que permitan a los niños abrazar la diversidad y ser modelos de conducta positivos.

5.3 Condición C: Alojar contenidos generados por el usuario y conectar a los usuarios

Hubo un tiempo en que Internet estaba dominado por los adultos, pero está claro que ahora son los niños y jóvenes los principales actores en la creación y el intercambio de una ingente cantidad de contenidos en crecimiento exponencial, creados por el usuario y publicados en múltiples plataformas. Este servicio se refiere, entre otros, a los servicios de medios sociales, aplicaciones y sitios web relacionados con la realización creativa.

Los servicios que conectan a los usuarios entre sí pueden dividirse en tres categorías:

- Aplicaciones destinadas principalmente a la mensajería (Facebook Messenger, Groupme**,** Line, Tinder, Telegram, Viber, WhatsApp).
- Servicios utilizados principalmente como redes sociales en los que se buscan y alojan contenidos generados por el usuario y permiten su difusión y conectarse dentro y fuera de sus redes (Instagram, Facebook, SnapChat, TikTok).
- Aplicaciones principalmente de emisión en continuo (*streaming)* (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Los proveedores de servicios exigen que los usuarios tengan una edad mínima para darse de alta en sus plataformas, pero es difícil de conseguir que esto se cumpla porque la verificación de la edad depende de la edad que dice tener el usuario. La mayoría de los servicios que conectan a los usuarios entre sí también permiten dar a conocer su ubicación, lo que hace que los niños y jóvenes que utilizan esos servicios estén más expuestos a peligros fuera de Internet.

En el cuadro 4, que se ha adaptado a partir de las normas aplicadas por una de las mayores redes sociales, se ofrece orientación a los proveedores de servicios que albergan contenidos generados por usuarios y conectan a estos entre sí sobre las políticas y medidas que pueden adoptar para mejorar la protección de los menores en línea y su participación.

Cuadro 4: Lista de control de PIeL para la condición C: Alojar contenidos generados por el usuario y conectar a los usuarios

Tener en cuenta los derechos del menor en todas las políticas corporativas y procesos de gestión	Los proveedores de servicios que hospedan contenidos generados por el usuario y conectan usuarios entre sí pueden detectar, prevenir y reducir las consecuencias negativas de las TIC en los derechos de los niños y jóvenes y descubrir oportunidades para promover esos derechos.
	Consulte las directrices generales en el Cuadro 1.
Elaborar procesos normalizados para hacer frente a la pornografía infantil	En colaboración con el gobierno, los organismos encargados de hacer cumplir la ley, la sociedad civil y las organizaciones de líneas de protección, las empresas que hospedan contenidos generados por el cliente y conectan a usuarios entre sí tienen un papel fundamental en la lucha contra la pornografía infantil. Para ello pueden:
	Establecer procedimientos para que todos los sitios presten asistencia inmediata a los organismos encargados de hacer cumplir la ley durante situaciones de emergencia y en investigaciones rutinarias.
	Indicar que la empresa cooperará plenamente en las posibles investigaciones de los organismos encargados de hacer cumplir la ley que pudieran producirse si se denunciase o descubriese contenido ilegal e informar de las posibles sanciones, como multas o cancelación de privilegios fiscales.
	serujon funciones internas, como atención al cliente, prevención del fraude y seguridad, para que las empresas puedan presentar denuncias sobre contenidos sospechosos directamente a los organismos encargados de hacer cumplir la ley y a líneas de protección del menor. Lo ideal sería hacerlo de un modo que no expusiese al personal que atiende a las llamadas a los contenidos, ni hiciese que el menor tuviese que volver a vivir la experiencia viendo las imágenes en cuestión. Para las situaciones en las que el personal de la línea telefónica de protección del menor pudiese verse expuesto a imágenes de abusos sexuales, aplicar una política o un programa de apoyo destinado a su seguridad, bienestar y recuperación.
	Utilizar condiciones de servicio para prohibir contenidos y comportamientos ilegales, destacando que: • no se tolerarán contenidos dañinos, incluidos posibles comportamientos de seducción de niños con la intención de abusar de ellos con o sin contacto físico; • no se tolerarán contenidos ilegales, incluida la carga o ulterior difusión de pornografía infantil; • la empresa recurrirá a investigaciones de organismos encargados de hacer cumplir la ley, y colaborará en ellas, en caso de que se denuncien o descubran contenidos ilegales o cualquier incumplimiento de la política de protección de la infancia.

	Documentar las prácticas de la empresa relativas al tratamiento de la pornografía infantil, desde la supervisión de los contenidos hasta su transferencia final y destrucción. Incorporar en la documentación una lista de todo el personal encargado de la gestión del material.
	Adoptar políticas de responsabilización de los contenidos generados por el usuario, incluida la opción de eliminar esos contenidos a petición del usuario. Eliminar los contenidos que infrinjan las políticas del proveedor y alertar al usuario que lo haya publicado sobre la infracción.
Elaborar procesos normalizados para hacer frente a la pornografía infantil **(cont.)**	Indicar a los usuarios las consecuencias de incumplir las políticas de uso aceptable, por ejemplo: • eliminación del contenido, suspensión o cierre de la cuenta del usuario; • suspensión de la posibilidad de compartir determinados tipos de contenido o de utilizar ciertas opciones; • imposibilidad de ponerse en contacto con menores; • remisión del posible caso a los organismos encargados de hacer cumplir la ley
Elaborar procesos estándar para gestionar material de abuso sexual infantil	Promover mecanismos para denunciar la pornografía infantil y cualquier otro contenido ilegal, y velar por que los clientes sepan cómo presentar una denuncia si descubren contenido semejante. Construir sistemas, y contar con personal capacitado, para evaluar cuestiones caso por caso y para tomar las medidas apropiadas. Establecer equipos de operación de apoyo al usuario completos y bien dotados de recursos. Lo ideal sería que esos equipos estuvieran capacitados para manejar diferentes tipos de incidentes para poder dar una respuesta adecuada y tomar las medidas pertinentes. Cuando el usuario presente una denuncia, dependiendo del tipo de incidente, debería ser dirigida al personal apropiado. La empresa también podría crear equipos especiales para atender las reclamaciones presentadas por usuarios con motivo de denuncias incorrectas.
	Disponer de procesos para eliminar o bloquear inmediatamente el acceso a pornografía infantil, incluidos procesos de notificación y retirada con los que eliminar el contenido ilegal tan pronto como sea detectado. Velar por que las terceras partes con las que la empresa tiene una relación contractual apliquen procedimientos de notificación y retirada similares. Si la legislación lo permite, el material puede guardarse como prueba de un delito para posibles investigaciones.

	Desarrollar sistemas técnicos con los que detectar contenidos ilegales e impedir que se carguen en la red, incluso en grupos privados, o con los que marcar esos contenidos para una revisión inmediatamente posterior por el equipo de seguridad de la empresa. Tomar todas las medidas pertinentes para que los servicios no se utilicen indebidamente para albergar, difundir o crear pornografía infantil. Si fuese posible, crear medidas técnicas dinámicas para analizar objetos y metadatos vinculados a un perfil con miras a detectar comportamientos o pautas delictivas, y a adoptar las medidas adecuadas.
	Si la aplicación o el servicio permiten a los clientes cargar y almacenar fotografías en servidores de la empresa o en servidores operados por ella, disponer de procesos y herramientas para detectar imágenes en las que muy probablemente se muestre pornografía infantil. Estudiar la posibilidad de utilizar técnicas de identificación dinámicas, como la tecnología de escaneado o el examen realizado por una persona.
Crear un entorno en línea más seguro y apropiado para los diferentes grupos de edad	Los proveedores de servicios que ofrecen contenidos generados por los usuarios y que conectan a estos entre sí pueden ayudar a crear un entorno digital más seguro y agradable para los niños de todas las edades tomando las siguientes medidas:
	Comunicar en las condiciones de servicio y en las directrices para el usuario, en un lenguaje sencillo, un conjunto claro de "reglas de la casa" en las que se defina: • la naturaleza del servicio y lo que se espera de sus usuarios; • lo que es y lo que no es aceptable en términos de contenido, comportamiento y lenguaje, así como los usos ilegales; • las consecuencias de cualquier infracción, por ejemplo, la denuncia a los organismos responsables de hacer cumplir la ley o la suspensión de la cuenta del usuario.
	Los mensajes de seguridad y jurídicos más importantes deben presentarse en un formato adaptado a las diferentes edades (es decir, utilizando iconos y símbolos intuitivos) tanto en el momento de la inscripción como de manera oportuna a medida que se vayan realizando diferentes acciones en el sitio.
	Mediante procesos estándar y accesibles, facilitar a los clientes la tarea de informar al servicio de atención al cliente de sus preocupaciones sobre algún uso indebido, como la recepción de comunicaciones no deseadas (correo basura o intimidación) o la visualización de contenidos inapropiados.
	Proporcionar opciones de visibilidad y de divulgación de contenidos apropiadas para cada edad. Por ejemplo, hacer por defecto que los ajustes de privacidad y visibilidad para niños y jóvenes sean más restrictivos que los ajustes para adultos.

	Hacer que se cumplan los requisitos de edad mínima y apoyar la investigación y desarrollo de nuevos sistemas de verificación de la edad, como la biometría, basándose en normas internacionales reconocidas para la elaboración de esos instrumentos. Tomar medidas para detectar y retirar del sitio a usuarios menores de edad que han falseado su edad para acceder. Es necesario tener en cuenta la recopilación de datos personales adicionales que lo anterior puede requerir y la necesidad de limitar esa recopilación y almacenamiento de información y su procesamiento. Si todavía no se ha puesto en marcha, desarrollar procesos de inicio de sesión adecuados para determinar si los usuarios tienen la edad suficiente para acceder al contenido o servicio sin tener que desvelar su identidad, ubicación y otros datos personales. Utilizar sistemas funcionales de verificación de la edad establecidos a nivel nacional, según proceda, cuando existan medidas pertinentes para la privacidad de datos de menores. Establecer una función de denuncia o un centro de asistencia que pueda alentar a los usuarios a denunciar a las personas que han falsificado su edad.
Crear un entorno en línea más seguro y apropiado para los diferentes grupos de edad **(cont.)**	Proteger a los usuarios más jóvenes ante posibles comunicaciones no deseadas y garantizar que se apliquen las directrices sobre privacidad y recopilación de información.
	Buscar formas de revisar las imágenes y los vídeos alojados y eliminar aquellos inapropiados una vez se detecten. Para ello pueden utilizarse herramientas como el escaneado de *hashes* de imágenes conocidas y el software de reconocimiento de imágenes. En los servicios dirigidos a menores, pueden revisarse las fotos y los vídeos antes de su publicación para asegurarse de que los niños no publican información personal delicada sobre ellos mismos o sobre otros.

	Pueden utilizarse una serie de medidas para controlar el acceso a contenidos generados por los usuarios y proteger a los niños y jóvenes en línea contra aquellos contenidos inapropiados o ilegales. Utilizar contraseñas seguras para proteger a los niños y jóvenes en sitios de juegos y en otros medios sociales. Algunas otras técnicas son: • revisar los grupos de debate para detectar temas dañinos, expresiones de odio y conductas ilegales, y suprimir esos contenidos cuando se determine que violan las condiciones de uso; • desarrollar herramientas para buscar y eliminar activamente contenidos ilegales o que infringen las condiciones de servicio de la empresa, así como herramientas para evitar la carga de contenidos ilegales en el sitio; • preparar la moderación de los espacios de mensajes con un equipo de moderadores especializados en niños y jóvenes que revisará los contenidos para ver si cumplen las "reglas de la casa" publicadas. Cada mensaje puede revisarse antes de ser publicado, y los moderadores también pueden detectar y señalar a usuarios sospechosos, así como a usuarios en dificultades; • establecer un equipo de anfitriones de comunidad que sirva como primer punto de contacto para los moderadores cuando estén preocupados por un usuario.
	Encargarse de revisar contenidos comerciales, incluso en foros, redes sociales y sitios de juegos. Aplicar normas y reglas apropiadas para proteger a los menores de publicidad inapropiada para su edad y establecer límites claros para la publicidad en línea dirigida a niños y jóvenes.
Educar a niños, padres y educadores sobre la seguridad del menor y el uso responsable de las TIC	Los proveedores de servicios que ofrecen contenidos generados por los usuarios pueden complementar las medidas técnicas con actividades educativas y de empoderamiento aplicando las siguientes medidas:
	Crear una sección dedicada a consejos de seguridad, artículos, reportajes y diálogos sobre la ciudadanía digital, así como enlaces a contenidos útiles de terceros expertos. Los consejos de seguridad deben localizarse fácilmente y comunicarse en un lenguaje sencillo. También se alienta a los proveedores de plataformas a que dispongan de la misma interfaz de navegación en distintos dispositivos, como ordenadores, tabletas o teléfonos móviles.
	Ofrecer a los padres información clara sobre los tipos de contenidos y los servicios disponibles, incluida, por ejemplo, una explicación de las redes sociales y los servicios basados en localización, la forma en que se accede a Internet mediante dispositivos móviles y las opciones de las que disponen para aplicar controles.
	Informar a los padres sobre cómo denunciar abusos, usos indebidos y contenidos inapropiados o ilegales, y sobre cómo se gestionará la denuncia. Informarles sobre qué servicios están restringidos en función de la edad y sobre otras formas de actuar de manera segura y responsable al utilizar servicios interactivos.

	Establecer un sistema basado en la confianza y la reputación para fomentar el buen comportamiento y permitir que otros usuarios muestren mejores prácticas a los demás mediante su forma de actuar. Destacar la importancia de la comunicación social por la que las personas se ponen en contacto con otros usuarios o amigos de confianza para poder resolver un conflicto o entablar una conversación sobre contenidos problemáticos.
	Ofrecer consejos y recordatorios sobre la naturaleza de un determinado servicio o contenido y sobre cómo disfrutarlo de forma segura. Incorporar directrices comunitarias en los servicios interactivos, por ejemplo, con ventanas emergentes en las que se recuerde a los usuarios cómo actuar de forma apropiada y segura y sobre la importancia de no facilitar sus datos de contacto.
	Cooperar con los padres y orientarlos para que la información divulgada en Internet sobre menores no ponga en peligro a sus hijos. Obtener el consentimiento fundamentado de los menores antes de presentarlos en contenidos creados por ellos mismos, siempre que sea posible, y respetar cualquier negativa a participar.
Promover la tecnología digital como un modo de fomentar la participación cívica	Los proveedores de servicios que albergan contenidos generados por los usuarios pueden alentar y empoderar a los niños y jóvenes apoyando su derecho a la participación.
	Consulte las directrices generales en el Cuadro 1.

5.4 Condición D: Sistemas basados en inteligencia artificial

Ahora que se presta cada vez más atención a las tecnologías de aprendizaje profundo, los términos "inteligencia artificial", "aprendizaje automático" y el propio "aprendizaje profundo", el público en general utiliza estos términos de manera un tanto intercambiable para reflejar la idea de que las máquinas imitan comportamientos "inteligentes". En la presente sección nos centramos en las formas en que el aprendizaje automático y los procesos de aprendizaje profundo afectan a la vida de los niños y, en última instancia, a sus derechos humanos.

"Debido al avance exponencial de las tecnologías basadas en la inteligencia artificial en los últimos años, en el actual marco internacional de protección de derechos de la infancia no se abordan explícitamente muchas de las cuestiones que plantea el desarrollo y la utilización de esas tecnologías. Con todo, en él se definen varios derechos que pueden estar relacionados con esas tecnologías, por lo que supone un importante punto de partida para cualquier análisis de cómo los derechos de los niños pueden verse afectados positiva o negativamente por las nuevas tecnologías, por ejemplo los derechos a la privacidad, a la educación, al juego y a la no discriminación"[18].

La aplicación de la IA puede influir en cómo los menores utilizan los diferentes servicios en las redes sociales, como las plataformas de transmisión en continuo de vídeos. Los algoritmos de aprendizaje automático, que son el motor de recomendación utilizado principalmente por las plataformas más populares de intercambio de vídeos, han sido optimizados para obtener

[18] UNICEF y UC Berkeley, *Executive Summary: Artificial Intelligence and Children's Rights* (Resumen ejecutivo: inteligencia artificial y derechos del niño), 2018.

la máxima visualización de determinados vídeos en un tiempo concreto[19]. La tecnología de pantalla táctil y el diseño de esas plataformas permiten a los niños muy pequeños navegar por sus contenidos. Es especialmente preocupante que los algoritmos que se utilizan para recomendar vídeos puedan hacer que los menores queden atrapados en un "burbuja filtro" de contenidos pobres o inapropiados. Como los niños son particularmente susceptibles a las recomendaciones de contenidos, si los vídeos relacionados que se recomiendan son chocantes, es posible que atraigan su atención y los aparten de una programación más amigable para ellos[20].

La IA también influye en la protección de la infancia en línea en lo relativo a los juguetes inteligentes. Existen ciertos riesgos asociados a cada uno de los distintos procesos que intervienen en el funcionamiento de los juguetes inteligentes: el juguete (que interactúa con el menor), la aplicación móvil (que actúa como punto de acceso para la conexión WiFi) y la cuenta en línea personalizada del juguete/consumidor (donde se almacenan los datos). Esos juguetes se comunican con servidores basados en la nube que almacenan y procesan los datos proporcionados por los menores que interactúan con el juguete. Este modelo tiene problemas de privacidad si no se aplican medidas de seguridad en todos los niveles, algo que ha quedado demostrado por numerosos casos de piratería informática en los que se han filtrado datos personales. Además, algunos de los dispositivos pirateados (incluidos los dispositivos inteligentes habilitados para la web, como monitores de bebés, asistentes de voz, etc.) pueden utilizarse para vigilar a los usuarios sin su conocimiento o consentimiento.

Cuando se utilizan mecanismos para responder a las amenazas contra los menores que utilizan esos dispositivos, por ejemplo cuando se ofrecen consejos y recomendaciones basados en comportamientos estudiados (como se mencionó anteriormente con la aplicación Own It de la BBC), es fundamental que las empresas que diseñan esos dispositivos inteligentes desarrollen sus recomendaciones a partir de pruebas y en consulta con expertos en protección y salvaguardia de la infancia.

Aunque algunas empresas están promoviendo principios para el uso ético de la IA[21], no está claro si existen políticas públicas dirigidas a esta tecnología y a los menores[22]. Varias asociaciones de tecnología y comercio, y grupos de informática, han redactado principios éticos con respecto a la IA[23]. Con todo, en ellos no se hace referencia explícita a los derechos del menor, a las formas en que esas tecnologías de IA pueden suponer riesgos para ellos o a los planes preventivos para evitar esos riesgos.

"Al igual que las empresas, los gobiernos de todo el mundo han adoptado estrategias para convertirse en líderes en el desarrollo y el uso de la IA, fomentando entornos favorables para innovadores y empresas".[24] Ahora bien, no está claro cómo en esas estrategias nacionales se abordarán directamente los derechos del niño.

---

19 Ibíd.
20 Ibíd.
21 Véase Microsoft, *Salient Human Rights Issues* (Nuevos problemas sobre derechos humanos), informe FY17; y Google, *Responsible Development of AI* (Desarrollo responsable de IA) (2018).
22 Blog oficial de Microsoft, *The Future Computed: Artificial Intelligence and its role in society* (El futuro computarizada: la inteligencia artificial y su función en la sociedad), 2018.
23 The Guardian, *'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft* (Alianza sobre IA formada por Google, Facebook, Amazon, IBM y Microsoft), 2016.
24 Ibíd.

Mejorar la gestión de Facebook de los contenidos relacionados con el suicidio y las autolesiones

En 2019, Facebook comenzó a celebrar consultas periódicas con expertos de todo el mundo para discutir algunas de las cuestiones más complicadas relativas al suicidio y las autolesiones. Entre ellas, la forma de tratar las notas de suicidio, los riesgos relacionados con los contenidos de carácter deprimente en Internet y las imágenes de suicidios que atraen el interés del público. Puede encontrarse más información sobre esas reuniones en la nueva página de prevención de suicidios de Facebook, en su Centro de Seguridad. Gracias a esas consultas se ha mejorado la forma en que Facebook maneja ese tipo de contenidos. La política relativa a las autolesiones, por ejemplo, se reforzó para prohibir imágenes en las que se viesen cortes, con miras a evitar la promoción involuntaria de este problema. Incluso cuando alguien escribe buscando ayuda o para informar de su recuperación, Facebook oculta las imágenes de heridas curadas. Ese tipo de contenidos potencialmente perjudiciales puede descubrirse ahora con la IA para tomar medidas al respecto, por ejemplo su eliminación u ocultación de forma automática. De abril a junio de 2019, Facebook actuó sobre más de 1,5 millones de contenidos relativos a suicidios y autolesiones en su sitio web, de los cuales pudo detectar más del 95% antes de que ningún usuario los denunciase. Durante ese mismo periodo, Instagram actuó sobre más de 800 000 contenidos similares, de los cuales más del 77% se detectaron antes de ser comunicados por un usuario.

Detectar posibles intimidaciones o actos de violencia entre usuarios de mensajería en tiempo real

Instagram está utilizando la IA para acabar con comportamientos como insultar, avergonzar y faltar el respeto. Mediante sofisticadas herramientas de denuncia, los moderadores pueden cerrar rápidamente la cuenta de quien intimide a alguien en Internet.

Buenas prácticas: Utilización de la inteligencia artificial en la detección de material de abusos sexuales a menores

Basándose en la generosa contribución de Microsoft para luchar contra la explotación infantil, PhotoDNA, y en el reciente lanzamiento de Google, Content Safety API, Facebook también ha desarrollado tecnologías para detectar contenidos de abuso sexual infantil.

Conocidas como PDQ y TMK+PDQF, esas tecnologías forman parte de un conjunto de herramientas que Facebook utiliza para detectar contenidos dañinos. En el sector hay disponibles otros algoritmos y herramientas, como pHash, aHash y dHash. El algoritmo de Facebook para detectar determinados contenidos en fotografías, PDQ, se ha inspirado claramente en pHash, aunque ha sido diseñado completamente como un algoritmo distinto con aplicación de software independiente. La tecnología para detectar determinados contenidos en vídeos, TMK+PDQF, fue desarrollada conjuntamente por el equipo de investigación de IA de Facebook y profesionales académicos de la Universidad de Módena y Reggio Emilia en Italia.

Esas tecnologías crean una forma eficiente de almacenar archivos como *hashes* digitales cortos que pueden servir para determinar si dos archivos son iguales o similares, incluso sin la imagen o el vídeo original. Los *hashes* también pueden ofrecerse más fácilmente a otras empresas y organizaciones sin ánimo de lucro.

PDQ y TMK+PDQF fueron diseñados para operar a gran escala, soportando *hashing* de fotogramas de vídeos y aplicaciones en tiempo real.

En el cuadro 5 se presentan algunas de las recomendaciones para que las empresas armonicen sus principios al diseñar y aplicar soluciones basadas en inteligencia artificial dirigidas a los menores.

Las recomendaciones se basan en el trabajo de UNICEF para desarrollar orientaciones políticas mundiales sobre IA y menores, destinadas a gobiernos y empresas del sector. Para obtener más información sobre el proyecto puede leerse https://www.unicef.org/globalinsight/featured-projects/ai-children . Las recomendaciones también se basan en el documento de UNICEF y UC Berkeley sobre IA y derechos del menor[25].

[25] UNICEF y UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

Cuadro 5: Lista de control de PIeL para la condición D: Sistemas basados en IA

Tener en cuenta los derechos del menor en todas las políticas corporativas y procesos de gestión	Los proveedores de sistemas basados en IA pueden detectar, prevenir y reducir las consecuencias negativas de las TIC en los derechos de los niños y jóvenes y descubrir oportunidades para promover esos derechos.
	Los sistemas de inteligencia artificial deberían diseñarse, desarrollarse, aplicarse e investigarse para respetar y promover los derechos del niño, tal como se describen en la Convención sobre los Derechos del Niño. La infancia, que se vive cada vez más en el entorno digital, es un tiempo en el que debe primar un cuidado y una asistencia especiales. Los sistemas de IA deberían aprovecharse para ofrecer esa ayuda en su máximo potencial.
	Utilizar un diseño inclusivo en el desarrollo de productos para niños en el que se tenga en cuenta la diversidad de género, geográfica y cultural, y se incluya una amplia gama de interesados, como padres, maestros, psicólogos infantiles y, cuando proceda, los propios niños.
	Deberían establecerse marcos de gobernanza, incluidas directrices éticas, leyes, normas y órganos reguladores, para supervisar los procesos que garantizan que la aplicación de los sistemas de inteligencia artificial no infringen los derechos del menor.
Elaborar procesos normalizados para hacer frente a la pornografía infantil	En colaboración con el gobierno, los organismos encargados de hacer cumplir la ley, la sociedad civil y las organizaciones de líneas de protección, los proveedores de sistemas basados en IA tienen un papel fundamental en la lucha contra la pornografía infantil. Para ello pueden:
	Consulte las directrices generales en el Cuadro 1.
Crear un entorno en línea más seguro y apropiado para los diferentes grupos de edad	Los proveedores de sistemas basados en IA pueden ayudar a crear un entorno digital más seguro y agradable para los niños y jóvenes de todas las edades tomando las siguientes medidas:
	Adoptar un planteamiento multidisciplinario al desarrollar tecnologías que puedan afectar a los menores y consultar con la sociedad civil, incluidos los profesionales académicos, para determinar las posibles repercusiones que esas tecnologías pueden tener en los derechos de diversos posibles usuarios finales.
	Aplicar seguridad y privacidad a través del diseño de los productos y servicios dirigidos a los menores o utilizados comúnmente por ellos.

	Como los sistemas de inteligencia artificial necesitan muchos datos, las empresas que utilizan esa tecnología para sus servicios deberían vigilar con especial cuidado todo lo relativo a la recopilación, procesamiento, almacenamiento, venta y publicación de datos personales de menores. Los sistemas de IA deberían ser transparentes, en el sentido de que debería ser posible descubrir cómo y por qué han tomado una decisión en particular o, en el caso de robots, han actuado de una manera determinada. Esa transparencia es crucial para desarrollar confianza y facilitar auditorías, investigaciones y recursos cuando se sospeche que se ha producido un daño a menores. Ofrecer mecanismos funcionales y legales de denuncia por si los menores se viesen o sintiesen perjudicados por los sistemas de IA. Establecer procesos para corregir oportunamente cualquier resultado discriminatorio, y crear órganos de supervisión encargados de gestionar las denuncias y vigilar de forma continua la seguridad y la protección de los menores. La responsabilidad y los mecanismos de corrección van de la mano.
	Elaborar planes para manejar datos especialmente delicados, incluidas revelaciones de abusos u otros daños que puedan comunicarse a la empresa a través de sus productos. En las plataformas digitales y los sistemas de IA debería reducirse al mínimo la recopilación de datos sobre menores y controlarse al máximo la información generada por ellos. Las condiciones de uso deberían ser comprensibles para los menores con miras a fomentar su conocimiento y capacidad de acción.
Educar a niños, padres y educadores sobre la seguridad del menor y el uso responsable de las TIC	Los proveedores de sistemas basados en IA pueden complementar las medidas técnicas con actividades educativas y de empoderamiento.
	Debería ser posible explicar el propósito de los sistemas de inteligencia artificial a los niños y sus padres o cuidadores para que puedan decidir si desean utilizarlos o no.
Promover la tecnología digital como un modo de fomentar la participación cívica	Los proveedores de sistemas basados en inteligencia artificial pueden alentar y empoderar a los niños y jóvenes apoyando su derecho a la participación.
	Consulte las directrices generales en el Cuadro 1.
Utilizar avances tecnológicos para proteger y educar a los niños	Los sistemas basados en IA deberían diseñarse, desarrollarse y aplicarse para apoyar el desarrollo y el bienestar del menor. Para ello, su punto de referencia deberían ser las mejores medidas de desarrollo y bienestar disponibles aceptadas ampliamente. Las empresas deberían invertir en la investigación y el desarrollo de herramientas éticas basadas en IA para detectar casos de pornografía infantil, acoso e intimidación en línea, en colaboración con expertos destacados en derechos de la infancia y con los propios niños y jóvenes. Los avances en las tecnologías de IA deberían aplicarse a las soluciones de mensajería para menores sin comprometer su identidad, ubicación o información personal.

Referencias

Texto del GDPR (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo), de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y texto publicado en el Diario Oficial de la UE.

Directiva de servicios de comunicación audiovisual por la que se modifica la Directiva 2010/13/UE, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual, a la vista de la evolución de las realidades del mercado y el Texto publicado en el Diario Oficial de la UE.

Política de la BBC:

- *Child protection and safeguarding policy version 2017* (Política de salvaguarda y protección de la infancia, versión 2017), revisada en 2018, y la versión actualizada en 2019
- *Working with young people and children at the BBC* (Trabajar con jóvenes y niños en la BBC);
- *Framework for Independent Production Companies working on BBC Productions* (Marco para las empresas de producción independientes que trabajan para BBC Productions sobre las normas de proveedores externos sobre la protección de menores);
- *Guidance: Interacting with children and young people online* (Interacción con niños y jóvenes en línea sobre las directrices editoriales para las actividades en línea).

Investigación que demuestra que no se cumplen los procesos de verificación de la edad en los medios sociales en el Reino Unido: 2016, 2017; 2020.

Glosario

Las definiciones que figuran a continuación se han extraído principalmente de la terminología existente establecida en la Convención sobre los Derechos del Niño, 1989, así como por el Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes en las Orientaciones Terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, 2016 (Orientaciones de Luxemburgo), por el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, 2007, así como en el Global Kids Online Report del UNICEF, 2019.

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 18-19 años de edad son adultos salvo que, en virtud de la ley que les sea aplicable, hayan alcanzado antes la mayoría de edad[26].

Inteligencia artificial

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 (sistemas de identificación automática descritos como "débiles" o moderados, como de reconocimiento facial o de voz, conducción de vehículos)[27].

Sistemas de inteligencia artificial

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. Los sistemas de IA están diseñados para funcionar con diversos niveles de autonomía[28].

Alexa

Amazon Alexa, o simplemente Alexa, es un asistente virtual de IA desarrollado por Amazon. Es capaz de interactuar con la voz, reproducir música, hacer listas de tareas, configurar alarmas, transmitir podcasts, reproducir audiolibros y proporcionar información sobre el tiempo, el tráfico, los deportes y otra información en tiempo real, como noticias. Alexa también puede controlar varios dispositivos inteligentes actuando como un sistema de automatización del hogar. Los usuarios pueden ampliar las capacidades de Alexa instalando skills o "destrezas" (funcionalidad adicional desarrollada por terceros, más conocidas con el nombre de aplicaciones en otros entornos, como programas meteorológicos y funciones de audio)[29].

Interés superior del niño

[26] UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria*, 2014.
[27] Consejo de Europa, *What's AI?* (¿Qué es la inteligencia artificial?).
[28] OCDE, *Recommendation of the Council on Artificial Intelligence* (Recomendación del Consejo sobre la Inteligencia Artificial), 2019.
[29] UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria*, 2014.

Se refiere a todos los factores necesarios para tomar una decisión en un caso específico para un niño en particular o un grupo de niños[30].

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[31].

Explotación y abuso sexuales infantil

Describe toda forma de explotación sexual y abuso sexual, "a) La incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal o psicológicamente perjudicial; b) La utilización de un niño con fines de explotación sexual comercial; c) La utilización de un niño para la producción de imágenes o grabaciones sonoras de abusos sexuales a niños"[32]; así como el "contacto sexual que normalmente implica el uso de la fuerza sobre una persona sin consentimiento"[33]. La explotación y el abuso sexuales de los niños suceden cada vez más por Internet, o guarda cierta relación con el entorno en línea.

Material de explotación y abuso sexual infantil

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[34]. 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[35] y describe más en detalle 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 y un delito grave. [...] 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". El término se refiere al material que representa actos de explotación o abuso sexual de un niño. Comprende, entre otras cosas, grabaciones de abusos sexuales de niños por adultos; imágenes de niños en actos sexuales explícitos; e imágenes de órganos sexuales de niños producidas o utilizadas con fines principalmente sexuales.

En las Orientaciones de Luxemburgo pueden consultarse términos como "Materiales de abuso sexual de niñas, niños y adolescentes generados por ordenador/de forma digital".

---

30 Véase la Convención de las Naciones Unidas sobre los Derechos del Niño.
31 UNICEF y UIT, "Directrices de protección de la infancia en línea para la Industria", 2014.
32 Artículo 34 de la Convención de las Naciones Unidas sobre los Derechos del Niño.
33 Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales (Luxembourg Guidelines), 2016.
34 Las Orientaciones de Luxemburgo (véase arriba), 2016 y el *Global Kids Online Report* del UNICEF, 2019.
35 Comisión de Banda Ancha para el Desarrollo Sostenible, *Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online* (Seguridad en línea del menor: reducir al mínimo el riesgo de violencia, abuso y explotación en línea), 2019; WePROTECT Global Alliance, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response* (Evitar y combatir la explotación y el abuso infantiles: un modelo de respuesta nacional), 2016.

Niños y jóvenes

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 WiFi 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[36].

Ciberacoso

Por ciberacoso se entiende la agresión deliberada y reiterada por una persona o grupo, utilizando la tecnología digital, contra una víctima que no puede defenderse fácilmente[37]. 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"[38].

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"[39].

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[40].

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 realizan cada vez más a través de tecnologías digitales como las plataformas de Internet, los medios

---

36 cJeremy Greenberg, *Dangerous Games: Connected Toys, COPPA, and Bad Security* (Juegos peligrosos: juguetes conectados, Ley de Protección de la Privacidad en Línea para Niños y mala seguridad) Georgetown Law Technology Review, 2017.

37 Anna Costanza Baldry et al. *Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities* (Ciberacoso y cibervictimización frente a supervisión, monitorización y control parental de las actividades en línea de adolescentes), Children and Youth Services Review, 2019.

38 Las Orientaciones de Luxemburgo, 2016 y el UNICEF Global Kids Online Report, 2019 (véase arriba).

39 UNICEF Global Kids Online Report, 2019 (como arriba).

40 Council of Europe, Digital Citizenship and Digital Citizenship Education (Ciudadanía digital y educación ciudadana digital).

sociales y los dispositivos móviles[41]. 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. También se refiere a la inteligencia emocional que se 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[42].

Rector

Persona a cuyo cargo está la estructura de administración/gobernanza de la escuela.

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, en línea o fuera de línea, con esa persona". Es "la actividad criminal de hacerse amigo de una niña, un niño o un adolescente [...] con el propósito de persuadir a la niña, el niño o el adolescente de mantener una relación sexual".

Tecnologías de la información y la comunicación

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 computadores, portátiles, tabletas, teléfonos inteligentes, consolas de juegos, televisores y relojes[43]. También incluye otros servicios como la radio y televisión, la banda ancha, los equipos de red y los sistemas de satélite.

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[44].

Herramientas de control parental

41 Western Sydney University, *What is digital literacy?* (¿Qué es la alfabetización digital?).
42 Dr. Andrew K. Przybylski, y otros, "*A Shared Responsibility: Building children's' online resilience*" (Una responsabilidad compartida: crear resiliencia en línea para niños), Virgin Media and Parent Zone, 2014.
43 UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria*, 2014 (véase arriba).
44 UNICEF, *Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry* (Derechos del niño y juegos en línea: oportunidades y problemas para los niños y el sector), 2019.

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. Los programas normalmente estarán protegidos por contraseña[45].

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[46].

Medios de servicios públicos

Se trata de emisoras o medios de comunicación nacionales que han recibido su licencia de transmisión sobre la base de una serie de obligaciones contractuales con el Estado o el Parlamento. Estas obligaciones se han extendido en muchos países en los últimos años para hacer frente a las consecuencias de la transformación digital mediante programas de alfabetización mediática y digital y requisitos para abordar la brecha digital.

Sexteo (sexting)

Por sextear se entiende el envío, recepción o intercambio de contenido sexual autoproducido, como imágenes, mensajes o vídeos, a través del móvil y/o Internet[47] . 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 tomadas por ellos mismos, los adultos no deben verlas. El hecho de que un adulto intercambie imágenes sexuales con un niño es siempre un acto delictivo, que puede ser perjudicial y que puede requerir la denuncia y eliminación de esas imágenes.

Sextorsión o extorsión sexual de niños

La sextorsión 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

45 UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria*, 2014 (véase arriba).
46 US Federal Trade Commission, *Children's Online Privacy Protection Act* (Ley de protección de la privacidad en línea del menor), 1998.
47 Las Orientaciones de Luxemburgo, 2016 (véase arriba).

de publicar dichas imágenes sin el consentimiento de la persona en cuestión (por ejemplo, colgando las imágenes en las redes sociales)"[48].

Internet de las cosas

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[49].

URL

Es la sigla utilizada para 'localizador uniforme de recursos', es decir, la dirección de una página web de Internet[50].

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[51].

WiFi

WiFi (Wireless Fidelity o fidelidad inalámbrica) es el conjunto de normas técnicas que permiten la transmisión de datos a través de redes inalámbricas[52].

48 Las Orientaciones de Luxemburgo, 2016 (véase arriba).
49 Comisión Europea, *Policy*: *The Internet of Things* (Política: la Internet de las cosas).
50 UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria*, 2014 (véase arriba).
51 NASA, *Virtual Reality: Definition and Requirements* (Realidad virtual: definiciones y requisitos).
52 US Federal Trade Commission, *Children's Online Privacy Protection Act* (Ley de protección de la privacidad en línea del menor), 1998.

Con el apoyo de:

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

ISBN: 978-92-61-30413-3

Publicado en Suiza
Ginebra, 2020