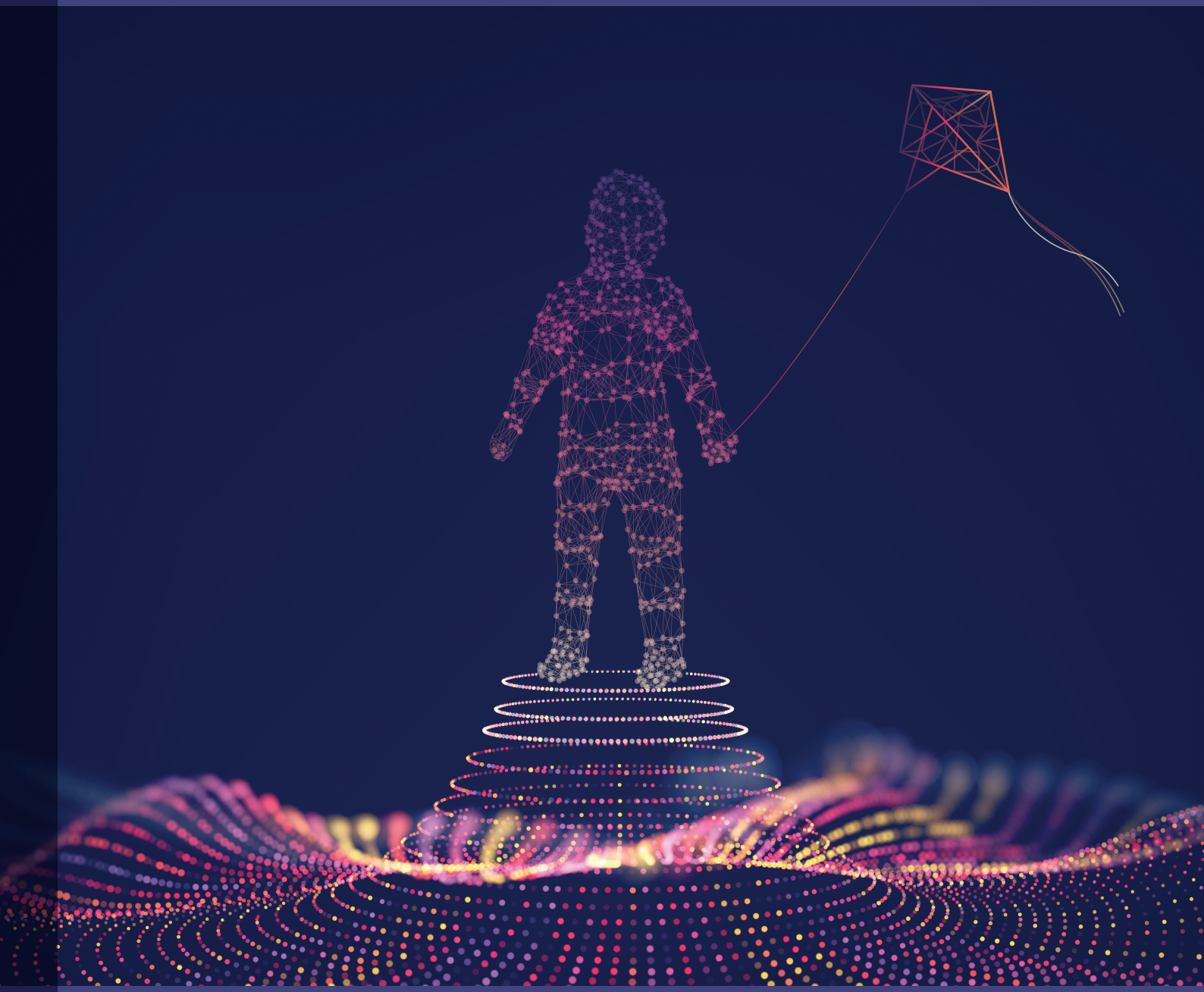


Seguridad de los niños en línea:

Minimizando el riesgo de la violencia, el abuso y la explotación en línea.

Octubre de 2019

BROADBAND COMMISSION
FOR SUSTAINABLE DEVELOPMENT

Seguridad de los niños en línea: Minimizando el riesgo de la violencia, el abuso y la explotación en línea.

Octubre de 2019

Esta traducción no fue creada por la Unión Internacional de Telecomunicaciones (UIT) ni la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). Ni la UIT ni la UNESCO son responsables del contenido o la precisión de esta traducción. La edición original en inglés será la edición vinculante y auténtica.

Este informe se llevó a cabo por medio de un proceso de interacción y colaboración, y con la experiencia de los participantes del Grupo de trabajo para la seguridad en línea de los niños de la Comisión de Banda Ancha para el Desarrollo Sostenible (Broadband Commission for Sustainable Development). Este Grupo de trabajo fue creado como una iniciativa de la Comisión de Banda Ancha y forman parte de este comisionados y expertos externos.

La coordinación de los expertos externos y el desarrollo del contenido se llevaron a cabo bajo la dirección de la Dra. Joanna Rubinstein (presidenta y directora ejecutiva de World Childhood Foundation USA) y Scott Gegenheimer (director general de Zain). El proceso mediante el cual se elaboró el reporte fue posible gracias a la ayuda de Doreen Bogdan-Martin (Directora de la Oficina de Desarrollo de las Telecomunicaciones), Carla Licciardello (Coordinadora de la Iniciativa de Protección de Niños en línea) y Anna Polomska de la Secretaría de la Comisión de Banda Ancha de la Unión Internacional de Telecomunicaciones (UIT).

Los comisionados de la Comisión de Banda Ancha, encargados de los ejes temáticos de los comisionados, y en particular, los miembros del Grupo de trabajo, ofrecieron una ayuda invaluable.

Miembros del grupo de trabajo

Comisionados de la Comisión de Banda Ancha:

Scott GEGENHEIMER (copresidente)
Zain

Dra. Joanna RUBINSTEIN (copresidenta)
World Childhood Foundation USA

Audrey AZOULAY (covicepresidenta)
UNESCO

Ms. Doreen BOGDAN-MARTIN
Directora de la Oficina de Desarrollo de las Telecomunicaciones

Bocar BA
Consejo de telecomunicaciones de SAMENA

Dra. Yee-Cheong LEE
ISTIC

Marcin CICHY
UKE, Polonia

Börje EKHOLM
Grupo Ericsson

Kristalina GEORGIEVA
Banco Mundial

Mats GRANRYD
GSMA

Dr. Carlos M. JARQUE
América Móvil

Baronesa Beeban KIDRON
Presidenta de 5Rights Foundation

Adrian LOVETT
Web Foundation

S. E. Hamad Obaid Al MANSOORI
Emiratos Árabes Unidos

Kevin MARTIN
Facebook

Paul MITCHELL
Microsoft Corporation

Sunil Bharti MITTAL
Bharti Enterprises

Dra. Speranza NDEGE
Kenyatta University

Denis O'BRIEN
Digicel Group

Dr. Abdulaziz Bin Salem AL RUWAIS
Communications and Information Technology Commission, Reino de Arabia Saudita

Sun YAFANG
Huawei Technologies

Expertos externos:

Uri Sadeh
INTERPOL

Dr. Howard TAYLOR
Global Partnership to End Violence Against Children

John CARR
Consultor independiente

Paul SHAPIRO
ICMEC

Susie HARGREAVES
WePROTECT Global Alliance and Internet Watch Foundation

Robbert VAN DER BERG
ECPAT

Anna BORGSTROM
NetClean

Dra. Yuhyun PARK
World Economic Forum y DQ Institute

Johan DENNELIND y Heddy RING
Telia Company

Amandeep SINGH
Panel de Alto Nivel del Secretario General de las Naciones Unidas sobre la Cooperación Digital

Julie CORDUA
Thorn

Charlotte Petri GORNITZKA y Jasmine BYRNE
UNICEF

Elizabeth LETOURNEAU
Universidad Johns Hopkins

Ernesto CAFFO
Telefono Azzurro

Helen MASON
Child Helpline International

Dushica NAUMOVSKA
INHOPE

Un especial agradecimiento a quienes con su apoyo hicieron posible este informe:

Jennifer SULEIMAN
Zain

Lina FERNANDEZ DEL PORTILLO
World Childhood Foundation USA

ÍNDICE

Prólogo 5

Resumen ejecutivo 9

Introducción 15

¿Cómo sería un entorno más seguro? 21
- Un niño está más seguro cuando cuenta con un marco legal sólido que lo proteja 23
- Una cultura corporativa que promueve activamente la seguridad de los niños 23
- Un niño está más seguro cuando conoce sus derechos 24
- El papel fundamental de la educación para construir un entorno más seguro para los niños 24
- Cómo garantizar la seguridad de los niños desde el diseño de los productos 25
- El papel de la tecnología para que los niños estén "más seguros" en línea 26
- Un resumen de lo que significa estar "más seguros" 27

Situación actual de los niños en línea 29
- Por qué debemos actuar ahora para proteger a los niños 32
- Alcance del material de abuso sexual de niños (MASN) en línea 33
- Riesgos de contacto: grooming, cyberbullying, acecho y hostigamiento 34
- Riesgos de contenido: pornografía, MASN, violencia, extremismo, juegos y apuestas en línea 35
- Riesgos de comportamiento: mal uso de los datos, gastos no autorizados y comportamiento inapropiado 36
- Riesgos de los contratos: ¿qué tan bien informado es el consentimiento de un niño en línea? 37
- Resumen de la situación actual de los niños en línea 37

Oportunidades 39
- Inteligencia artificial y la lucha contra la explotación de niños en línea 40
- Otros tipos de tecnologías emergentes 40
- Aumento de la cooperación internacional 41

Amenazas y el entorno amenazador 43
- Vacíos en las políticas y leyes nacionales 45
- Las leyes sobre ciberseguridad necesitan modernizarse 45
- Falta de sistemas de rendición de cuentas y estándares obligatorios 46
- Necesidad de conocer y monitorear a delincuentes 47
- Las amenazas provenientes del mal uso de la tecnología 48
- Los vacíos en la tecnología permiten el abuso y la explotación 49
- El crecimiento de la red oscura (*darknet*) 49
- El rol del entorno sociocultural de los niños 50
- Responsabilidades de los principales interesados 50

El papel del sector privado 53

Recomendaciones 57

Disposiciones modelo sobre protección de los niños para incluir en el plan nacional de banda ancha 61

Conclusiones 65

Casos de estudio y mejores prácticas 69

Glosario 77

Referencias bibliográficas 79

Materiales adicionales 87

Prólogo 1



Prólogo de la Dra. Joanna Rubinstein, presidenta y directora general de World Childhood Foundation USA, y Scott Gegenheimer, director ejecutivo de Zain Group

Los Objetivos de Desarrollo Sostenible adoptados por todas las naciones del mundo en 2015 y la Convención sobre los Derechos del Niño que es un documento legal vinculante, el cual este año celebra su 30° aniversario, representan el compromiso global por un mejor futuro para todos, especialmente para los niños; para nuestra próxima generación, para mantenerlos saludables, ofrecerles acceso a la educación, al entretenimiento y a las nuevas habilidades que les aseguren el poder ser empleados en el futuro; y protegerlos de cualquier tipo de violencia, negligencia o tortura. Para ofrecerles un futuro.

Proteger a los niños no solo es nuestro deber moral, sino también es una buena práctica apoyar su desarrollo saludable y feliz. Depende de nosotros asegurar un camino para un futuro sostenible para todos. Para que esto suceda, los adultos, ya sean los padres, cuidadores, maestros, legisladores, el sector privado y otras partes interesadas, debemos garantizar que los niños alcancen su máximo potencial.

Para que este compromiso se convierta en una realidad, la Comisión de Banda Ancha para el Desarrollo Sostenible creó un equipo de trabajo conformado por diversos sectores dedicado al estudio de la seguridad de los niños en línea como un asunto global. El grupo estuvo conformado por representantes de alto nivel de agencias de la ONU y una variedad de organizaciones públicas y privadas.

Al grupo de trabajo se le dio la tarea de crear un informe que reuniera la evidencia disponible en cuanto al alcance y la naturaleza de los peligros y daños que enfrentan los niños en línea y dar recomendaciones que se puedan llevar a la práctica para dar prioridad a la seguridad de los niños en línea.

La conectividad a la banda ancha es un facilitador fundamental para el futuro de los niños. Esto ayuda a alcanzar las metas de desarrollo sostenible y a asegurar que todos los niños tengan las mismas oportunidades para progresar y así ningún niño se quede atrás.

El Internet ya ha transformado nuestras vidas a un ritmo y escala sin precedentes. Para los niños en países desarrollados el mundo digital es el mundo en el cual han nacido y en el que viven todos los días. Se están convirtiendo en la generación 5G y, en definitiva, en la generación lista para la 4.ª revolución industrial, con el Internet de las cosas (IdC), la robótica, la realidad virtual (RV) y la inteligencia artificial (IA) que están transformando la manera en que vivimos y trabajamos.

Muchos adultos ven el Internet de una manera instrumental, como una herramienta que utilizan ocasionalmente para lograr algo específico. Los niños no. Para muchos de ellos, el Internet y las tecnologías relacionadas con este están completamente integradas en la forma en que viven sus vidas a lo largo de una amplia variedad de actividades cotidianas. El Internet es al mismo tiempo una parte y una extensión de sus vidas: la manera más importante en que se comunican o interactúan para hacer su tarea, con los amigos, la escuela, sus grupos favoritos y clubes deportivos e incluso con sus familiares.

Teniendo esto en cuenta, el objetivo de la Comisión de Banda Ancha es convertir la conectividad en un derecho universal y asegurar que todos los niños tengan el acceso al Internet y a los beneficios que este les ofrece. ¿Qué significa esto en cifras? Hoy en día los niños representan una tercera parte de los usuarios de Internet. Aunque se benefician enormemente de la conectividad para su educación y para su entretenimiento, también están expuestos a grandes peligros y amenazas en línea, que incluyen varias formas de violencia y explotación, como la explotación y abuso sexual de niños (EASN), el acoso, la radicalización y más.

Los desafíos que existen para combatir el lado oscuro de la conectividad son enormes. Si no actuamos ya, la explotación de niños en línea podría ahora alcanzar niveles todavía más alarmantes a la vez que se amplía la banda ancha hacia los países en desarrollo en donde viven hoy la mayoría de los niños. A menudo, en estos nuevos territorios digitalizados, las infraestructuras educativas y de aplicación de la ley tendrán dificultades para seguirles el paso a los sofisticados y decididos criminales que abusan de las plataformas y de los servicios digitales. Contar con una estrategia global unificada es más importante y urgente que nunca.

El objetivo de este informe es aumentar la prioridad de la seguridad de los niños en línea entre los principales involucrados y encargados de los gobiernos, el sector privado, la sociedad civil, las organizaciones no gubernamentales y el mundo académico. Las recomendaciones del informe se pueden poner en práctica y son un llamado a la acción conjunta. Tienen como fundamento el conocimiento y el dominio en la materia de los principales grupos de expertos que cuentan con una vasta experiencia y compromiso en la lucha de las diferentes formas de violencia contra los niños en línea.

El hecho de que 22 comisionados se hayan unido al grupo de trabajo es una muestra del compromiso que tiene la Comisión de Banda Ancha para el Desarrollo Sostenible en darle prioridad a los niños en nuestra agenda común.

Estamos muy agradecidos con cada uno de los miembros del grupo de trabajo, los comisionados y los más de 20 expertos, por su participación en el desarrollo de este informe y por sus recomendaciones. Esperamos que estas ayuden como catalizador para llevar a cabo acciones urgentes para afrontar la seguridad de los niños en línea.

Sabemos que es labor de todos el mantener a los niños a salvo tanto en línea como fuera de ella. Por esa razón, confiamos en que cada uno de los interesados le de prioridad a la niñez y colabore y genere acciones colectivas para prevenir y tratar todas las formas de violencia, abuso y explotación de niños en línea.

La travesía de los niños en el mundo digital y su seguridad en el mundo real, el cual todos estamos construyendo, es asunto de todos.

Gracias

Scott Gegenheimer, director general de Zain Group

Dra. Joanna Rubinstein, presidenta y directora general de World Childhood Foundation USA

Resumen ejecutivo

2



Resumen ejecutivo

Hoy más que en otras épocas la conectividad accesible y confiable está llegando a más países. Esto tiene el potencial de transformar las vidas de los niños al ofrecerles el acceso a oportunidades educativas, culturales y económicas antes inimaginables. Pero muy a menudo, los niños no se percatan de estas oportunidades, ya que el Internet también es un lugar donde los vulnerables están expuestos al riesgo de graves peligros.

Existen 2200 millones de personas menores de 18 años en el planeta, convirtiendo a los niños en el grupo más vulnerable en nuestras sociedades [1].

En todo el mundo, los niños se encuentran constantemente expuestos a los peligros y amenazas en línea, los cuales incluyen:

- Abuso sexual, explotación y tráfico; que van desde el grooming hasta la violación, y que los perpetradores graban y suben a la red.
- Acoso en línea, victimización y cyberbullying.
- Radicalización y reclutamiento por parte de organizaciones de extremistas.
- Estar expuestos a desinformación y contenido no apropiado para su edad, como pornografía y violencia.
- Aplicaciones y juegos diseñados para fomentar hábitos y comportamientos dañinos.
- Ser víctimas de recolección ilegal o inmoral de información y robo de la misma.
- La normalización de la violencia de género a través de la exposición de material abusivo en línea.

Para combatir estos peligros y riesgos se requiere una estrategia coordinada a nivel mundial. Desafortunadamente, la lucha contra el abuso y la explotación de niños en línea no es unificada ni se lleva a cabo de forma consistente por parte de todos los países. La capacidad, la infraestructura legal, el conocimiento, la carencia de recursos destinados específicamente al tema y la voluntad de actuar varían ampliamente entre las diferentes agencias y jurisdicciones.

Riesgos y peligros en línea

De acuerdo a estudios recientes:

- En el 2018, el National Center for Missing & Exploited Children (Centro nacional de niños extraviados y explotados, o NCMEC) de los EE. UU., recibió 18.4 millones de denuncias de material de abuso sexual de niños (MASN) en línea [2].
- En un estudio reciente se descubrió que el 17 % de los padres afirmaron que sus hijos habían sido víctimas de cyberbullying. En algunos países, ese número sube hasta el 37 % [3].
- De acuerdo con el informe de DQ Impact Report del 2017, en 29 países el 56 % de los niños entre 8 y 12 años han estado exuestos demasiado tiempo frente a la pantalla y por lo menos a un ciberriesgo en promedio: incluyendo cyberbullying, adicción a videojuegos, comportamiento sexual y encuentros fuera de línea [4].
- Uno de cada cinco niños entre 9 y 17 años ven material sexual autogenerado en línea y el 25 % de ellos afirmaron haber sentido miedo o angustia extrema [5].
- Un estudio del 2019 encontró que el 99 % de los términos y condiciones en línea están redactados en un lenguaje demasiado complejo como para que los niños puedan entenderlo [6].
- El número de imágenes y videos ilegales confirmado por las líneas de ayuda en Internet del sitio INHOPE aumentó en un 83 % del 2016 al 2018*.
- INHOPE también reportó que la prevalencia de niños preadolescentes (de 3 a 13 años) que aparecen en imágenes y videos de EASN aumentó de 56 % de todo el material ilegal (122.276) en el 2016, a 79 % (148.041) en el 2017 y 89 % (223.999) en el 2018*.

*Informe anual de INHOPE de 2018: http://88.208.218.79/Libraries/IC-CAM_IHRMS/INHOPE_Statistics_Report_2018.sflb.ashx

La Organización Mundial de la Salud (OMS) calcula que 200 millones de niños son abusados sexualmente cada año [7]. Y cada vez más, gran parte de este abuso se lleva a cabo en línea o se registra y distribuye de manera digital. En este caso, el Internet facilita el abuso y la explotación.

Entre los problemas que actualmente obstaculizan la lucha contra la explotación y demás formas de abuso de niños en línea, algunas de las más graves son:

- La falta de uniformidad entre todas las jurisdicciones, y en el caso de algunas jurisdicciones, la falta de leyes que abarquen específicamente los crímenes de abuso de niños que se comenten en línea.
- La falta de regulaciones y leyes que hagan responsables a los proveedores de servicios del material de abuso de niños (MAN) contenido en sus plataformas.
- La falta de estándares, definiciones y formatos de colaboración transfronterizos, que hace más dificil estimar la dimesion del problema y cooperar ampliamente en su eliminación.
- Muchos países no tienen la capacidad, ni la infraestructura para involucrar a todos los sectores de los cuales se requiere la cooperación, si queremos eliminar el abuso de niños en línea.

- La falta de datos e investigación que aborden el problema a nivel mundial (incluso dentro de este informe, muchas de las estadísticas que usamos, por necesidad, provienen del hemisferio norte).

- La naturaleza de los espacios, a menudo no moderados, en los que los niños pasan tiempo en línea (redes sociales, plataformas de mensajería, aplicaciones de transmisión en vivo, espacios virtuales, juegos interactivos, etc.).

- Lo difícil que es controlar el tráfico en Internet, aunado al surgimiento de nuevas tecnologías tales como teléfonos inteligentes más accesibles, equipados con cámaras y video cámaras de alta resolución, mensajería con fotos, transmisión en vivo, y con mensajería cifrada, todo lo cual hace más difícil la prevención del abuso de niños en línea.

- Las tecnologías digitales a menudo están diseñadas sin tener en consideración las diferentes maneras en que estas pueden usarse para explotar o abusar de los niños.

- La naciente adopción y uso de las tecnologías diseñadas para detectar y enfrentar el peligro y la explotación en línea, así como los esfuerzos redoblados para desarrollar y aplicar dichas tecnologías. Existe una clara y apremiante necesidad de compartir prácticas fundadas en buena y comprobada evidencia para prevenir y reducir la agresión.

- Las actitudes sociales y otros factores del ambiente que en algunos países y culturas facilita a los abusadores victimizar a los niños y pasar inadvertidos.

- La brecha generacional digital en la que padres, cuidadores, educadores y legisladores a menudo están mal preparados para entender las vidas digitales de los niños, o para ayudarles a comprender y evitar los peligros en línea.

- La poca financiación, el limitado conocimiento y el fracaso en construir y compartir las buenas prácticas en la protección de niños en línea.

La relación entre la seguridad de los niños en línea y el desarrollo sostenible

Estas prácticas no solo son un agravio a los derechos más fundamentales de los niños, sino que además amenazan con debilitar los beneficios potenciales que la transformación digital puede traer a todos los países, pero particularmente a las sociedades en desarrollo del hemisferio sur.

La UIT calcula que por cada 10 % de aumento en la penetración de los servicios digitales, un país puede esperar 1.3 por ciento de crecimiento del PIB per capita [8]. Sin embargo, estos beneficios solo pueden materializarse si todos los ciudadanos, incluyendo a los niños, son capaces de obtener el mayor provecho posible de las oportunidades que la conectividad ofrece. Y esto solo lo pueden hacer si están seguros cuando están en línea.

Por estas razones, los Objetivos de Desarrollo Sostenible (ODS) de la ONU también establecen una meta bajo el ODS 16.2 para acabar con el abuso, la explotación, el tráfico, la tortura y todas las formas de violencia en contra de los niños para el 2030. Para dar vida a la acción que se requiere si queremos lograr esta ambiciosa meta, el Grupo de trabajo ha redactado una Declaración Universal para la Seguridad de los Niños en Línea.

En la declaración se describen las medidas que deben tomar las entidades públicas y privadas para salvaguardar a los niños en línea. Nuestra petición es que todos los estados, así como las entidades privadas de relevancia, firmen la declaración y se comprometan a llevar a la práctica estos principios. Para leer y firmar la declaración visite: **www.childonlinesafety.org**

Acerca del informe

El informe lo llevó a cabo el grupo de trabajo para la Seguridad de los niños en línea de la Comisión de Banda Ancha. Este grupo de trabajo intersectorial está dedicado a tratar la seguridad de los niños en línea como un tema a nivel global. Está conformado por representantes de alto nivel de organismos a nivel mundial que incluyen agencias de la ONU, organizaciones no gubernamentales (ONG), agencias policiales, organismos reguladores y compañías privadas. Para una lista completa de los miembros, vaya a la página 2.

Introducción

3



Por qué debemos adoptar medidas ahora para proteger a los niños en línea

La Comisión de Banda Ancha para el Desarrollo Sostenible trabaja con estados miembros de la ONU y con otras organizaciones importantes para promover el alcance de la disponibilidad del Internet de banda ancha, principalmente en áreas donde la población está actualmente desatendida.

Al reconocer el papel de transformación que tiene la conectividad, la Comisión ha decidido darle prioridad al avance de la conectividad en masa, debido a que la evidencia con la que se cuenta ha demostrado que el estar conectado fomenta el crecimiento económico y las oportunidades.

La Comisión se ha puesto sus propias metas para asegurar que, para el 2025:

- El 75 % de la población mundial esté conectada en línea.
- El 60 % de los niños tenga por lo menos el dominio digital básico.
- El 40 % de la población mundial cuente con servicios financieros digitales.
- Las mujeres y las niñas tengan el mismo acceso a los beneficios de la conectividad.

Para alcanzar estas metas y hacer realidad los beneficios que obtendrán, es fundamental que las herramientas y servicios digitales estén accesibles para todos por igual. Esto no se puede llevar a cabo si se deja a los grupos vulnerables sin la protección adecuada. Los niños son, por mucho, el grupo demográfico más vulnerable.

En un estudio reciente de la UIT y la UNESCO se descubrió que más del 50 % de la población mundial tiene hoy acceso a Internet [9]. Los niños representan más del 30 % de los usuarios de Internet. Para el 2022, se añadirán a esta cifra 1200 millones de nuevos usuarios, siendo los niños el grupo demográfico en línea de mayor crecimiento [10]. Incluso los países del mundo menos desarrollados están en camino a tener cobertura de Internet móvil universal dentro de unos cuantos años [11].

Este auge en la conectividad beneficiará a toda la humanidad, particularmente a los países con ingresos medios y bajos entre cuyas poblaciones aún existe una demanda de oportunidades económicas, culturales y educativas sin cubrir, que el acceso a Internet puede proporcionar.

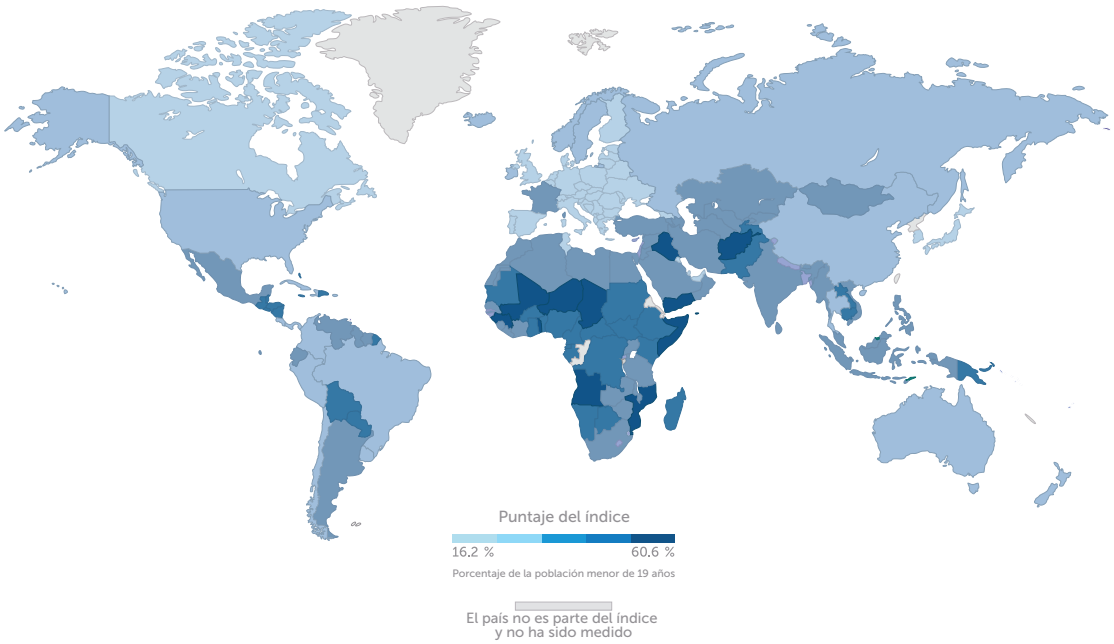
Desde el 2011, 1200 millones de personas han abierto su primera cuenta bancaria. Esto les ha permitido participar más de lleno en los mercados locales e internacionales. Esto se ha logrado en gran parte gracias al crecimiento de la inclusión digital y en línea, particularmente a través del acceso a la banca móvil [12].

Un estudio de la UIT demuestra que el aumento de la tasa de ingreso a los servicios digitales estimula el crecimiento económico de los países [8]. El acceso seguro al Internet también aumenta las posibilidades de conseguir empleo en más de un 13 % [8]. Y esta adopción tiene una relación directa con un aumento en los sueldos de un 2.3 % [8].

No podemos subestimar estos resultados positivos. A nivel global, existen más de 2200 millones de niños menores de 18 años [1]. En algunos países en vías de desarrollo, los niños representan cerca de un 50 % de la población [13]. Para poder desarrollar todo el potencial que ofrece la transformación digital a nivel global, estos niños deberán tener acceso a toda la gama de oportunidades que el Internet ofrece, de manera segura.

Desafortunadamente, sabemos por la experiencia en los mercados desarrollados que, sin las salvaguardas apropiadas, el Internet puede ser un medio complicado (y peligroso para algunos) en el cual desenvolverse.

¿En dónde viven los niños?



Fuente: Organización de las Naciones Unidas, Departamento de Asuntos Económicos y Sociales, División de Población (2019). World Population Prospects 2019, Edición en línea.

La mayoría de los niños vive en el hemisferio sur, particularmente en África, en países en donde aún se encuentran en el proceso de digitalización.

> Como dijo un niño, cuando los investigadores le pidieron que explicara por qué los jóvenes necesitan ser escuchados respecto al tema de la seguridad en Internet: "Es importante que los jóvenes opinen sobre estas cosas porque mucha gente mayor trata de pensar sobre cómo sería ser un joven en el Internet, pero no se dan cuenta de lo vulnerables que son los jóvenes. Así que, es importante que los jóvenes tengamos la oportunidad de hablar por nosotros mismos" [14].

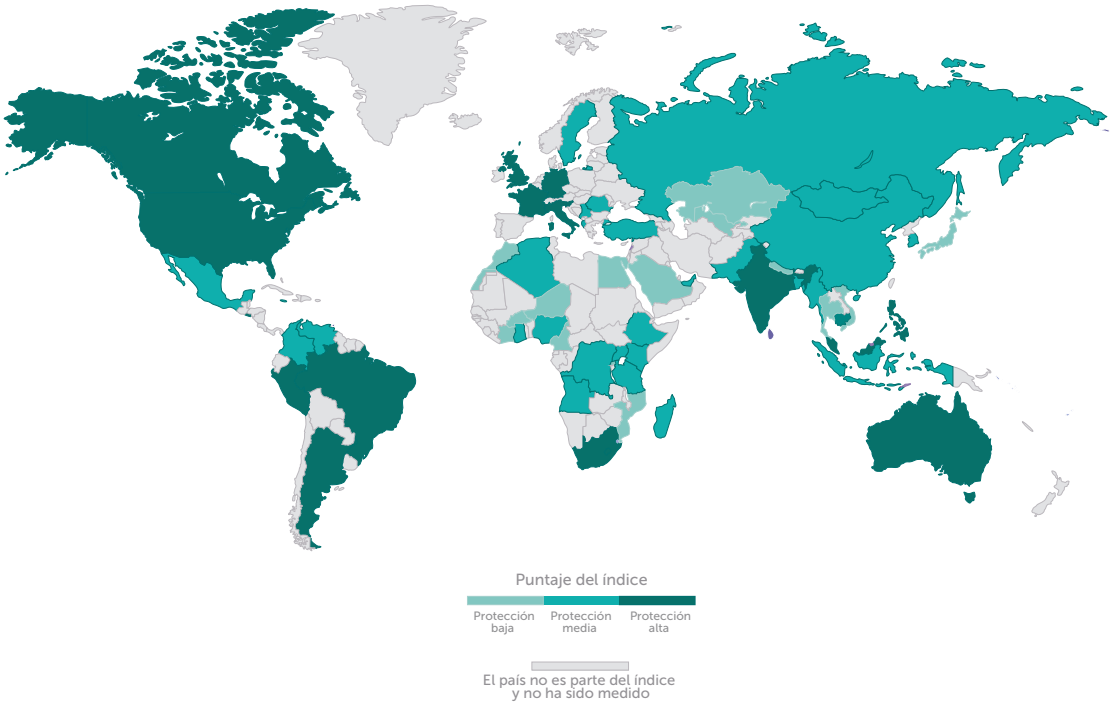
Los niños se enfrentan a toda una gama de peligros y riesgos cuando están en línea, desde servicios pobremente diseñados que los engañan (intencionalmente o no) con contratos no apropiados para su edad, por medio de cyberbullying y exponiéndolos a contenido inadecuado, directamente hasta el acoso grave, grooming en línea, radicalización y explotación y abuso sexual. Es trabajo de los adultos encontrar una manera de mitigar y prevenir estos daños y riesgos.

Por medio de los resultados de la más reciente investigación, este informe describe la amplia gama de riesgos que los niños enfrentan cuando están en línea. Ofrece una idea de la escala y la naturaleza de esos riesgos y recomienda pasos concretos y factibles que los diferentes actores pueden dar para minimizar los riesgos, amenazas, y daños, y para hacer que los niños estén más seguros en línea.

Ejemplos de la escala y el alcance del problema

- En tan solo un año, la Internet Watch Foundation (Fundación de vigilancia en línea, o IWF) encontró más de 105.000 sitios web con material de abuso sexual de niños [15].
- En el 2018, INHOPE confirmó 223.999 imágenes y videos en línea mostrando actividad de EASN.
- En un estudio de 2018 se encontró que la mayoría de las apps móviles dirigidas a los niños estaban recabando datos de formas que violaban las normas de protección de datos, y el 19 % estaban recolectando información de identificación personal [16].
- Se calculó que más de un 30 % de los estudiantes de escuela secundaria sufrirán de cyberbullying [17].

Existencia de legislación que busca proteger a los niños del grooming en línea



Fuente: Out of the shadows: shining light on the response to child sexual abuse and exploitation, The Economist Intelligence Unit, 2019.

De los 60 países cubiertos por el Out of the Shadows Index (Índice fuera de la penumbra) de The Economist Intelligence Unit, solo 21 cuentan con legislación específica que prohíbe el grooming en línea.

Dondequiera que podemos reunir información vemos lo mismo, muchas plataformas y servicios en línea no toman las medidas adecuadas para proteger a los niños de una variedad de peligros. En consecuencia, muchos niños inevitablemente son víctimas de estos peligros.

Hemos aprendido de los países que ya han digitalizado sus economías e infraestructura social, que existen medidas concretas que hay que tomar para que los niños estén más seguros en línea.

Entre estas medidas se incluye:

1. Crear una autoridad única con la máxima responsabilidad de la seguridad de los niños en línea en el país.
2. Asegurar que se cuente con una legislación sólida.
3. Garantizar que los productos y servicios sean seguros por defecto desde su concepción.
4. Construir un ecosistema en el cual la prevención, la detección y la intervención trabajen efectivamente y sin problema.
5. Asegurar la cooperación entre las diferentes agencias a nivel nacional y regional, tales como las entidades gubernamentales, el sector privado, la sociedad civil y los institutos de investigación.
6. Educar a niños, padres y cuidadores sobre sus derechos y asegurarse de que sepan a quién recurrir si necesitan ayuda.

Además, deben incluir el contar con información y estadísticas confiables, con consistencia transfronteriza sobre las experiencias en línea de los niños.

Hoy en día, muchas agencias recolectan estadísticas para la población entre 0 y 14 y de 15 a 24 años. Esto hace invisible a los niños. En todas las estadísticas se debería considerar a los niños menores de 18 años como un grupo aparte, para que de esta manera las agencias responsables de su bienestar tengan información precisa, detallada y específica en la cual basar sus estrategias y acciones. También existe una falta de definiciones comunes en las que haya un acuerdo, por ejemplo, el identificar quién es un niño o que constituye una EASN, lo cual dificulta tener un cuadro detallado del estado de la seguridad de los niños en línea a nivel mundial.

Es para corregir esos vacíos que el grupo de trabajo desarrolló este informe con el objetivo de darle prioridad a la seguridad de los niños en línea. El objetivo del grupo de trabajo es ofrecer al lector, y particularmente a los miembros del gobierno, legisladores, compañías en el sector privado, incluyendo proveedores de servicio de Internet (ISP), miembros de la sociedad civil, organizaciones no gubernamentales (ONG) y a intelectuales, un punto de referencia que contenga información sobre la práctica adecuada, respuestas en cuanto a políticas y las herramientas tecnológicas para usar en la lucha contra el abuso y la explotación de los niños en línea.

Aunque ya existen excelentes estudios e informes respecto a la seguridad de los niños en línea, varios de ellos desarrollados por los miembros expertos del grupo de trabajo, a menudo estos informes se centran en un único problema o forma de violencia, que es por lo general la explotación y el abuso sexual en línea. Sin embargo, este es solo un aspecto de la amenaza del entorno en línea. Existen varios temas más, como el cyberbullying, los juegos en línea y la radicalización, solo por mencionar algunos, los cuales debemos tratar de manera colectiva si queremos que los niños aprovechen al máximo las oportunidades que les ofrece la expansión de una conexión por banda ancha rápida y asequible.

El grupo de trabajo reconoce que la mayoría del conocimiento y las herramientas que los países y compañías necesitan para afrontar estos problemas ya están disponibles (para más detalles vea la sección de "recursos" al final de este informe). Sin embargo, están los retos técnicos de la detección y aplicación, muchos de los cuales son ocasionados por el aumento del cifrado en línea. Aunque, un reto aún más grande es la falta de conciencia entre los principales involucrados con influencia y capacidad de toma de decisiones respecto al alcance y la magnitud de los peligros en línea para los niños y las herramientas con las que se cuenta para combatir esos peligros.

Desde 2010, la Iniciativa de Protección de la Infancia en Línea ha tratado estos problemas ofreciendo una plataforma para compartir información y para sensibilizar. Las directrices de Protección de la Infancia en Línea de la UIT abordan con amplitud el tema de la seguridad de los niños en línea, alentando a las partes interesadas a tomar las medidas apropiadas para asegurar la protección de los niños en el mundo digital.

Un obstáculo más que tiene el darle prioridad a la seguridad y al bienestar de los niños, es el estigma relacionado con la discusión de estos temas, especialmente el del abuso sexual de niños. Necesitamos facilitar el acceso al conocimiento y a las herramientas, y dar a quienes estén dispuestos a ser agentes de un cambio positivo los datos y el conocimiento que necesitan para movilizar el compromiso de invertir en la seguridad de los niños en línea.

En este informe, revisamos la situación actual de los niños en línea. ¿Qué oportunidades se les están presentando? ¿Qué riesgos y daños enfrentan? ¿Cómo estos últimos pueden prevenirles de adquirir los anteriores? ¿Y qué podemos hacer para asegurarnos de que esto no suceda? Nuestro principal objetivo y enfoque es cómo dar prioridad a la seguridad en línea para todos los niños, pero en particular a los niños en países de bajos ingresos, en donde las estructuras de salvaguarda están a menudo subdesarrolladas, lo que aumenta el peligro de sufrir daños.

A lo largo del informe, el grupo de trabajo ha hecho su mejor esfuerzo para ofrecer los recursos y sugerencias que serán los apropiados para una gama de mercados, cada uno con su propia variedad de tecnologías, tensiones sociales y otros factores de influencia, reconociendo que una medida única no es la solución. Este informe deberá ser tan útil para lectores en países de ingresos bajos y medios, con altos niveles de penetración de banda ancha móvil pero con poco suministro de línea fija, como para aquellos lectores en mercados más establecidos.

Al trabajar juntos, a través de las fronteras, creemos que podemos construir un ecosistema de Internet que fomente la creatividad y aproveche la energía de la próxima generación. Con la libertad de explorar un mundo digital cada vez más conectado, sin temor a ser lastimados, los niños expandirán sus horizontes y se enfrentarán al reto de desarrollar su potencial al máximo. De esta manera, serán la fuerza de la siguiente ola de crecimiento económico y del cambio social positivo.

Este informe, que está centrado en los niños, complementa el informe del Panel de alto nivel sobre cooperación digital del secretario general de la ONU, el cual ubica la seguridad de los niños en línea dentro del contexto más amplio de los derechos y la cooperación digital.

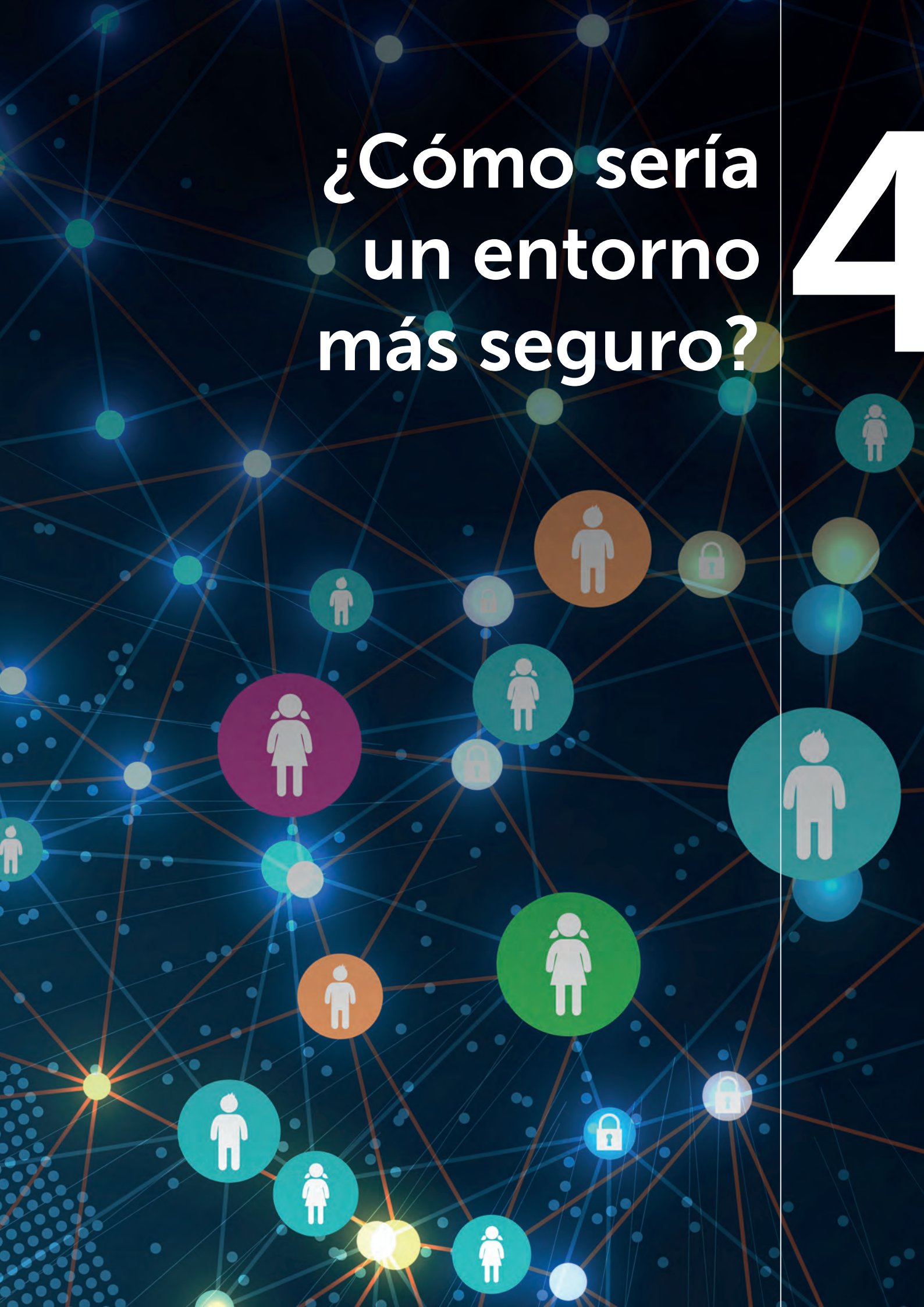
La Declaración universal de la seguridad de los niños en línea ligada a esta informe es una herramienta para ayudar a movilizar y ampliar los compromisos de los gobiernos, el sector privado y la sociedad civil para darle prioridad a la seguridad de los niños en línea por medio de un marco de acciones comunes y concretas.

¿Qué es un niño?

En todo este informe, niño se define como cualquier persona menor de 18 años. Esto es congruente con el Artículo 1 de la Convención sobre los Derechos del Niño (CDN) de la ONU, en el cual se afirma que "un niño es cualquier ser humano menor de 18 años de edad". En la práctica, en algunos mercados se trata como adulto a cualquier persona con suficiente edad para dar su consentimiento para el proceso de sus datos, la cual puede ser de hasta 13 años. Esta asunción no está justificada por evidencia alguna en cuanto a las etapas de desarrollo de la niñez. Menoscaba los derechos de los niños y amenaza su seguridad. Vea la página 70 para conocer un caso práctico que describe el impacto de la CDN respecto a los derechos de la niñez a nivel mundial.

¿Cómo sería un entorno más seguro?

4



¿Cómo sería un entorno más seguro?

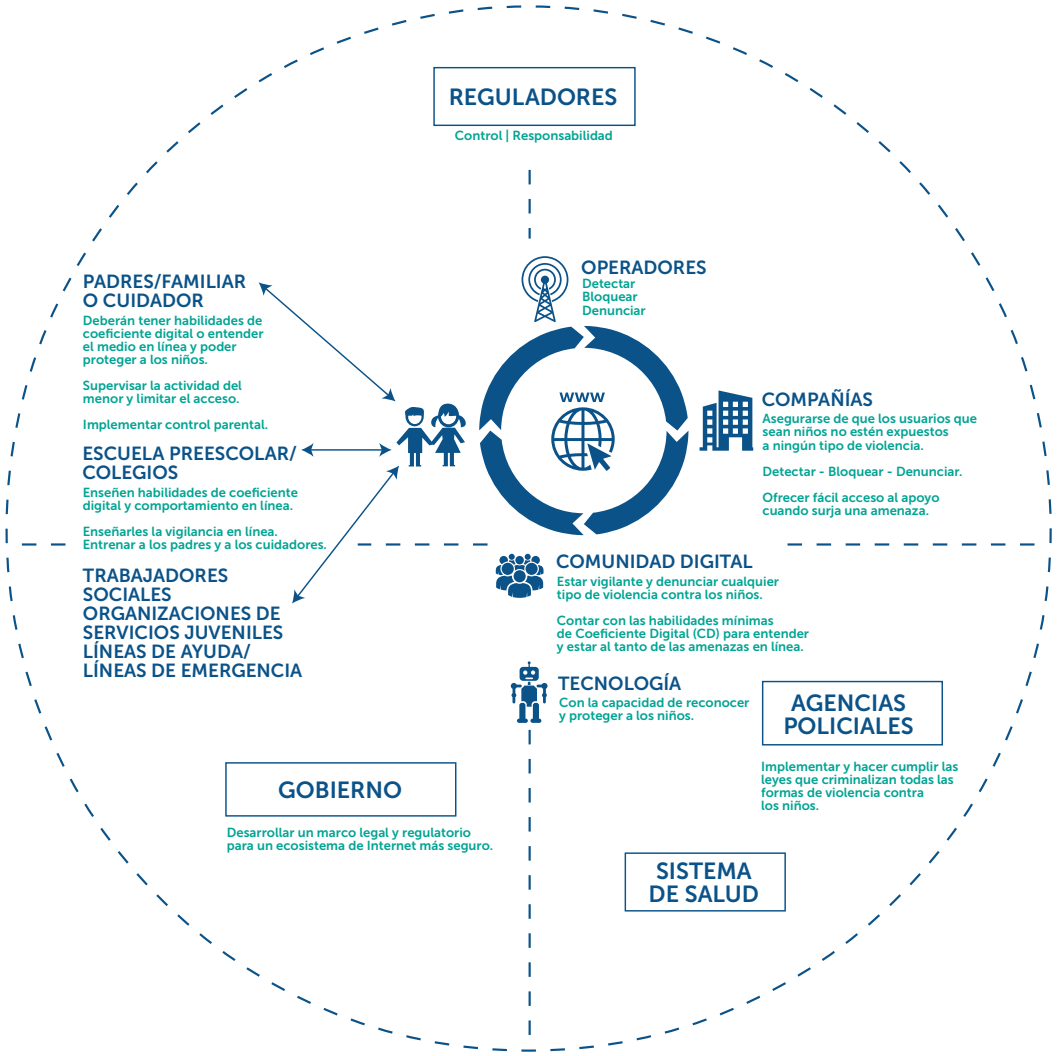
Con frecuencia, millones de niños en países de ingresos bajos y moderados aún en proceso de digitalización, no están protegidos de la manera adecuada. Tenemos que corregir esto con urgencia, para proteger a la niñez y asegurarnos de que obtenga el mayor beneficio posible de estar en línea.

Esto es particularmente importante en países en desarrollo, donde vive hoy un mayor porcentaje de niños.

Estos países son los que más se beneficiarían de la conectividad, al obtener acceso a educación de calidad, entretenimiento, salud y otro tipo de servicios.

Para entender lo que necesitamos hacer para que la niñez esté más segura en línea, primero debemos entender qué significa estar "más seguro". ¿Cómo sería un sistema en el cual la niñez estuviera tan segura como nosotros quisiéramos que estuvieran? ¿Y cómo sería la experiencia de un niño en Internet dentro de este sistema?

Un ecosistema de Internet más seguro



Fuente: Lina Fernández del Portillo.

Para proteger completamente a los niños de cualquier peligro en línea o exposición a riesgos en línea inaceptables, todas las principales partes involucradas deberán estar informadas, empoderadas e involucradas.

Un niño está más seguro cuando cuenta con un marco legal sólido que lo proteja

Para proteger a la niñez del abuso en línea, un país debe contar con una amplia infraestructura legal que defina los derechos de los niños, los delitos cometidos contra los niños y las sanciones para esos delitos. Un buen punto de partida es incorporar las convenciones internacionales vigentes a las leyes nacionales.

Estas convenciones y protocolos internacionales son:

- **La Convención sobre los Derechos del Niño de la ONU (CDN 1989):** en esta se recogen una amplia variedad de derechos para los niños, incluyendo derechos civiles, culturales, económicos, políticos y sociales.
- **Protocolo Facultativo de la Convención sobre los Derechos del Niño, relativos a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (2002):** un sistema para analizar los procesos para afrontar los delitos por material de abuso sexual de niños (MASN).
- **Budapest Convention on Cybercrime (Convenio de Budapest contra la ciberdelincuencia) (2001):** el primer instrumento intergubernamental vinculante que trata con los delitos sobre pornografía infantil que son facilitados por los dispositivos electrónicos.
- **The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Consejo de la convención europea sobre la protección del menor contra la explotación y el abuso sexual) (2007):** trata los delitos de MASN y grooming en línea.

La adopción posterior a 2015 de la Agenda de desarrollo con 17 Objetivos de Desarrollo Sostenible (ODS) de la Asamblea General de la ONU, presenta nuevas oportunidades para darle prioridad a la protección de los niños en línea. Un niño que use el Internet en una jurisdicción que integre estas disposiciones y que se haya incorporado a los ODS, disfrutará de una variedad de derechos positivos. Estos derechos deberán dar forma al medio legal y normativo de los proveedores de servicio de Internet y a las compañías que ofrecen acceso al Internet. Además imponen obligaciones y ofrecen una guía de acción a las agencias responsables del bienestar de los niños.

Para más información, vea la página 62 donde encontrará un modelo de las disposiciones para la protección de los niños en línea, el cual tiene como propósito servir como un formato para uso de los países al momento de actualizar su plan de acción nacional de banda ancha.

Para leer acerca de las iniciativas exitosas que han llevado a cabo las agencias policiales y sus socios en Albania y las Filipinas, vea los casos de estudio y mejores prácticas en las páginas 71 y 72.

Una cultura corporativa que promueve activamente la seguridad de los niños

Para que los niños estén tan seguros en línea como sea posible. En sus Directrices de Protección de la Infancia en Línea para la Industria (PIeL) (2015), UNICEF identifica cinco cosas que las compañías de tecnología deben hacer para proteger a los niños y a los jóvenes que usan sus productos y servicios:

1. Los derechos de los niños deben integrarse en todas las políticas y procesos correspondientes de la compañía.
2. La compañía debe haber incorporado procesos para lidiar con las violaciones a los derechos de los niños.
3. Los medios que ofrecen las compañías tienen que ser apropiados de acuerdo a la edad.
4. La compañía debe educar a los niños, a sus padres y a sus cuidadores respecto a cómo usar los productos de manera responsable.
5. La tecnología digital debe promoverse como un medio para aumentar la participación cívica.

Para más detalles, lea las Directrices de Protección de los Niños en Línea para la Industria de UNICEF: **https://www.unicef.org/csr/files/COP_Guidelines_English.pdf**

Un niño está más seguro cuando conoce sus derechos

Desde la edad más temprana posible, los niños deben saber y entender sus derechos. Esto les da el poder de saber cuando algo está mal para poder advertir a un adulto responsable, y para poder denunciar una violación a sus derechos. Para que esto suceda, maestros y padres también deben entender los derechos de los niños en línea y ser capaces de transmitírselos en un lenguaje que sea apropiado para su edad [18].

El papel fundamental de la educación para construir un entorno más seguro para los niños

Para proteger a los niños; maestros, padres y cuidadores deben contar por lo menos con las habilidades digitales básicas: las suficientes para ayudar a los niños a obtener el máximo beneficio de estar conectados, y al mismo tiempo reconocer y responder de manera adecuada a cualquier peligro. Pero en los mercados que están experimentando una rápida transformación digital, los adultos a menudo no cuentan con el conocimiento para apoyar a sus niños.

El DQ Institute, un centro de estudios internacional dedicado a establecer estándares a nivel global respecto a la educación sobre inteligencia digital, ha definido ocho áreas claves de las aptitudes digitales que debe dominar un niño para estar seguro y tener una experiencia en línea positiva.

Estas ocho áreas son:

- **Identidad digital:** la capacidad de crear y mantener una identidad en línea positiva.
- **Uso digital:** la capacidad de usar la tecnología de forma sana y equilibrada.
- **Salvaguarda digital:** la capacidad de atenuar una serie de riesgos que existen en línea.
- **Seguridad digital:** la capacidad de manejar y evitar los riesgos de dispositivos y datos.
- **Coeficiente emocional (CE) digital:** la capacidad de reconocer, navegar y expresar emociones en línea.
- **Comunicación digital:** la capacidad de comunicarse y colaborar por medio de la tecnología.
- **Alfabetización digital:** la capacidad de encontrar, leer, evaluar, crear y compartir información digital.
- **Derechos digitales:** la capacidad de entender y defender los derechos humanos y legales en línea.

Estas ocho aptitudes son importantes para que un niño disfrute completamente de sus derechos en línea. En algunos casos, esta estrategia ha demostrado ser eficaz. Se demostró que los niños que recibieron capacitación en las ocho aptitudes redujeron el riesgo de sufrir un daño en línea en un 15 % que los niños que no habían recibido capacitación [19].

En las condiciones actuales, la investigación de UNICEF ha descubierto que el 43 % de los niños sudafricanos afirman que muy raras veces o nunca les piden a sus padres consejos sobre lo que ven en línea [20]. Ese número es bastante similar en todos los mercados que fueron estudiados: en Italia, por ejemplo, es del 53 % [21], en Serbia del 46 % [22].

Solamente la educación, que aporte habilidades digitales, incluyendo el derecho de los niños a la seguridad en línea y lo que las partes involucradas pueden hacer para asegurar ese derecho, puede llenar ese vacío. Y la manera más fácil de impartir esta educación es por medio de los profesores, padres y cuidadores. Es por esta razón que enseñar habilidades digitales a todos los niños debería ser un derecho universal.

Los profesores, padres y cuidadores desempeñan un papel fundamental en asegurar que los niños sepan cómo usar la tecnología digital de manera responsable y segura. Por medio de reuniones y seminarios para educadores, alumnos, padres y cuidadores se puede ayudar a sensibilizar a los niños respecto de los peligros que representa el comportamiento riesgoso en línea.

Cómo garantizar la seguridad de los niños desde el diseño de los productos

Para estar lo más seguro posible, a un niño se le debería proporcionar el software, las apps y los sistemas apropiados para su edad y que hayan sido creados pensando en los niños. El software y los servicios diseñados para ser seguros y apropiados para cada edad deberían:

- Tener en cuenta el bienestar de la infancia como principio fundamental del diseño.
- Ser apropiados para cada edad y contar con una función de verificación de edad estricta.
- Ser transparentes y sensibles en cuanto a la manera en que recaban y usan la información personal.
- Recabar y retener solo la información que necesitan para cumplir con su función.
- Contar con políticas y estándares de comportamiento que protejan a los niños de cualquier daño posible.
- Ser instalados con configuraciones que den prioridad a la privacidad sobre todo lo demás.
- Compartir información solo en casos de suma necesidad y en los que el interés del menor esté plenamente definido.
- Incluir comentarios y declaraciones de parte de los niños, los padres y los cuidadores respecto al contenido o comportamientos inapropiados.

Asegurarse de que el software, los programas en Internet, las apps y los sitios web cumplan con estos estándares es una de las maneras más importantes en las que el sector privado, en particular las compañías de tecnología, pueden contribuir a proteger a los niños en línea.

Para que la tecnología sea segura desde su concepción debe contar desde su diseño con protecciones en contra de los siguientes tipos de riesgos:

1. Riesgos de contacto: los niños participan en comunicaciones que pueden llevarles a sufrir daños (esto incluye riesgos como acecho en línea: depredadores que se hacen pasar por niños y observan los patrones de uso de ciertos niños para identificar a los que se sienten solos, o también para identificar posibles víctimas).
2. Riesgos de contenido: los niños pueden ver contenido autogenerado o dañino.
3. Riesgos de conducta: son los comportamientos peligrosos entre niños, por ejemplo el bullying (acoso), mensajes explícitamente sexuales, etc.
4. Riesgos de contratos: los servicios en línea deben asegurarse de que un adulto, y no el menor, dé su consentimiento.

Entre los daños incluidos dentro de estas categorías se encuentran la explotación y el abuso sexual de niños o EASN; tráfico; radicalización; contenido y actividades ilegales o inapropiadas para la edad; contendido que promueve el auto lastimarse; contacto personal dañino o ilegal, como el grooming, el acecho o el bullying. A menudo, estas actividades inapropiadas para la edad están técnicamente permitidas ya que los términos y condiciones de los proveedores en línea no han sido diseñados pensando en los niños.

Lectura adicional

Los organismos reguladores tanto del Reino Unido como de Australia han producido lineamientos claros y extensos para crear sistemas para niños que sean seguros desde su concepción.

En el Reino Unido, el comisionado de información muy pronto presentará el Age Appropriate Design Code (Código de diseño adecuado a la edad), que es un código de práctica reglamentario que presenta las protecciones específicas que los niños necesitan respecto de sus datos [24]. Este ofrecerá a todos los niños menores de 18 años un alto nivel de protección de datos desde su diseño y de manera predeterminada, y se aplicará a todos los servicios a los que muy probablemente accedan los niños.

En Australia, el comisionado de seguridad electrónica (eSafety) ha desarrollado un conjunto de principios fundamentales dedicados a la seguridad y ha comenzado un proyecto para crear un marco que sirva como guía para uso de la industria [25]. El comisionado está dando asesoramiento respecto a las herramientas y los recursos que se necesitan para garantizar que la seguridad del usuario y del menor estén incorporados en el diseño del servicio.

Se puede encontrar más información en **ico.org.uk** y en **www.esafety.gov.au**

El papel de la tecnología para que los niños estén "más seguros" en línea

La tecnología por sí sola no hará que los niños estén más seguros. Una compañía o servicio podría tener disponible el software de protección para niños más sofisticado y aún así, si la seguridad del menor y su derecho no son la base o los pilares para la sensibilización y educación del público, la política, el diseño de productos, y los sistemas de operación, los niños no estarán a salvo. La evidencia más reciente señala que los controles parentales no son tan eficientes para prevenir daños como se pensaba [27].

Dentro de la cultura adecuada y la prevención del crimen, la tecnología desempeña un papel vital, debido a que la mayoría de los servicios cuentan con demasiados usuarios como para ser monitoreados solamente por seres humanos. El sistema adecuado juega un papel esencial para prevenir daños y para llamar la atención de los moderadores humanos respecto de cualquier comportamiento grave.

Entre las tecnologías vigentes con protección para niños se encuentran:

- **Tecnologías de bloqueo:** por lo general operan al nivel de los proveedores de servicio de Internet (ISP). Dichas tecnologías tecnologías reconocen y bloquean los sitios y el contenido que promueve cualquier cosa dañina para los niños.
- **Filtración heurística:** son tecnologías que observan variables como la dirección de IP, el contenido y las palabras clave, y bloquean los sitios que no forman parte de una lista negra pero que pueden tener contenido dañino.
- **Detección automática de material de abuso sexual de niños (MASN):** por medio de soluciones, tales como clasificadores que hacen referencia a listas negras de MASN con codificación tipo *hash*, los proveedores pueden localizar, bloquear o reportar instantáneamente contenido de abuso de niños.
- **Rastreadores web:** a través de la búsqueda de las mismas variables y filtros (palabras clave, imágenes de MASN, etc.), los rastreadores web buscan activamente sitios dañinos para después alertar a las autoridades.

- **Reconocimiento facial:** por medio de tecnología de reconocimiento facial, las autoridades y otros actores de la industria pueden identificar rápidamente a víctimas y perpetradores.

Muchas de estas tecnologías funcionan por medio de inteligencia artificial (IA). Sin ella, no sería posibles la protección en tiempo real a escala ni la localización de patrones en base a tendencias a largo plazo, debido al volumen de datos que se generan en línea todos los días.

Sin embargo, vale la pena dar la voz de alerta. Los expertos en el campo de la IA han descubierto que muchos de los algoritmos están hechos de manera tendenciosa. Por ejemplo, debido a que los algoritmos no controlan suficientemente la correlación con respecto a la causalidad, pueden confundir a los usuarios humanos sobre la percepción que producen para que vean una relación entre dos fenómenos cuando de hecho no existe tal relación [26].

Otro desafío que existe con las soluciones que son completamente automatizadas es que algunos de los riesgos que afectan a los niños, como por ejemplo el grooming y el bullying, dependen del contexto, y dichos sistemas no tienen la capacidad de interpretar el contexto (humano).

Esto puede llevar, entre otras cosas, a resultados impulsados por la IA que sean discriminatorios contra las minorías, las mujeres y las niñas, y otros grupos que están tradicionalmente en desventaja. Debido a estos límites en la tecnología, la intervención y la supervisión humana sigue siendo un elemento de suma importancia en el espacio de la protección al menor en línea. En este momento, ninguna herramienta de protección al menor debe ser usada de manera aislada sin las salvaguardas y protocolos adicionales que aseguren la exactitud de los datos.

Otro desafío que existe es que muchos de los sistemas digitales están dirigidos a los adultos y requieren de toma de decisiones o de acciones con ciertos matices que no son apropiados para los niños. Para contener este problema, debemos garantizar que los sistemas les ofrezcan a los niños protecciones especiales y no esperar que los niños tomen decisiones de adultos.

Un resumen de lo que significa estar "más seguro"

Como conclusión, para que un menor esté lo más seguro posible en línea deberá:

- Estar protegido por un marco jurídico sólido, eficiente y obligatorio que proteja los derechos de los niños.
- Usar soluciones y servicios en línea apropiados para niños, diseñados para protegerlos y para mitigar los riesgos.
- Estar empoderados por un conjunto de capacidades digitales amplias que les permitan a los niños minimizar riesgos y maximizar su potencial en Internet; reconocer cuándo se han violado sus derechos; y contar con el apoyo de adultos que comprendan los derechos de los niños y cómo mantenerlos a salvo en línea, que tengan acceso a mecanismos seguros y confiables para denunciar cualquier violación a esos derechos.

5 Situación actual de los niños en línea



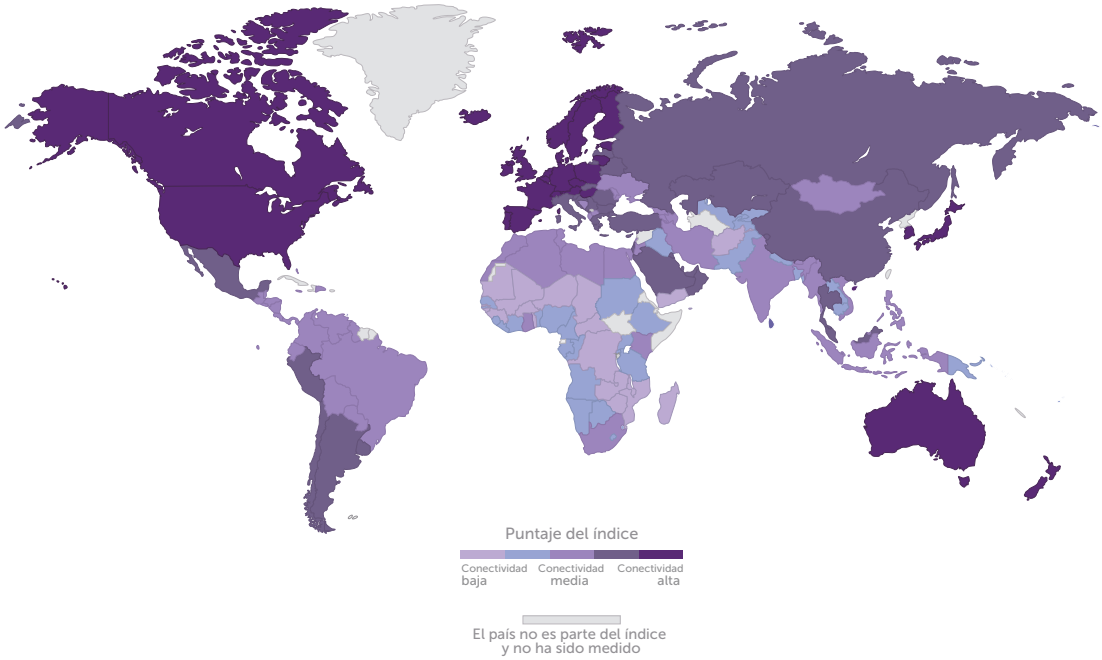
Situación actual de los niños en línea

De acuerdo a la investigación de UNICEF, a nivel mundial, 71 % de los jóvenes están conectados [28]. Además, la disponibilidad de teléfonos inteligentes y el acceso a la banda ancha móvil está facilitando que los jóvenes estén en línea. De acuerdo a la UIT, en los países menos desarrollados (PMD), 35 % de los usuarios de Internet son personas jóvenes, en comparación con 13 % en mercados digitales más establecidos [29].

Sin embargo, aún existen partes del mundo en las que millones de jóvenes siguen esperando conectarse por primera vez. En África, por ejemplo, 60 % de los jóvenes no están todavía conectados [30]. Pero con el número de usuarios de Internet en África que aumenta en un 20 % al año [31], muchos de estos jóvenes pronto estarán conectados. Lo mismo ocurre a nivel global en los países menos desarrollados, en los que el 70 % de los jóvenes todavía no están conectados [29]. Existe también una austera brecha entre género en los países menos desarrollados: las niñas tienen un 71 % menos de probabilidades que los niños de usar Internet [32].

En el África subsahariana, Asia y América Latina, la conectividad no ha llegado aún a todos los niños. Con la expansión de la banda ancha asequible hacia estas partes del mundo en vías de desarrollo, existe una necesidad urgente de implementar las medidas para minimizar los riesgos y amenazas para estos niños, para que al mismo tiempo puedan capitalizar todos los beneficios que el mundo digital puede traer a nuestras sociedades.

Índice de conectividad móvil de GSMA: Situación de la conectividad móvil alrededor del mundo al 2018

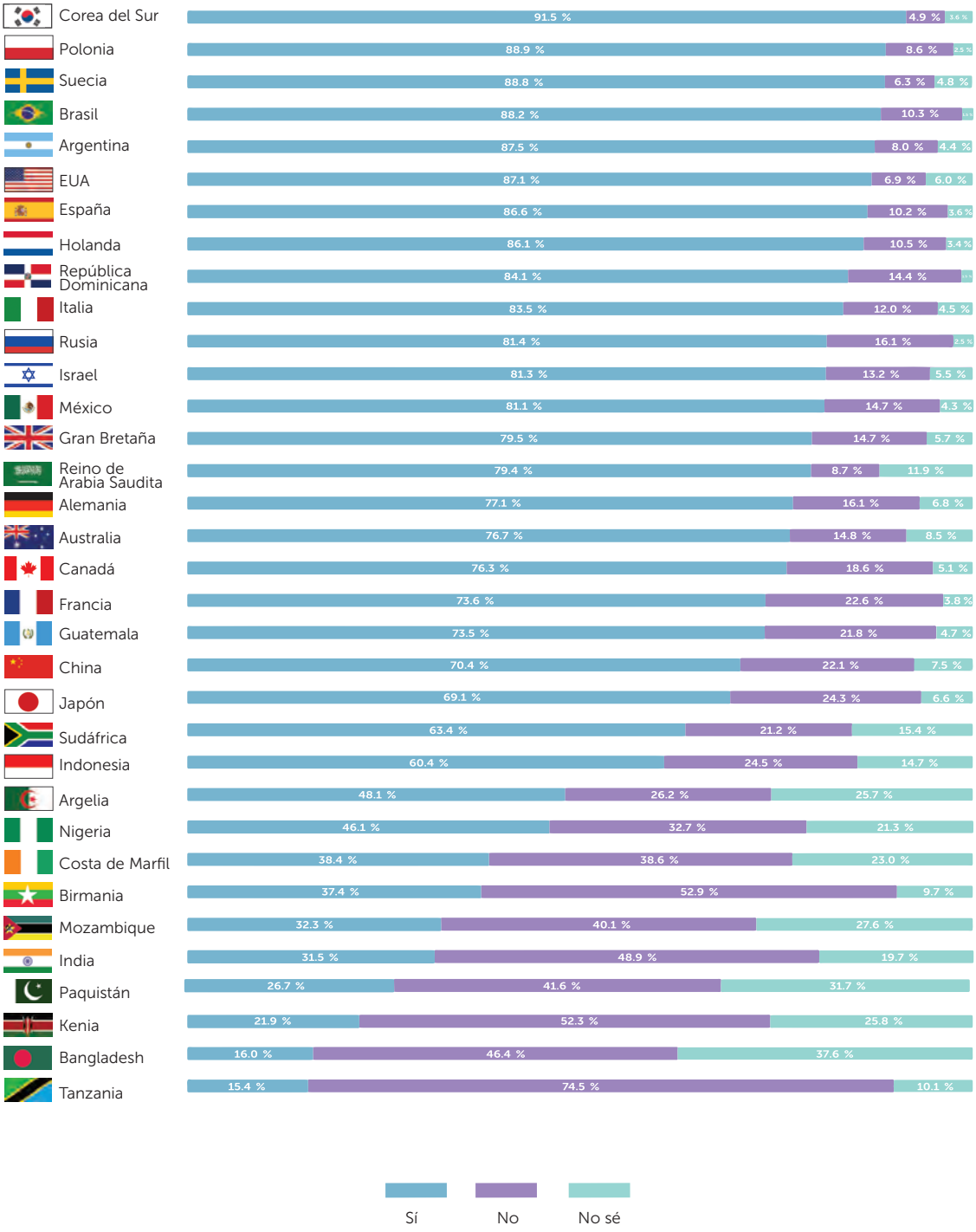


Fuente: Índice de conectividad global 2019 de GSMA, GSMA Intelligence Unit
https://www.mobileconnectivityindex.com/#year=2018

En los países desarrollados, la conectividad móvil se está convirtiendo en algo omnipresente. En el futuro cercano sucederá lo mismo en los países en desarrollo.

Uso de teléfonos móviles por parte de los niños para usar Internet en 34 países.

¿Ha usado su hijo o cualquiera de sus hijos (entre 5 y 17 años) el Internet en un teléfono móvil en los últimos 3 meses?



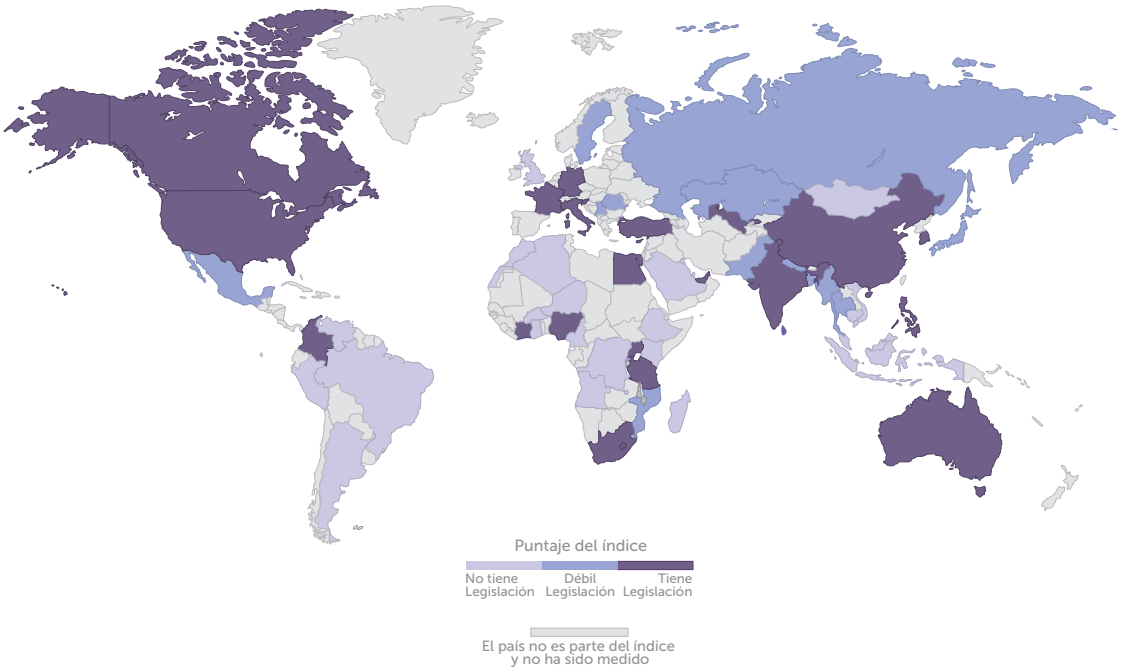
Fuente: GSMA Intelligence Unit

Las encuestas y los estudios muestran que la mayoría de los niños en países desarrollados y en muchos países en vías de desarrollo usan con frecuencia teléfonos móviles para ingresar a Internet.

Por qué debemos actuar ahora para proteger a los niños

Ningún país cuenta con los sistemas perfectos de protección de niños en línea. Incluso en los países con dos décadas de crecimiento de Internet en su haber, a menudo existen vacíos en el ecosistema de protección de niños en línea.

Protección en Internet desde la perspectiva de la legislación
Reporte obligatorio, bloqueo de contenido, detección y registro de MASN



Fuente: Out of the shadows: shining light on the response to child sexual abuse and exploitation, The Economist Intelligence Unit, 2019.

En este caso en particular, el índice descubrió que solo 9 de los 60 países establecieron en su legislación la denuncia obligatoria, el bloqueo de contenido, el eliminar y mantener registros de MASN. Los países que se destacan en esta lista corta son China, India, Filipinas, Sudáfrica, Tanzania y Turquía. De las tres acciones esperadas 11 países solo llevan a cabo dos, y 15 países solo llevan a cabo una. Además, 25 de 60 no hacen nada al respecto sobre este tema en particular.

Si un renovado énfasis a nivel global respecto de la seguridad digital de los niños motivara a reguladores y legisladores a llenar esos vacíos, los efectos positivos para los niños serían profundos. En un gran número de países, se han preguntado si depender de mecanismos de auto regulación para alcanzar un cambio progresivo para los niños sigue siendo el mejor modelo. Las preocupaciones actuales sobre el impacto del cifrado de extremo a extremo en los esfuerzos a nivel global para detectar e interrumpir la distribución de MASN, demuestra la urgencia de estas preguntas [33] [34].

En algunos países en los que se está llevando a cabo la digitalización no existen las leyes, las políticas, las tecnologías ni los sistemas necesarios para mantener a los niños a salvo. Aparte de algunos cuantos ejemplos, como Ruanda (ver el Caso de

estudio 2 en la página 71), la presión para expandir la conectividad no ha estado acompañada por el mismo nivel de esfuerzo para garantizar la seguridad de los niños. Esto no solamente deja a millones de niños y jóvenes en riesgo de sufrir algún daño, sino que también debilita la habilidad de la transformación digital para traer el progreso económico y social.

El alcance del material de abuso sexual de niños (MASN) en línea

De acuerdo con la Organización Mundial de la Salud (OMS), cada año 200 millones de niños sufren de abuso sexual [7]. Y cada vez más, gran parte de este abuso se lleva a cabo en línea o se registra y distribuye de manera digital. En este caso, el Internet facilita el abuso y la explotación.

La base de datos de la INTERPOL sobre el abuso sexual de niños contiene más de 1.5 millones de imágenes y videos, los cuales registran en conjunto el abuso de más de 19.400 víctimas a nivel mundial [35]. En los EE. UU., el National Center for Missing & Exploited Children (Centro nacional de niños extraviados y explotados, o NCMEC) cuenta con una base de datos de más de 25 millones de archivos que contienen imágenes de víctimas menores de edad [36]. Se reconoce que dichas cifras son solo una pequeña fracción de todo el MASN disponible (fotos originales y copias de copias) y que una gran parte pasan desapercibidos. Es alarmante que el número de denuncias cibernéticas que recibe el NCMEC aumentó casi diez veces en tres años, de 1.1 millones en el 2014 a 10.2 millones para el 2017, y casi se duplicó en el 2018 al recibirse 18.4 millones de denuncias.

En el 2018, la Internet Watch Foundation (fundación para la supervisión del Internet, o IWF) anunció un aumento del 32 % en el número de sitios reportados con contenido confirmado de MASN [37]. Descubrieron lo siguiente respecto al contenido de MASN:

- 39 % de las víctimas eran menores de 10 años, 55 % tenían entre 11 y 13 años, y 5 % tenían entre 14 y 15.
- El 78 % del MASN representaba niñas, el 17 % representaba niños, y el 4 % representaba ambos sexos.
- El 23 % de todo el MASN en línea en el 2018 era del tipo más grave, incluyendo imágenes de violación y tortura.
- El 82 % del MASN se encontró en sitios que albergan imágenes y que no cuentan con un sistema de verificación del usuario o es muy limitada.

INHOPE, la asociación internacional de líneas directas de ayuda en Internet, trabaja con 46 miembros de líneas de ayuda en 41 países. Cuando alguna persona reporta MASN que esté alojado en un país diferente del que se ubica la línea de ayuda, INHOPE informa a la línea de ayuda del país anfitrión por medio de su software seguro, ICCAM, financiada por la Comisión Europea [107]. La International Survivor's Survey (Encuesta internacional de sobrevivientes) realizada por el Canadian Center for Child Protection (Centro canadiense para la protección del menor) también muestra que los niños más pequeños tienen un mayor riesgo, ya que el 56 % de los sobrevivientes indican que el abuso que sufrieron comenzó antes de los cuatro años de edad, y el 87 % tenía 11 años de edad o menos [38]. Una investigación de ECPAT descubrió que el 56 % de las víctimas de MASN eran prepúberes y 4.3 % eran bebés o niños de hasta dos años. Y cuanto más joven la víctima, más grave era el abuso [39].

De acuerdo con un informe de NetClean que se especializa en soluciones para detectar MASN en línea, el 85 % de los oficiales de policía que investigan el abuso de niños en línea afirman haber encontrado grupos organizados de delincuentes dirigiendo foros y comunidades en línea. Además, casi la mitad de los oficiales encuestados informaron que el número de grupos organizados iba en aumento [40].

El desafío de la producción de contenido autogenerado

En tan solo los primeros seis meses del 2019, la Internet Watch Foundation (IWF) recibió 22.482 denuncias de MASN autogenerado: un tercio de todas las denuncias que respondió la IWF. El 96 % de las víctimas que aparecían en este contenido eran niñas y el 85 % tenía entre 11 y 13 años de edad. Estas imágenes y videos muestran a niños, principalmente en un entorno de hogar, que han sido acosados sexualmente o que han sido obligados a realizar actos sexuales para ser vistos por medio de una cámara web. Los agresores graban videos que comparten en línea.

Peligros de contacto: grooming, cyberbullying, acecho y hostigamiento

El cyberbullying es otra violación a los derechos de los niños. UNICEF define el cyberbullying como el uso de mensajes electrónicos para hostigar, amenazar o acosar a otra persona. Los adultos a menudo no están al tanto de que esto está sucediendo, por lo que no pueden ayudar. Debido a la conectividad, los ambientes que alguna vez pudieron haber sido santuarios para el menor, en particular su hogar, se han convertido en un espacio de tormento en secreto. De manera interesante, un estudio realizado en el 2018 descubrió que los adolescentes a menudo consideran el cyberbullying como algo normal, y no quieren que sus padres se involucren, aumentando su aislamiento [41].

Al mismo tiempo, en una investigación llevada a cabo en 28 países, incluyendo los EE. UU., China, India, Rusia y Brasil se encontró que, en promedio, el 17 % de los padres afirmaron que sus hijos habían sido víctimas del cyberbullying. En algunos países, ese número sube hasta el 37 % [3].

Otro aspecto del bullying es el acoso sexual en línea. En un estudio sobre niños hecho en el 2017 en Dinamarca, Hungría y el Reino Unido se encontró que las fotos de contenido explícito del 6 % de los niños se había compartido sin su consentimiento. 25 % habían sido sujetos de rumores en línea respecto a sus vidas sexuales.

Además, 31 % habían visto a personas de su misma edad crear perfiles falsos para poder compartir con terceros fotos de naturaleza sexual. Aún más preocupante es el hecho de que el 9 % había recibido amenazas sexuales de personas de su misma edad [42].

Por último, otra forma bien conocida de daño por contacto es el grooming. El International Centre for Missing and Exploited Children (Centro internacional de niños extraviados y explotados, o ICMEC) define el grooming como el proceso por medio del cual un adulto entabla una relación con un menor para facilitar el contacto sexual en línea o fuera de ella [43]. Ya que por lo general es la antesala de un delito más grave, es difícil encontrar estadísticas aisladas respecto a magnitud del grooming en línea. Pero el impacto en las víctimas menores de edad es profundo.

Las víctimas afirman sentirse avergonzadas, haber perdido la confianza, autolesionarse, y sufrir ataques de pánico. En un reciente informe hecho por la compañía sueca de telecomunicaciones Telia, el 17 % de los niños encuestados afirmaron que sus fotos habían circulado en los medios sociales sin su consentimiento y el 7 % afirmó que habían sido extorsionados con las mismas. Uno de cada cuatro niños afirmó haber recibido contactos y mensajes perturbadores en línea, y más a menudo las niñas que los niños [44].

La radicalización como grooming

En el 2014, tres niñas estadounidenses de una escuela secundaria en Denver fueron interceptadas en Alemania, cuando iban de camino para unirse al Estado islámico yihadista (ISIS) [45]. Las tres habían sido radicalizadas y reclutadas en línea. En la mayoría de los países del Medio Oriente se han visto casos similares. Este no es solo un problema limitado a ISIS. Existen innumerables grupos extremistas a nivel mundial, que incluyen el Talibán, Al Shabab, grupos defensores de la supremacía blanca y otros, que buscan radicalizar y reclutar a niños. Los niños y jóvenes en estas situaciones son extremadamente vulnerables y, una vez que se encuentran en manos de quienes los radicalizan, les será casi imposible escapar. Es por eso que es tan importante desarrollar sistemas para identificar a los niños en riesgo antes de que pasen de la acción en línea a la acción fuera de ella.

Riesgos de contenido: pornografía, MASN, violencia, extremismo, juegos y apuestas en línea

En la era previa al Internet era relativamente fácil prevenir que los niños tuvieran acceso a contenido dañino o inapropiado para su edad. Para obtener un permiso para operar, los negocios para adultos tenían que hacer cumplir el límite de edad. Desafortunadamente, este no es el caso con los negocios en línea. Para los niños es demasiado fácil encontrar y ver contenido para adultos que tienen que ver con temas como apuestas, pornografía, MASN y violencia.

Muchos de los niños están ahora expuestos a pornografía para adultos en línea. En un estudio del 2018 de The Journal of Adolescent Health se encontró que uno de cada cinco niños de entre 9 y 17 años de edad ven material de contenido sexual autogenerado en línea [5].

En otro estudio se encontró que casi el 40 % de los adolescentes quieren imitar las prácticas sexuales que han visto en la pornografía en línea [46]. Un estudio en el Reino Unido del 2017 demostró que cuatro de cada cinco niños piensan que las compañías responsables de los medios sociales y del Internet deberían hacer más para protegerlos contra el material sexual [47].

Muchos niños desafortunadamente también están expuestos a incitación al odio y extremismo en línea. Un informe en los EE. UU., encontró que el 37 % de los estadounidenses sufrieron de odio y acoso sexual graves en línea en el 2018. También, el 38 % había dejado de usar dicho servicio o había cambiado la manera de usarlo [48].

Los niños también pueden estar expuestos a peligros por medio de los juegos en línea. A pesar de contar con restricciones de edad, muchos de los juegos no cuentan con una verificación de edad que sea efectiva. Por esta razón, a menudo los niños pueden entrar a foros y funciones de chat que no están regulados. Además, pueden estar expuestos a contenido sexual y de juegos violentos inapropiados para ellos, sufrir de cyberbullying y grooming en los foros y salas de chat [49].

Un reciente análisis de la literatura académica respecto a las apuestas encontró que hasta un 12 % de los adolescentes a nivel internacional pudieran tener problemas con las apuestas [52]. Estudios en una variedad de mercados entre los que se incluyen el Reino Unido, Canadá, los EE. UU. y los países nórdicos han encontrado que entre un 8 % y un 34 % de los niños menores de 18 años han apostado en línea en algún momento de sus vidas [53].

Los peligros potenciales relacionados con el problema de las apuestas es significativo, como también lo es la posibilidad de incurrir en una deuda significativa. En un reciente estudio se encontró que los jóvenes con problemas con apuestas tenían 15 veces más probabilidades de suicidarse que el promedio [54].

Por último, los niños que no son supervisados cuando están en línea corren por lo general más peligro de ver contenido violento, el cual puede ser inapropiado para su edad, perturbador o incluso mostrar actividad delictiva. Un estudio llevado a cabo en el 2018 demostró que la exposición a medios violentos tiene una estrecha relación con una mayor susceptibilidad a mostrar un comportamiento antisocial [50]. En otro estudio de la red EU Kids Online se encontró que 18 % de los niños afirmaban que les preocupaba estar expuestos a contenido violento en línea [51].

Riesgos de comportamiento: mal uso de los datos, gastos no autorizados y comportamiento inapropiado

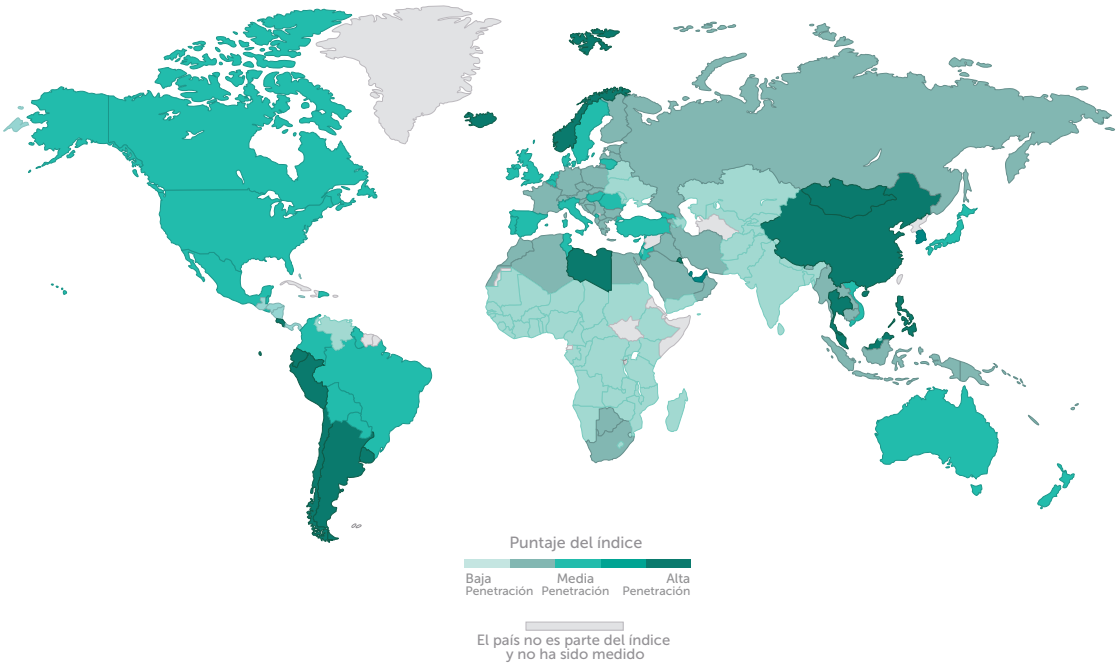
Muchos de los servicios están diseñados con un límite de edad, y por lo general están prohibidos para menores de 13 años, en acato a la Ley de Protección de la Privacidad de los Niños en Internet (COPPA) de los EE. UU. Sin embargo, en demasiadas ocasiones es comúnmente fácil para los niños evitar estas restricciones. Estudios realizados por el Pew Center en los EE. UU. y la National Society for the Prevention of Cruelty to Children (Sociedad Nacional para la Prevención de la Crueldad Contra los Niños) en el Reino Unido han descubierto que para cuando los niños cumplen 12 años, cerca de la mitad ya tienen cuentas en los medios sociales [55] [56].

Los daños potenciales relacionados con el uso de medios sociales por parte de menores de edad incluyen:

- Bajos índices de actividad física que contribuyen a una salud precaria [57].
- Alteración del sueño, lo que tiene un impacto en el desempeño escolar [58].
- Ansiedad y depresión, que los estudios demuestran que se intensifican con el uso de los medios sociales [59].

Otro riesgo, en el que muy fácilmente caen los niños, es el gasto involuntario y no autorizado. Muchos programas ofrecen

Índice de conectividad móvil de GSMA: Penetración móvil en los medios sociales en 2018



Fuente: GSMA Mobile Connectivity Index 2019, GSMA Intelligence Unit

Los jóvenes en muchos de los países del mundo ya tienen acceso a los medios sociales a través de dispositivos móviles. Con la expansión de la banda ancha, la penetración de los medios sociales aumentará rápidamente, dejando expuestos a más niños a peligros y daños en línea.

compras dentro de las apps, fuertemente promovidas por los anunciantes dentro del juego o aplicación.

En un reciente estudio publicado en la Society for Developmental and Behavioral Pediatrics (Sociedad para el desarrollo y comportamiento pediátrico) se encontró que casi todas las apps dirigidas a niños contienen publicidad, mucha de la cual los investigadores describen como "manipuladora". Entre otras prácticas, la investigación señaló el uso frecuente de anuncios emergentes que interrumpen el juego y personajes del juego que invitan a los niños a realizar compras voluntaria o involuntariamente [60].

Riesgos de los contratos: ¿qué tan bien informado es el consentimiento de un niño en línea?

Todos los riesgos descritos en las páginas anteriores en esta sección caen dentro de un marco de interacciones digitales que no son adecuadas para niños. Un estudio del 2019 llevado a cabo por dos profesores de leyes apuntó a que el 99 % de los términos y las condiciones en línea estaban escritos en un lenguaje demasiado complicado de entender para el graduado universitario promedio [6].

No es posible que los niños entiendan lo que están firmando al momento de instalar la app o ingresar al sitio web. Los servicios y responsabilidades diseñadas para los adultos deben tener un límite de edad, para que así los niños no puedan inscribirse en ellos sin el permiso del tutor. Al no comprender lo que están haciendo, los niños pueden inscribirse en una variedad de sistemas de vigilancia de datos. En la mayoría de los contextos, las compañías no tienen permitido tratar a los niños de esa manera. Pero si sus sistemas no toman primero en cuenta el bienestar de los niños, entonces terminaran haciéndolo de cualquier manera.

Cuando los niños están en línea también corren el riesgo de gastar dinero sin el permiso de sus padres o cuidadores, y de que se recolecte su información. La investigación muestra que el 90 % de las apps de terceros en la tienda Android Play recolectan datos como la edad, género, ubicación y patrones de uso [61].

La huella digital de los niños, y la capacidad de las diversas plataformas de combinar e integrar esos datos para producir información detallada, tiene el potencial de determinar y afectar el futuro de los niños. Corremos el riesgo de permitir que la niñez de una generación entera sea tratada como si fueran datos, que sean cuantificados, vendidos y revendidos. Estos datos— que van desde detalles personales delicados, como la fecha de nacimiento, hasta detalles de la actividad en línea del menor — recabados sin el consentimiento bien fundado de los sujetos menores de edad, pudiera repercutir en las oportunidades futuras de los niños, incluyendo su acceso a educación, servicios y empleo.

Resumen de la situación actual de los niños en línea

A nivel mundial, los niños muy frecuentemente están expuestos a daños, abusos y violencia debido a la falta de vigilancia en Internet. Incluso los niños que no caen víctimas del comportamiento predatorio de los adultos, a menudo se ven desfavorecidos por las acciones y omisiones de los servicios y productos que no toman en cuenta sus necesidades ni dan los pasos necesarios para protegerlos [23].

El comisionado de asuntos de la infancia del Reino Unido crea términos y condiciones favorables para el menor

En el 2017, el comisionado de asuntos de la infancia en el Reino Unido creó versiones de los términos y condiciones sencillas para las plataformas de Facebook, Instagram, Snapchat, YouTube y WhatsApp. Escritos por abogados, estos términos y condiciones fueron diseñados para ser fáciles de entender, para que padres y cuidadores puedan entender a lo que los niños se estaban inscribiendo al unirse a uno de estos servicios. Puede encontrar estos términos y condiciones simplificados en:

https://www.childrenscommissioner.gov.uk/publication/simplified-social-media-terms-and-conditions-for-facebook-instagram-snapchat-youtube-and-whatsapp/

Oportunidades

6



Oportunidades

Estamos experimentando una transformación digital a nivel global. Esto no solamente promete brindar una gama de beneficios para los niños, como por ejemplo, mayor acceso a oportunidades educativas, culturales y económicas, sino que también existen señales alentadoras de que los cambios tecnológicos y sociales que traen consigo revolucionarán la lucha en contra de la explotación y el abuso sexual de niños en línea.

La inteligencia artificial y la lucha en contra de la explotación de niños en línea

El desarrollo de la inteligencia artificial (IA) tiene el potencial de ayudar a las compañías y a las instituciones policiales a procesar más MASN u otro tipo de contenido de abuso de niños, e identificar con exactitud material ilegal, a los abusadores y a las víctimas con más frecuencia y rapidez.

En el 2018, Google anunció la incorporación de una nueva red profunda neutra para mejorar la detección de MASN. En pruebas llevadas a cabo, la compañía reportó que el uso de IA había ayudado a mejorar los índices de detección y denuncia en un 700 % [62].

Microsoft en Alemania está trabajando con la policía del país para desarrollar IA que pueda identificar MASN más rápidamente [63], al igual que las autoridades en Holanda [64], Australia [65] y el Reino Unido [66]. La herramienta Griffeye Brain es un clasificador con IA que escanea material nunca antes visto y sugiere archivos que considera que muestran abuso sexual de niños. Esto ayuda a acelerar las investigaciones y a resaltar material de abuso sexual de niños previamente desconocido [67].

La policía del Reino Unido también está utilizando IA para encontrar e identificar contenido extremista en línea del tipo que es usado para radicalizar a niños [68]. Facebook está construyendo un sistema por medio de IA diseñado no solo para identificar material de abuso sexual de niños, sino también conversaciones que incluyen indicios de que se está llevando a cabo grooming [69].

A principios del 2019, Microsoft organizó un hackaton para trabajar con WePROTECT Global Alliance (Alianza global para la protección o WPGA), en la que se reunieron ingenieros y expertos legales y de operaciones de Microsoft, Google, Facebook, Snapchat y Twitter para desarrollar una herramienta de IA que afronte el grooming en línea [70]. En los EE. UU., Marinus Analytics ha desarrollado un software con IA que busca anuncios en línea de servicios sexuales para identificar a víctimas de tráfico y reunir la evidencia que ayude a la policía a llevar a los traficantes ante la justicia [71]. Thorn ha desarrollado tecnología de IA dentro de su herramienta de investigación de tráfico sexual, Spotlight, que da a las agencias policiales dentro de los 50 estados de los Estados Unidos y Canadá, la capacidad de acelerar la identificación de las víctimas y reducir el tiempo de investigación en más de un 60 % [72].

En la conferencia Code 8.7 del 2019 que llevó por título Uso de la ciencia computacional y de la IA para terminar con la esclavitud moderna, los participantes abrieron la posibilidad de tener una base de datos internacional común para víctimas (igual que la base de datos de explotación sexual de niños de la INTERPOL) o de traficantes, que sea accesible para las autoridades responsables de aplicar la ley alrededor del mundo [73]. Aunque menos llamativa que la IA o las tecnologías emergentes, este representaría un enorme paso tecnológico en la lucha contra el tráfico de niños.

Hay incluso planes de usar la IA para combatir el cyberbullying y el hostigamiento en línea. Recientemente, Instagram dio a conocer una herramienta con IA para detectar y anticipar los comienzos de un hostigamiento en línea [74]. En Europa, un proyecto de la UE, llamado Creep, emplea IA para detectar cyberbullying y para saber la diferencia entre bullying y una simple discusión en línea [75].

Otros tipos de tecnologías emergentes

Otro tipo de tecnologías emergentes también tienen el potencial de ayudar en la lucha contra el daño a niños en línea. En el capítulo 4 vimos tecnologías tales como las de bloqueo en base a listas, filtración heurística y el uso de rastreadores de la web para encontrar, detectar, denunciar y bloquear MASN y otro tipo de contenido de abuso de niños. Estas tecnologías no son nuevas, sin embargo no se han usado tan ampliamente.

Otras tecnologías realmente nuevas que se han aplicado en la lucha contra el abuso de niños en línea incluyen:

- Tecnología de reconocimiento facial mejorada que ayuda a identificar más rápido a niños que son víctimas de explotación sexual [76].
- Mayor poder de procesamiento y reconocimiento de imagen mejorado que permite escanear el disco duro de 1TB del sospechoso para buscar contenido ilegal conocido en tan solo 30 minutos [77].
- Análisis predictivo que usan las autoridades para identificar a niños en riesgo de abuso y que les permite intervenir antes de que suceda el abuso [78].

Al aproximarse la madurez de estas y otras nuevas tecnologías, las organizaciones tendrán muchas oportunidades para usarlas en la lucha en contra del abuso al menor en línea. Incluso, el solo hecho de que un país esté conectado al Internet puede facilitar y acelerar la cooperación entre sus agencias de aplicación de la ley y las compañías de aquellas en otros países.

Aumento de la cooperación internacional

Desde el 2008, la ITU dio a conocer la Child Online Protection Initiative (Iniciativa de protección al menor en línea, o COP) como un esfuerzo de las diferentes partes interesadas dentro del marco de la Global Cybersecurity Agenda (Agenda de ciberseguridad global, o GCA). Esta iniciativa reúne a socios de todos los sectores de la comunidad global para crear una experiencia en línea más segura y empoderadora para los niños alrededor del mundo. Con el paso de los años, la iniciativa ha traído continuamente el tema a la comunidad internacional.

Otro desarrollo alentador ha sido el aumento de la cooperación entre países y en los diferentes sectores para encontrar soluciones comunes en la lucha contra la explotación de los niños en línea. Las iniciativas globales recientes incluyen a WePROTECT Global Alliance y Child Dignity Alliance.

Cada vez más, las agencias de aplicación de la ley también trabajan en otras jurisdicciones. En la Operación Tantalio del 2017, la INTERPOL, la Europol y las agencias policiales de 15 países cooperaron para arrestar a 39 individuos y desmantelar una banda en línea que distribuía MASN [79]. En el 2019, Tailandia, los EE. UU., Australia, Nueva Zelanda y Bulgaria trabajaron en conjunto para arrestar y perseguir a delincuentes en Tailandia, en Australia y en los Estados Unidos, y rescatar a 50 niños [80].

También hay un aumento en la colaboración entre líneas de ayuda, proveedores de servicio de Internet (ISP) y agencias policiales. Por medio de su plataforma segura ICCAM, financiada por la Comisión Europea, INHOPE toma información de las líneas de ayuda de todo el mundo y actúa partiendo de la misma para eliminar el MASN de cualquier país participante. El testimonio de lo valiosa que es esta estrategia es el hecho de que el 60 % de los videos descubiertos por la ICCAM, financiada por la Comisión Europea en el 2017 no eran del conocimiento de las agencias policiales internacionales [81].

7

Amenazas y el entorno amenazador



Amenazas y el entorno amenazador

Los abusos, la explotación y los sistemas de pésimo diseño que exponen a los niños a riesgos innecesarios son demasiado comunes en el mundo en línea. Y estos daños no ocurren de manera aislada. Se dan por una variedad de factores técnicos, sociales y legales. Para proteger a los niños en línea, es importante comprender los riesgos que enfrentan y los factores detrás de esos riesgos.

Las compañías y otros organismos podrían fácilmente minimizar algunos de los riesgos en la etapa del diseño. Por ejemplo, podrían detener las ubicaciones en tiempo real de los niños que están a disposición de otros usuarios; integrar la seguridad por defecto en dispositivos inteligentes para el hogar (para prevenir el streaming accidental); incorporar el diseño de verificación de edad y centrado en el menor dentro de sus productos y servicios; y dejar de usar ganchos competitivos, los cuales promueven el comportamiento riesgoso.

Otro factor clave que contribuye al nivel de riesgo que enfrentan los niños en línea es la falta de mecanismos efectivos y sólidos (incluyendo la legislación adecuada) con los cuales el estado y la sociedad civil puedan responder ante aquellos que buscan activamente explotar o abusar de los niños en línea [83].

Los países con ingresos medios y bajos tienen una capacidad tecnológica menos desarrollada y menos recursos para prevenir o investigar los delitos que se llevan a cabo en línea. Incluso los países con ingresos altos carecen de estrategias contra la ciberdelincuencia.

Además, en algunos de los casos las leyes no han sido actualizadas para incluir delitos específicos e instrumentos vigentes para investigar y procesar la ciberdelincuencia [82]. La tecnología cambia más rápido de lo que los legisladores y agencias policiales puedan seguirle el paso, dando lugar a vacíos por los que caen la innovación negligente o los mismos agresores.

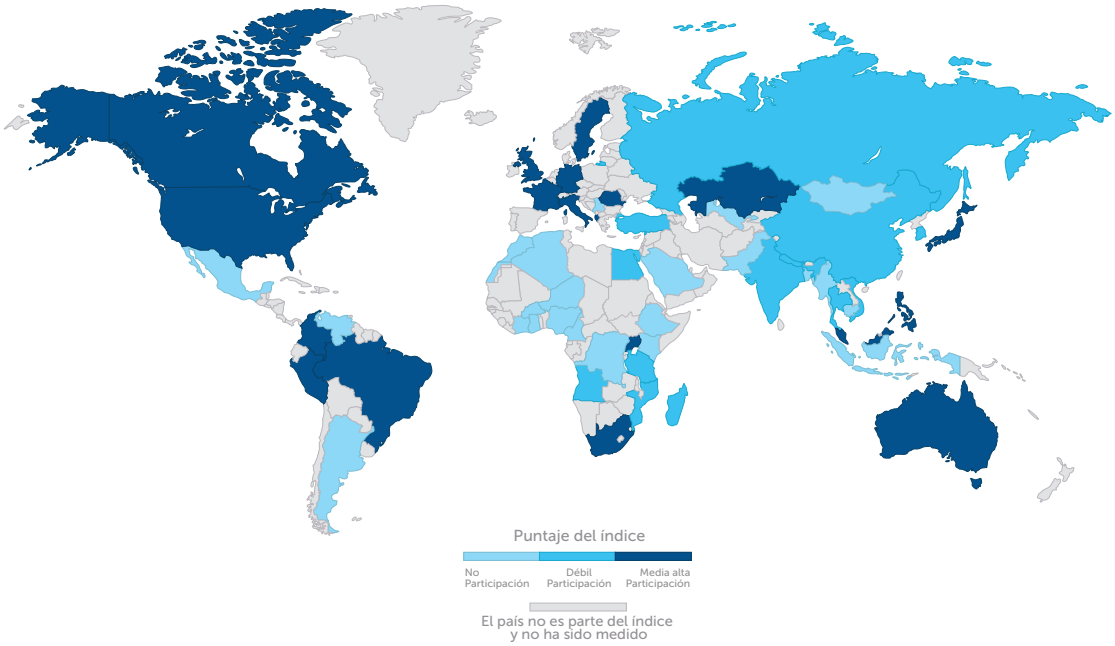
El índice Out of the Shadows del EIU

El índice Out of The Shadows [83], desarrollado por The Economist Intelligence Unit (EIU), llevó a cabo un estudio de 60 países (que abarcan el 85 % de los niños a nivel mundial) para evaluar su capacidad de respuesta ante la violencia sexual en contra de niños, incluyendo en línea.

Los datos recabados en este estudio fueron usados para crear el índice, con un alcance de 100 que indica el nivel de protección más alto y cero que indica el nivel más bajo. Entre otros hallazgos, el EIU descubrió que:

- Ningún país está haciendo lo suficiente y solo cuatro países recibieron una calificación mayor del percentil 75.
- 11 países recibieron una calificación de menos de 50 por el entorno que ofrecen a sus niños.
- 16 países recibieron una calificación de menos de 50 por la calidad de su marco legal de protección al menor.
- 36 países recibieron una calificación de menos de 50 por la participación de la sociedad civil y de la industria.
- 37 países recibieron una calificación de menos de 50 por su capacidad legal para proteger a los niños.

Participación de la industria: respuesta a la violencia sexual en contra de los niños en línea



Fuente: Out of the shadows: shining light on the response to child sexual abuse and exploitation, The Economist Intelligence Unit, 2019.

De los 60 países estudiados por el EIU, en solo 10 había mecanismos de denuncia de la industria tecnológica que se usaban activamente para la denuncia de violencia contra niños en línea.

Brechas en las políticas y leyes nacionales

A medida que la sociedad global pasa por una rápida transformación digital, existe el riesgo de que las nuevas tecnologías y métodos se apliquen sin la debida consideración sobre el impacto que tendrán en los miembros más vulnerables de la sociedad, y en particular en el caso de los niños.

Muchos países no tienen secciones respecto a las necesidades y los derechos de los niños en sus planes nacionales de banda ancha. Esto aumenta las probabilidades de que las entidades públicas y privadas creen políticas, plataformas y servicios que no sean, desde su diseño, aptos y seguros para niños.

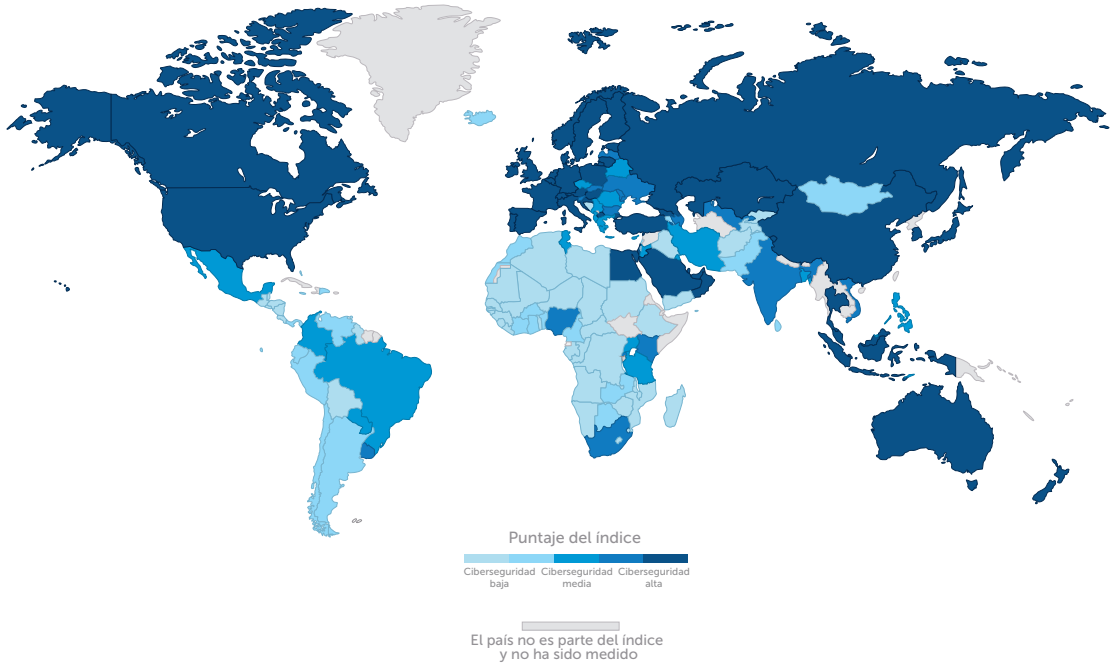
Para abordar este problema, UNICEF, UN Global Compact, y Save the Children han establecido los Derechos del Niño y Principios Empresariales [84]. Estos establecen un conjunto de principios claros y accionables que las organizaciones pueden seguir para edificar el respeto por los niños y por sus derechos en cada faceta de sus operaciones. Puede encontrar estos principios aquí: **https://www.unicef.org/csr/theprinciples.html**

Para un caso práctico respecto a cómo la legislación y la política nacionales pueden ser reestructuradas con éxito para proteger y mejorar los derechos de los niños en línea, vea el caso práctico en la página 71, el cual describe el trabajo realizado por el gobierno de Ruanda y sus socios.

Las leyes sobre ciberseguridad necesitan modernizarse

Hoy día, solo un 72 % de los países cuentan con una legislación sobre ciberdelincuencia que sea funcional [85]. Incluso dentro de las naciones mismas, existe con frecuencia una falta de definiciones operativas y legales congruentes respecto a lo que constituye una ofensa a un menor en línea y la falta de una acción coordinada entre las distintas agencias. Esa ventaja permite a los criminales operar en jurisdicciones con marcos legales permisibles y distribuir MASN con impunidad, a nivel mundial.

Índice de conectividad móvil de GSMA: Índice de ciberseguridad



Fuente: GSMA Mobile Connectivity Index 2019, GSMA Intelligence Unit

En el Índice de conectividad móvil de GSMA, muchos de los países con las calificaciones de ciberseguridad más bajas son también los países con la mayor concentración de habitantes menores de 19 años.

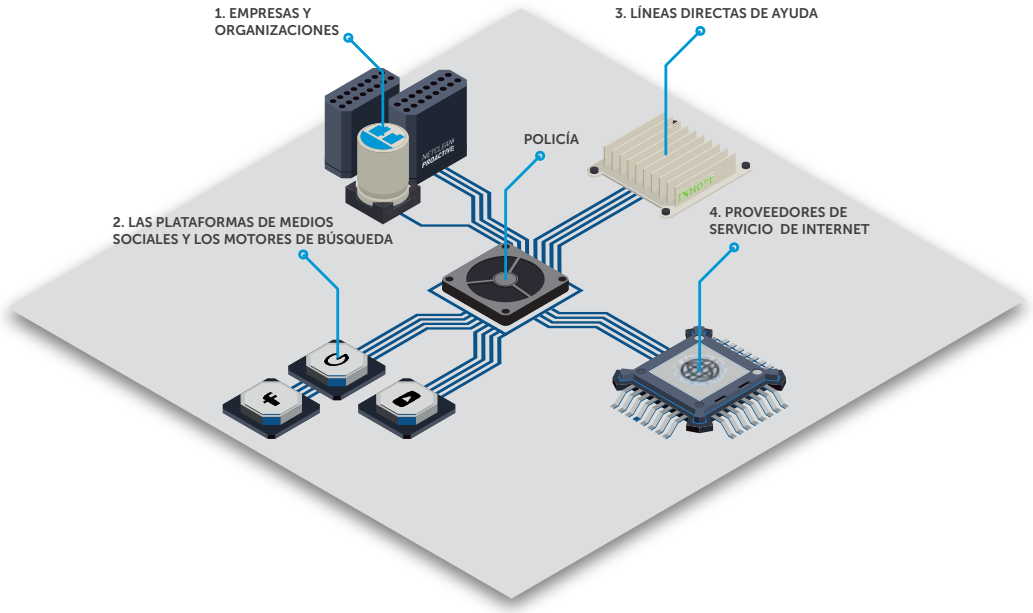
Para lidiar con esto, los países deben adoptar leyes de ciberseguiridad severas que sean aplicadas de manera consistente por las fuerzas policiales con el equipamiento, los recursos y la motivación adecuados. Debido a la naturaleza transfronteriza del abuso y la explotación de niños en línea, también es importante reconocer que la protección para el menor es un tema global, que requiere de una cooperación internacional y clasificaciones y marcos legales que estén en armonía y de acuerdo con las normas COP de la UIT y con las normas COP de UNICEF diseñadas para la industria [86].

Solo por medio de estándares y clasificaciones acordados a nivel internacional es que los estados podrán compartir los datos y los recursos comunes para combatir el abuso de niños que ocurre en línea.

Falta de sistemas de rendición de cuentas y estándares obligatorios

Convertir el Internet en un lugar más seguro para explorar es más fácil de hacer cuando los legisladores y quienes hacen cumplir las leyes pueden trabajar junto con los proveedores de servicio de Internet (ISP), operadores de telefonía móvil, buscadores, instalaciones de servicio de Internet públicas y agencias similares. Estas compañías tienen la capacidad de detectar el material de abuso de niños desde la fuente y hacer llegar los detalles pertinentes a las autoridades. Pero para poder lograr lo anterior, estos necesitan la legislación y los procedimientos que definan bien el rol y las responsabilidades en este proceso.

Flujo de la cooperación



Fuente: NetClean

Para tener éxito en detectar a los perpetradores, eliminar MAM y rescatar a las víctimas, todas las partes interesadas deber trabajar en conjunto y conocer sus respectivos roles.

Sin embargo, menos de uno de cada seis países han establecido en su legislación el reporte obligatorio de los ISP, denuncia, bloqueo y eliminación de contenido, y mantenimiento de registros. Más del 40 % de los países no cuentan con ninguna legislación al respecto. Otro obstáculo de importancia es los vacíos que existen en la definiciones estándares y el no respetar los lineamientos de Luxemburgo, lo cual dificulta la coordinación en contra del abuso y la explotación de niños en línea a nivel internacional [87].

Necesidad de conocer y monitorear a delincuentes

Al igual que existe la necesidad de encontrar y cerrar los sitios y servicios que los agresores usan para cometer sus crímenes, también existe la necesidad de identificar y entender a los agresores mismos. Esto es de vital importancia si queremos prevenir que los agresores conocidos vuelvan a victimizar a los niños, pero también si queremos aprender a detectar a potenciales agresores e intervenir antes de que vuelvan a cometer un delito.

Muy a menudo, sin embargo, los agresores pasan inadvertidos y quedan impunes. Además, incluso cuando los delincuentes son detectados y procesados, se ha descubierto que hasta el 8 % de aquellos que reciben condenas por delitos por contacto con niños en línea vuelven a reincidir [88].

Para aumentar los índices de detección de los agresores y reducir el riesgo de reincidencia de agresores declarados culpables, es necesario entender mucho mejor qué es lo que caracteriza y motiva a los agresores, para cometer crímenes de MASN pero también otro tipo de delitos, incluyendo cyberbullying, hostigamiento y radicalización.

En el 2018, Thorn publicó un informe en colaboración con NCMEC, que examinaba las tendencias en MASN activamente comercializado. Entre otros hallazgos,

este informe encontró que los productores hombres de este material superaban en número a las productoras mujeres. Los casos que involucraban a productoras mujeres eran más probable que describieran abuso intrafamiliar extremo de niños más pequeños. Además, esta investigación halló que el MASN que es distribuido con el tiempo se está haciendo más violento, con relativamente más casos que muestran penetración que hace 10 años [89]. De acuerdo a investigación de NetClean, el delincuente de MASN promedio es hombre, con más del 50 % de oficiales de policía que reportan nunca haber encontrado una delincuente mujer [90].

Desarrollar conocimiento como este es clave para ayudar a las agencias de policía a asignar sus escasos recursos de maneras que se determine puedan tener el mayor impacto posible. Además, debido al crecimiento de los sitios del darknet, los cuales son más difíciles y caros para investigar, prevenir delitos por primera vez y de reincidencia puede tener un impacto enorme en la escala de la tarea a la que se enfrentan las agencias de policías.

En los últimos años, han surgido líneas de ayuda para "Detener al instante" que ofrecen consejería y apoyo gratuitos y anónimos por teléfono o por chat a personas que tengan sentimientos o pensamientos de interés sexual con niños, quienes son potenciales delincuentes [91].

Las amenazas provenientes del mal uso de la tecnología

En los inicios del Internet, los foros de discusión de noticias fueron unos de los campos de distribución de material de abuso sexual de niños (MASN) más significativos. Con el surgimiento de la World Wide Web (red de informática mundial), gran parte del MASN y otro contenido de abuso se trasladó de los grupos de noticias para ser albergados en sitios web.

Para los años de la década del 2000, las autoridades y proveedores estaban cada vez más conscientes del problema de los sitios web que albergaban MASN, y se hicieron más activos para cerrar los sitios y procesar tanto a los publicadores como a los usuarios de estos sitios.

Esto llevó a muchos delincuentes a migrar su actividad a dispositivos para intercambiar archivos uno a uno (P2P). El solo volumen de tráfico proveniente de las redes P2P las hacían difíciles de controlar, un problema solo exacerbado por el creciente uso del cifrado. Los medios sociales también son populares entre los perpetradores como un canal en el cual dar con niños e intercambiar información unos con otros. Para poder ser efectivos para detectar el abuso y la explotación, rescatando niños y procesando a los agresores, debemos siempre abordar la gama completa de las amenazas y el ambiente completo de las amenazas. La evaluación WePROTECT Global Alliance Global Threat Assessment del 2018 identifica los siguientes factores, entre otros, como complicaciones significativas en la lucha contra el abuso y la explotación de niños en línea:

- La disponibilidad del Internet de alta velocidad permite que existan agresores y que se comparta MASN.
- La creciente disponibilidad de los mensajes cifrados ayuda a los agresores a comunicarse entre ellos de forma secreta.
- El uso de redes privadas virtuales (VPN) facilita a los criminales esconder sus actividades.
- Los costos de producción de medios enriquecidos, como videos y fotos de alta resolución, están disminuyendo todo el tiempo.
- La tecnología de manipulación profunda de fotos (deepfake) hace más fácil crear y esconder MASN.
- La transmisión en vivo permite que se comparta MASN una vez, lo cual dificulta que las autoridades puedan detectarlo.
- El almacenamiento en la nube que es de bajo costo facilita a los agresores almacenar y compartir MASN en línea.

- El almacenamiento en USB es ahora barato con lo que mover MASN es fácil. A menudo estos drives están protegidos por leyes de privacidad de datos que son más estrictas que las leyes para proteger a los niños.

La codificación y otras tecnologías de anonimización son cada vez más comunes y presentan un desafío para afrontar el problema del abuso y la explotación de niños en línea, tanto para las agencias de aplicación de la ley como para otras entidades. El cifrado hace imposible detectar el material de abuso sexual de niños hasta que el archivo es descifrado, al llegar a quien recibe el mensaje cifrado. Para tratar este problema, sería imprescindible que la legislación hiciera obligatorio que los ISP tengan acceso a soluciones de imágenes forenses que les permitan filtrar fotos y videos que detecten MASN. Las soluciones que pueden implementarse incluyen PhotoDNA, el cual ya utilizan muchas compañías de tecnología. Las agencias policiales también enfrentan el desafío de los espacios de almacenamiento cifrados, los cuales requieren de mucho esfuerzo y conocimiento técnico para penetrar. Los legisladores deberían lidiar con este desafío dando prioridad a los derechos de los niños y asegurándose al mismo tiempo de que no se viole el derecho a la privacidad.

Los vacíos en la tecnología permiten el abuso y la explotación

Existen ya softwares y soluciones para ayudar a las compañías privadas, encargadas de las regulaciones y las agencias de aplicación de la ley a detectar, denunciar y, en su defecto, actuar en contra de sitios y servicios que alberguen MASN. Muchas de estas soluciones son altamente automatizadas y emplean algoritmos de resumen criptográfico para minimizar la exposición del personal a contenido dañino. También muchos están disponibles a un bajo costo o sin costo.

Para ganar la lucha en contra del abuso y la explotación en línea, todas las agencias y organizaciones de relevancia en este asunto, incluyendo las compañías privadas que ofrecen servicios en línea, deben utilizar la amplia variedad de tecnologías adecuadas que están disponibles para cubrir los vacíos técnicos que facilitan a los agresores operar en línea.

Un ejemplo del tipo de paquetes de tecnología disponibles incluyen:

- **NetClean ProActive:** es un software en base a igualación de firma y otros algoritmos de detección, el cual detecta automáticamente imágenes y videos de abuso sexual de niños en entornos empresariales.

- **Thorn's Safer:** es una herramienta que puede implementarse directamente en la plataforma privada de la compañía para identificar, eliminar y denunciar MASN.

- **Griffeye Brain:** IA que escanea contenido previamente sin clasificar, lo compara con las características de contenido identificado como MASN, y señala artículos sospechosos para que sean revisados por un agente.

- **PhotoDNA:** es una herramienta que crea *hashes* de imágenes que compara con una base de datos de *hashes* de imágenes previamente identificados y que han sido confirmados del tipo de MASN. Si encuentra una imagen comparable, la bloquea.

Para obtener una lista más completa del software disponible, vea la sección de recursos adicionales al final de este informe.

Cabe destacarse que los planes de un buen número de compañías de Internet para implementar el cifrado de extremo a extremo en todos sus servicios, incluyendo en los buscadores, plataformas de medios sociales y servicios de mensajería populares, amenaza con anular las herramientas diseñadas para interferir con la distribución de MAN y MASN. Estas herramientas no son completamente compatibles con el cifrado de extremo a extremo. Es por eso que las partes involucradas, del sector público y privado, deben dar pasos concretos ahora para asegurarse de que el cifrado se

implemente de manera que permita que estas herramientas sigan funcionando.

El crecimiento de la red oscura *(darknet)*

El término "darknet" (red oscura) se refiere a los sitios y servicios que, más que estar fuera de simple vista, se esconden a propósito por medio de herramientas y protocolos de cifrado. El mejor de los cálculos estima que existen cerca de 8500 sitios en el darknet, y se tiene acceso a ellos por medio del buscador "Tor" que es cifrado y anónimo [92]. De acuerdo a una investigación del 2019, aproximadamente 100 de estos sitios son mercados donde se comercia con productos ilegales, los cuales incluyen potencialmente material de abuso sexual de niños [92].

Los sitios del darknet pueden ser simples mercados o pueden funcionar como comunidades en línea en las cuales los delincuentes crean un ambiente de normalidad compartida, lo que permite y fomenta las actividades de cada uno. Esto fomenta que los agresores cometan crímenes cada vez más graves. Aunado a la disponibilidad de teléfonos baratos con cámara de alta resolución, hoy día la darknet es una de las plataformas clave para el abuso y la explotación en línea.

De acuerdo a un estudio citado por ECPAT International, solo el 2 % de estos sitios en la darknet albergan material de abuso sexual de niños, pero esos sitios son responsables del 80 % del tráfico en la darknet [93].

El rol del entorno sociocultural de los niños

Los niños son por naturaleza vulnerables ante las personas responsables de su seguridad. Y aunque el abuso de niños nunca es responsabilidad del menor, existen muchos factores presentes en el ambiente y la educación de un niño que pueden aumentar su vulnerabilidad ante tales delitos.

Un menor educado en una cultura donde se fomenta guardar secretos, que está expuesto a material sexual, o que es testigo de situaciones en las que se intercambia sexo por dinero, drogas o protección, será menos capaz de ver la violación sexual como algo inaceptable. Un menor que ha sido expuesto a la violencia o al control opresivo, o quien tiene miedo a las figuras de autoridad, le será difícil buscar protección [94].

La negligencia, el aislamiento emocional o las discapacidades pueden llevar a una baja autoestima y a una imagen pobre de uno mismo. Esto a su vez puede ocasionar que el menor se vea a sí mismo como alguien que no merece ser protegido [95]. Un factor importante en esto es a menudo una conexión débil o ausente con un adulto confiable y seguro. Los niños que no cuentan con una red de protección, por ejemplo, los que escapan de casa, están particularmente en riesgo, así como los niños que viven en asilos, o niños con discapacidades [96].

Las normas socioculturales, incluyendo la vergüenza y el miedo, también son factores determinantes que permiten que no se denuncie el abuso y la explotación. Las amenazas en contra del menor o contra quienes cuidan de ellos, pueden llevar a una atmósfera de secretismo. La vergüenza y el temor a ser juzgados también pueden impedir que el menor revele estos delitos [97].

Otros factores que también pueden exacerbar el riesgo del abuso incluyen:

- El aislamiento social debido al tiempo excesivo frente a una pantalla.
- La falta de verificación de edad, lo que permite a los niños tener acceso a contenido y foros para adultos que no son seguros para ellos.
- La sexualización de los niños en la cultura general.

El problema tiene un alcance más amplio que tan solo la influencia de algunos cuantos "malos elementos". Este incluye todos los factores que influyen en el comportamiento del menor en línea y la capacidad del mismo de tener acceso a material y foros que no son seguros. Aquí también caben las actitudes de los adultos en la vida del menor y la naturaleza de las estructuras en las que se desenvuelven

dichos adultos. ¿Obstruyen o facilitan el abuso estas estructuras?

El rol del medio social no es solo un factor en la vulnerabilidad del menor frente a la explotación y abuso sexual de niños o EASN: también determina cuán seguro está un menor frente a una gama completa de riesgos y daños en línea, que incluyen el grooming, la radicalización y la explotación económica.

Responsabilidades de los principales interesados

Un gran número de personas es responsable de criar y brindar apoyo a los niños durante su crecimiento para llegar a la vida adulta: padres, cuidadores, familias, educadores, profesionales de la salud, líderes de la comunidad, agencias policiales y el sector privado, por ejemplo. Pero muchas de estas personas cuentan con poco o ningún tipo de entrenamiento para proteger a los niños de los peligros y daños que existen en línea.

El estado debe asegurarse de que todas estas partes interesadas puedan cumplir con su rol de protectores y que sepan cómo llevar a cabo su papel para mantener a salvo a los niños frente a los perjuicios que existen en línea, así como ayudar a los jóvenes a aprovechar al máximo las oportunidades educativas, económicas y culturales que ofrece el Internet.

Las acciones clave para dar apoyo a las partes interesadas incluye:

- Dar prioridad al entrenamiento de las partes interesadas e invertir de igual manera el tiempo y el presupuesto.
- Concientizar a educadores, padres y cuidadores respecto a los riesgos que existen en línea y cómo mitigarlos.
- Capacitar a los proveedores de servicios de los niños para detectar cuando esté ocurriendo un abuso y cómo intervenir.
- Darle a las agencias policiales los poderes, la tecnología y la pericia que necesitan.

El papel del sector privado

8



El papel del sector privado

Gran parte de la infraestructura clave y de los servicios que utilizamos todos los días en línea operan y fueron construidos por compañías privadas. Para tener éxito, cualquier esfuerzo que se haga para proteger a los niños en línea debe estar respaldado y contar con un compromiso total del sector privado. Las compañías privadas también deben comprometerse a financiar adecuadamente tanto sus esfuerzos como los esfuerzos colectivos para combatir el abuso de niños en línea.

Es normal que las compañías quieran hacer lo correcto con los niños que usan sus servicios. Sin embargo, los resultados por lo general dejan mucho qué desear. En solo seis meses en el 2018, la policía del Reino Unido registró 1944 casos de grooming en Instagram [98]. A principios del 2019, se reveló que los delincuentes estaban usando comentarios en YouTube para contactar a niños [99]. De acuerdo a una investigación por parte de una organización benéfica anti bullying, el 37 % de los adolescentes que participaron respondieron haber sufrido de bullying en Facebook [100].

¿Cómo puede mejorar el sector privado su estrategia para la seguridad del menor en línea? Para averiguarlo, el grupo de trabajo encuestó a algunos de los líderes en la materia. Esto es lo que reveló la encuesta:

- Las compañías y las ONG que hacen un buen trabajo con la protección al menor en línea, basan su estrategia en una infraestructura establecida; por ejemplo la infraestructura del Model National Response (modelo de respuesta nacional) de WePROTECT, o "Children's Rights and Business Principles" (principios para negocios y derechos de los niños, o CRBP), desarrollada por Save the Children, UNICEF y UN Global Compact.

- Los líderes hacen uso de una amplia gama de tecnologías, desde detección, filtración y bloqueo por medio de tecnologías emergentes, como la de inteligencia artificial.

- Las políticas y estrategias de protección al menor son desarrolladas en coordinación y con el asesoramiento de una variedad de partes interesadas internas y externas, incluyendo el gobierno, la sociedad civil y los niños mismos.

- Las políticas y las estrategias deben atacar la cultura y el uso diario de los servicios digitales que normalizan los comportamientos sexuales o peligrosos, o que ponen rutinariamente a los niños en ambientes diseñados para adultos. Se debe mostrar un compromiso mayor para proteger la información y la reputación del menor, y ofrecer experiencias y espacios apropiados de acuerdo a la edad [23].

- Las estrategias tienen metas claras y medibles. Esto no solamente hace posible determinar el éxito sino que además facilita a las partes interesadas adoptar las campañas.

La divulgación y la educación también tienen un papel clave en el éxito de la prevención. Los ejemplos incluyen la plataforma #DQEveryChild de DQ y la campaña EndViolence #SafetoLearn.

- Cuando se presentan estancamientos y obstáculos, los líderes de la protección al menor se involucran activamente con las partes reguladoras y con otras partes interesadas para vencer estos obstáculos.

- El éxito de las políticas y campañas para la salvaguarda del menor en línea se monitorea y se mide. Y las métricas se comparten con todas las partes interesadas relevantes.

Aunque las organizaciones involucradas reconocieron que la protección al menor en línea es un proceso de aprendizaje continuo, su búsqueda de mejores prácticas los ubican entre los líderes en la materia. Entre los participantes se encuentran Airtel, America Movil, DQ, Facebook, Global Partnership to End Violence Against Children, Ericsson, ITU, IWF, Kenyatta University, Microsoft, Moore Center, NetClean, Samena, Telia, UKE, UNESCO, UNICEF, WPGA, y Zain.

El mercado del talento tecnológico es extremadamente reñido, casi en cualquier parte del mundo.

La economía de los EE. UU. necesita 150.000 profesionales calificados más en el área de la tecnología de los que dispone [101]. En Europa, el número es de 420.000 [102]. En la región Asia Pacífico, es de un millón [103].

En un ambiente tan competitivo, el sector público y otras organizaciones dedicadas al combate del abuso de niños en línea se encuentran a menudo con la dificultad de atraer el talento tecnológico que se necesita para llevarle la delantera a los cada vez más motivados, innovadores y bien financiados agresores y ciberdelincuentes.

Algunas compañías privadas, que incluyen Facebook, Snapchat, Twitter y Google [70], trabajan de cerca con las agencias policiales, el gobierno y las ONG para desarrollar las herramientas y los métodos para combatir el abuso y la explotación de niños en línea. NetClean y Thorn han recopilado las prácticas adecuadas para la industria privada para confrontar el MASN en sus plataformas, además de ofrecer sus herramientas para que las compañías puedan detectar MASN [104] [105].

A parte de ayudar a las agencias especialistas dedicadas a promover la seguridad del menor en línea, las compañías privadas también pueden hacer importantes contribuciones para promover el bienestar digital de los niños, asegurándose de que sus propios servicios y plataformas sean seguros desde su diseño (vea la página 25 para más detalles).

Seis formas en que el sector privado puede ayudar en la lucha contra el abuso de niños en línea

Existen muchas maneras en las que el sector privado puede contribuir a la lucha contra el abuso de niños en línea, y estas son solo seis que podrían marcar una verdadera diferencia:

1. Garantizando que sus sistemas y servicios para niños son seguros desde su diseño.
2. Teniendo funciones moderadoras y de reporte destacadas y con amplios recursos.
3. Ofreciendo talento de programación e ingeniería que desarrolle tecnología antiabuso.
4. Trabajando de cerca con las agencias policiales para afrontar el abuso lo más rápido posible.
5. Trabajando con los reguladores e investigadores financieros para rastrear el flujo del dinero proveniente del abuso.
6. Trabajando para educar a maestros, padres y cuidadores, ayudándoles a mantener seguros a los niños de cualquier peligro en línea.

Recomendaciones 9



Recomendaciones

El objetivo principal del grupo de trabajo de la Comisión de Banda Ancha para la seguridad del menor en línea es hacer conciencia de los riesgos y amenazas para los niños que existen en Internet. También ofrece una serie de recomendaciones para minimizar dichos riesgos y amenazas, y además poder capitalizar de forma simultánea los beneficios que la expansión de la banda ancha traerá a los niños, particularmente a aquellos en países en vías de desarrollo.

El objetivo de las recomendaciones es movilizar la voluntad política y la acción colectiva por parte de las principales partes interesadas. Entre estas se incluyen gobiernos, reguladores, operadores, el sector privado, los medios sociales y las plataformas de juegos, los proveedores de servicio de Internet, la ONU y otras agencias enfocadas en el menor, además de los comisionados de la Comisión de Banda Ancha y sus socios. Ahora, debemos dar prioridad a la seguridad del menor en línea de manera colectiva.

Hoy en día, el mundo digital es el mundo en el que la mayoría de los niños en los países desarrollados viven, juegan y aprenden. Cada vez más, el mundo digital se está convirtiendo también en el mundo de los niños en los países en desarrollo. Este mundo debe respetar los derechos de los niños de ser libres de todas las formas de violencia, abuso y explotación. Debe de convertirse en un mundo más seguro, que prepare a las generaciones futuras para progresar en el espacio digital.

La meta de estas recomendaciones es brindar un marco que respalde la colaboración y la acción entre las partes interesadas, quienes juegan un papel integral en darle prioridad a la seguridad del menor en línea.

Declaración Universal de la Seguridad de los Niños en Línea

La Comisión de Banda Ancha para el Desarrollo Sostenible (Broadband Commission for Sustainable Development) recomienda que aquellos individuos y grupos que se consideren defensores de los derechos de los niños en el espacio digital, se unan a nuestra acción colectiva firmando la Declaración Universal de la Seguridad de los Niños en Línea para:

Incluir estrategias para la seguridad de los niños en línea en todos los planes nacionales de banda ancha o digitales para el 2021

En el 2003, la Comisión de Banda Ancha presentó una iniciativa de transformación que comprometía a los gobiernos para desarrollar planes nacionales de banda ancha. A la fecha, 163 países han implementado y siguen actualizando estos planes con socios que reciben el apoyo de la UIT que los evalúan y les exigen una rendición de cuentas.

Hacemos un llamado a todos los países para que implementen estrategias en base a evidencia para la seguridad de los niños en línea, siguiendo el ejemplo del Model National Response (respuesta del modelo nacional) de WePROTECT (para EASN y MASN) y otras estrategias que tratan los diferentes tipos de amenazas y riesgos, dentro de sus planes nacionales digitales o de banda ancha.

Prevenir, detectar, responder y actuar

Los jugadores de la industria a nivel nacional e internacional, incluyendo a operadores, proveedores de servicio de Internet y plataformas de medios sociales y de juegos, deben establecer un conjunto de capacidades mínimas, tecnologías, sistemas y protocolos, para detectar y lidiar con cualquier tipo de abuso (clasificado como actividad criminal) en contra de los niños. También deben trabajar con la sociedad civil para hacer conciencia de los problemas que rodean la seguridad de los niños en línea y ayudar a todos los adultos responsables del bienestar de los niños, incluyendo a los padres y cuidadores, colegios, organizaciones de servicio a la juventud y a las comunidades, a adquirir el conocimiento y las habilidades que necesitan para mantener a los niños a salvo.

La definición funcional del abuso en línea en contra de los niños debe incluir:

- Explotación y abuso sexual de niños (EASN).
- Material de abuso sexual de niños (MASN).
- Cualquier otra violación a la Convención sobre los Derechos del Niño (CDN), incluyendo el cyberbullying, la recolección de datos, o brindar servicios potencialmente dañinos para los niños.

Cuando estos detectan contenido en sus plataformas internas o en las plataformas que operan, que supervisan como reguladores, o tienen cualquier otro tipo de responsabilidades, las partes interesadas deben reportar y eliminar dicho contenido en colaboración con otros participantes relevantes.

Los líderes de la industria deben ayudar a las compañías más pequeñas a implementar soluciones por medio de tecnología, desarrollo de capacidad y procesos de denuncia.

Los derechos de los niños a ser protegidos contra crímenes (tanto en línea como fuera de la misma) deben ser una prioridad, sin tener que poner en riesgo el derecho a la privacidad de todos los usuarios de Internet (incluyendo a los niños mismos).

El establecimiento de mecanismos transparentes y responsables para garantizar los derechos de los niños están incluidos en el modelo operativo

Los niños representan más del 30 % de los usuarios de Internet. La expansión de la banda ancha en los países en desarrollo de África subsahariana, Asia y América Latina aumentarán significativamente esta cifra.

Al reconocer esto y la particular vulnerabilidad de los niños al abuso en línea, las partes interesadas deben comprometerse a establecer un cargo o equipo sénior, dedicado a integrar los principios de la Convención sobre los Derechos del Niño de la Organización de las Naciones Unidas dentro del modelo operativo de la organización misma.

Las compañías deben informar sobre las acciones, incluyendo los resultados, que lleven a cabo su equipo o administración, en sus informes anuales corporativos y de sustentabilidad. Los reguladores y otros organismos oficiales deben incluir esta información en su contabilidad anual a los legisladores u otros supervisores de relevancia.

Unificar las definiciones y la terminología y desarrollar estándares comunes

Las partes interesadas deben trabajar en conjunto para desarrollar un marco universal para la cooperación en la lucha contra el abuso de niños en línea. Esto debe incluir estándares para la operatividad interna que permita compartir los datos y la inteligencia entre las agencias de aplicación de la ley y las entidades de confianza de la sociedad civil y privada.

A lo largo de países y jurisdicciones, la legislación debe tener como objetivo adoptar definiciones y terminología consistentes, así como la clasificación de crímenes contra los niños en línea de acuerdo al Model National Response de WePROTECT y otros modelos e infraestructuras con base en evidencia. Debe removerse cualquier barrera legal a las compañías que empleen herramientas tecnológicas para combatir la violencia contra niños, por ejemplo haciendo que la información para hacer el análisis legal para la seguridad del menor en línea para cada país esté disponible por medio de entidades privadas de confianza sin costo alguno. Los países deben desarrollar una clasificación universal de contenido para poder facilitar el intercambio de datos.

Los datos técnicos deben estar disponibles para todos los sectores y jurisdicciones para facilitar los esfuerzos de gestión de casos por parte de las agencias policiales y así ayudar a identificar a las víctimas. Las partes interesadas deben comprometerse a apoyar el trabajo que produzca una mayor consistencia en la práctica respecto a la anotación de *hashes* y entrada de datos. Estos deben garantizar el mantenimiento seguro de datos concernientes a víctimas identificadas y sin identificar.

Deben usar un diseño apropiado a la edad y un consentimiento de datos serio para las plataformas de medios sociales y juegos, y otros servicios para niños en línea

Todas las compañías que desarrollan o utilizan soluciones para proteger a los niños, o que pueden ser usadas de cualquier manera directa o indirecta por ellos, deben reducir los peligros y las amenazas para la seguridad de los niños en línea. Deben tomar las medidas para verificar edades e identificar usuarios, y prevenir la propagación de odio, provocaciones o violencia, además de la producción y distribución de contenido dañino e ilegal como el MASN. Las compañías que ofrecen productos, servicios y apps en línea para niños deben usar un diseño de acuerdo a la edad, así como términos y condiciones que sean fáciles de entender para los niños. A los niños no se

les debe pedir su consentimiento de cosas que no sean, en términos legales, "lo más convenientes para el menor".

Invertir en recolección de datos e investigación y en el desarrollo y crecimiento de soluciones impulsadas por la tecnología

El sector privado debe trabajar con otros participantes, como las ONG y el mundo académico, para reducir los silos y fragmentaciones en el enfoque para el desarrollo y la disponibilidad de herramientas tecnológicas (incluyendo IA).

La tecnología que enfrenta las violaciones de los niños en línea debería, siempre que sea apropiado, ser una plataforma abierta o compartida, estandarizada, de acceso agnóstico y puesta a disposición de todas las partes involucradas de confianza, sin importar el sector al que pertenezcan. El sector privado y el público deben invertir recursos y apoyarse el uno al otro para desarrollar las soluciones tecnológicas que ayuden en la lucha contra el abuso de niños en línea.

Este trabajo no debe poner en peligro la labor de las agencias policiales ni la seguridad del menor. También existe la necesidad de invertir en investigación para entender el impacto que tienen las nuevas tecnologías digitales en los niños y poder así prevenir los riesgos y daños potenciales, y hacer algo antes de que los agresores en línea puedan aprovechar las nuevas tecnologías, las lagunas legislativas o en línea y los fenómenos sociales.

Desarrollar métricas comunes para la seguridad de los niños en línea

Trabajando juntos, la comunidad internacional debe desarrollar un conjunto de métricas universales que las partes interesadas puedan utilizar para medir cualquier aspecto relevante de la seguridad de los niños en línea. Las organizaciones y los individuos pueden utilizar estas métricas para determinar el éxito de las actividades de seguridad de los niños en línea leyendo los informes anuales de las instituciones y las agencias, incluyendo entre otras:

- UNICEF
- Unión Internacional de Telecomunicaciones (UIT)
- El Fondo Monetario Internacional (FMI)
- El Banco Mundial y otros bancos para el desarrollo
- La GSMA (asociación de la industria móvil)
- La Organización para la Cooperación y el Desarrollo Económicos (OCDE)
- La Unión Europea
- La Unión Africana
- La Liga Árabe
- El DQ Institute
- El Foro Económico Mundial

Usar las métricas del índice de The Economist Intelligence Unit y el Informe anual del estado de la banda ancha de la Comisión de Banda Ancha ayudará a las partes interesadas, a lo largo de las fronteras, a monitorear el progreso en las respuestas de los países ante el abuso sexual de niños y otras formas de violencia en línea.

Implementar la educación de habilidades digitales universales

A todos los niños se les debe enseñar habilidades digitales como parte de la estrategia para reducir los riesgos y aumentar las oportunidades que ofrece la tecnología.

La enseñanza de habilidades digitales debe ser parte de los planes de estudio centrales de los colegios y debe incluir una educación más amplia para los niños respecto al manejo de las relaciones, la creación de resiliencia, el desarrollo de habilidades de pensamiento crítico y la búsqueda de ayuda cuando sea necesario.

Para que esto sea posible, recomendamos que los líderes de los sectores público, privado y civil implementen en todos los niveles del currículum de inteligencia digital (DQI), desarrollada por el DQ Institute, o una que sea equivalente.

Para información adicional, vea el informe sobre Tecnología, Banda Ancha y Educación en: **https://www.broadbandcommission.org/Documents/publications/BD_bbcomm-education_2013.pdf**

10

Disposiciones modelo sobre protección de los niños para incluir en el plan nacional de banda ancha



Provisiones modelo para la protección al menor en línea para ser incluidas en los planes nacionales de banda ancha y leyes contra la ciberdelincuencia

La intención de estas provisiones es servir como guía para que la usen los países al momento de redactar su propia sección de protección al menor en línea en su plan nacional de banda ancha.

1.1. Provisiones relevantes que deben verse reflejadas en los planes nacionales de banda ancha

Las siguientes provisiones deben ser incluidas en los planes nacionales de banda ancha para establecer la base adecuada para un enfoque que sea informado, efectivo y que se pueda hacer cumplir para la protección al menor en línea.

1.1.1 Adhesión a las convenciones y protocolos internacionales

La adhesión a las convenciones y protocolos internacionales demuestra la conciencia así como la disposición y el compromiso de un país para adoptar las mejores prácticas, códigos de conducta, herramientas, políticas, terminologías estándares, y la información compartida a nivel internacional y también a cooperar con otros firmantes. Además, ayuda a acelerar el conocimiento y la implementación de los procesos relevantes.

Debe incluirse una provisión que establezca formalmente la adhesión de un país a la Convención sobre los Derechos del Niño de la ONU (CDN), la cual entró en vigencia el 2 de septiembre de 1990. El objetivo de la CDN es asegurar una amplia variedad de derechos humanos para los niños, incluyendo derechos civiles, culturales, económicos, políticos y sociales.

También se debe incluir una provisión que establezca la adhesión del país al Protocolo Opcional de la Convención sobre los Derechos del Niño de la ONU, referente a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, el cual entró en vigor el 18 de enero de 2002. Este es uno de los instrumentos internacionales jurídicamente vinculantes más importantes que pueden usarse para analizar los procesos legislativos y regulatorios para tratar los delitos de MASN, alineado con los estándares internacionales de relevancia.

Se debe incluir una provisión que establezca la adhesión al Convenio de Budapest contra la ciberdelincuencia del 23 de noviembre de 2001. Este representa el primer instrumento vinculante intergubernamental que trata los delitos de MASN que son facilitados por el computador.

Debe incluirse una provisión que establezca la adhesión al Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación Sexual y el Abuso Sexual o Convenio de Lanzarote del 25 de octubre de 2007. Este instrumento contiene provisiones que tratan con delitos de MASN y delitos de grooming en línea. Establece las diferentes formas de abuso sexual a niños como crímenes, incluyendo el abuso cometido en el hogar o por familiares, por medio de la fuerza, intimidación o amenazas.

1.1.2 Definiciones

Deben establecerse provisiones en los planes nacionales de banda ancha y leyes sobre ciberdelincuencia para definir lo que significa un delito dentro del contexto de la protección al menor en línea. Se anticipa que pudiera adoptarse la siguiente definición:

Un delito en contra de un menor en el medio en línea debe definirse como:

- Cualquier acto u omisión que incluyan, entre otros, el manejo de (producción, preparación, transmisión, almacenamiento, publicación o promoción) contenido (libros, escritos, dibujos, fotos, películas, símbolos con el propósito de explotación, seducción, distribución o exhibición, grabación de audio, música, programas de software, aplicaciones móviles o juegos electrónicos) si el tema tiene que ver con un menor de 18 años de edad y si el material muestra o puede ser usado para cometer abuso sexual a un menor.
- Grooming en línea, explotación sexual, contacto no autorizado y pago para que un menor lleve a cabo actos ilegales.

- Provisión ilegal de bienes o servicios a niños y jóvenes, que son dirigidos a adultos.
- Provisión de bienes o servicios que, si se usan sin restricciones, pueden ocasionar que los niños o jóvenes desarrollen una adicción a la tecnología.
- Uso de herramientas en línea para perpetuar el tráfico de niños.
- El no reportar un delito en contra de un menor o de menores, dentro de un tiempo razonable, a las autoridades policiales u organismo de supervisión cuando un individuo o entidad tiene conocimiento implícito o real de dicho delito.

1.1.3 Iniciativas a nivel nacional

Las provisiones deben estar descritas en los planes nacionales de banda ancha estableciendo compromisos para llevar a cabo iniciativas de protección al menor en línea en base a objetivos específicos.

Por ejemplo, al plan de acción adoptado por Suecia:

- Los objetivos que tiene el gobierno son para garantizar que ningún menor en Suecia sea sometido a explotación sexual; que ningún menor de otro país sea explotado sexualmente por personas de Suecia; que las víctimas de explotación sexual que sean menores de edad reciban todo el apoyo y la ayuda que necesitan; y que Suecia contribuya a la cooperación internacional relacionada con este tema.

1.1.4 Responsabilidades de los intermediarios

Debe incluirse una provisión que aborde las responsabilidades de los intermediarios, tales como los proveedores de redes de comunicaciones electrónicas y los prestadores de servicio de Internet. Esta provisión debe demostrar el compromiso del país para garantizar que las compañías de información, comunicaciones y tecnología que lleven a cabo obras dentro de sus fronteras nacionales, y que actúen como intermediarios, den los pasos constructivos para prevenir que aparezcan en los portales gestionados por estas compañías imágenes, videos y enlaces a material de abuso de niños. Debe incluir provisiones que obliguen a los proveedores de tecnología a garantizar que las nuevas técnicas de codificación no hagan imposible el uso de las herramientas diseñadas para detectar material de abuso de niños, identificar víctimas y reunir evidencias de los delincuentes.

La ley requerirá que los ISP quiten de la vista el material de abuso sexual de niños en cuanto sepan de su existencia. Al mismo tiempo, el ISP denunciará el material y la persona o entidad que lo publicó con las autoridades policiales relevantes al caso o a la línea de ayuda de denuncia en Internet. El ISP no notificará de modo alguno al cliente de que se ha retirado el MASN de la vista, ya que con esto se corre el riesgo de alertar a los delincuentes de que están siendo investigados.

1.1.5 Obligaciones impuestas a los creadores de juegos

Debe incluirse una provisión que requiera que los creadores de plataformas de juegos apliquen controles de tiempo de pantalla (por defecto) y otros controles parentales para monitorear y supervisar el uso de dispositivos de juegos y para mitigar los efectos negativos del uso prolongado y excesivo de los dispositivos que dan como resultado las adicciones. Las compañías que no estén involucradas directamente en la creación sino en el mercadeo de dichos juegos en línea, deben hacer todo lo posible para que los creadores de las plataformas de juego implementen dichos controles. Las plataformas de juegos que operen salas de chat, foros y otros elementos parecidos deben asegurarse de que los niños estén a salvo del grooming, el bullying, el robo de datos y de otras amenazas cuando usen estas funciones.

1.1.6 Compromiso para trabajar con organizaciones de terceros

Se debe incluir una provisión en la que el país se comprometa a asegurarse de trabajar con organizaciones internacionales de terceros, tales como Child Online Protection (protección al menor en línea, o COP) de la UIT, WePROTECT Global Alliance, Global Partnership to End Violence Against Children, Child Dignity Alliance, Virtual Global Taskforce (VGT), o Internet

Watch Foundation (IWF), por nombrar algunos.

El WPGA es un movimiento internacional dedicado a la acción nacional y global para terminar con la explotación sexual de niños en línea. El VGT es un grupo de colaboración internacional de agencias policiales, organizaciones no gubernamentales y socios de la industria, para proteger a los niños de la explotación sexual en línea y fuera de la misma. La IWF ofrece una vía segura para la denuncia anónima de imágenes y videos de abuso sexual de niños en línea, lleva a cabo sus búsquedas por medio de lo último en tecnología y retira cualquier contenido ilegal. Además, existen otras organizaciones e iniciativas que tratan el tema del cyberbullying y otras formas de amenazas y daños en línea.

1.1.7 Protección de datos

Debe incluirse una provisión en la que el país hará cumplir los estándares legales pertinentes para la protección de datos personales y la privacidad en línea, particularmente de los niños. El gobierno del Reino Unido ya lo hizo, con su Data Protection Act (Ley de protección de datos) de 2018, la cual incluye provisiones de protección de datos específicos para menores de 18 años, y con su estrategia de privacidad desde el diseño, líder en el mundo. La ley se basa en los esfuerzos que han dado a los legisladores del Reino Unido una mejor comprensión del papel que tienen los datos en las experiencias en línea de los niños: por ejemplo, el papel que tienen las máquinas de búsqueda de recomendaciones que por medio de los datos que recaban promueven material inapropiado, como sitios pro anorexia, materiales para autolesionarse, contenido adictivo, y cosas por el estilo, para usuarios menores de edad [106]. Muchos otros países están ahora en proceso de hacer lo mismo.

1.2 Provisiones relevantes para las leyes contra la ciberdelincuencia

1.2.1 Definiciones

Debe incluirse una provisión en la ley de ciberdelincuencia en la que se defina lo que significa un ciberdelito en contra de un menor. La definición que se estableció anteriormente en la sección 1.1.2. se puede aplicar.

1.2.2 Creación de mecanismos de denuncia y de una agencia de apoyo institucional para la protección al menor en línea

Debe incluirse una provisión que establezca una agencia reconocida oficialmente que brinde el apoyo institucional para la protección al menor en línea. Por lo general, el Computer Emergency Response Team (equipo de respuesta a emergencias por computadora, o CERT) toma la responsabilidad de gerenciar la protección a los niños en línea, y reporta al NCMEC, a la INTERPOL y al ICMEC.

Debe incluirse otra provisión que institucionalice la creación de una vía, como un portal, línea de ayuda telefónica, la línea nacional de ayuda al menor (donde funcione) o aplicación móvil, por medio de la cual se puedan denunciar los incidentes que tengan que ver con la protección al menor en línea. Además, debe ponerse un portal a disposición de los niños, los padres y educadores para informarles respecto a las amenazas que existen en línea, mejores prácticas, políticas y herramientas para la ciberseguridad y por medio del cual se puedan hacer consultas o denuncias.

De manera similar, debe ponerse un portal a disposición de los representantes del gobierno, agencias policiales, organizaciones no gubernamentales y académicos para que también puedan monitorear y detener de manera continua amenazas en línea. El Global Partnership to End Violence Against Children (sociedad global para acabar con la violencia en contra de los niños) con su demostrada capacidad de convocatoria, neutralidad y alcance global, podría desempeñar un papel en la creación de una plataforma para que todas las partes interesadas se involucren y actúen para que los niños estén seguros en línea y poner esto dentro de la agenda general enfocada en acabar con todo tipo de violencia.

Conclusiones 11



Conclusiones

La humanidad está en medio de la 4.ª Revolución Industrial, impulsada por la conectividad en masa y las tecnologías emergentes, como la inteligencia artificial (IA), el Internet de las cosas (IdC), la realidad virtual (RV), criptomonedas y fabricación aditiva (impresión en 3D).

La nueva revolución industrial, igual que su predecesora, tiene el potencial de hacernos más ricos, más seguros y más felices. Pero como su predecesora, también trae consigo muchos daños potenciales, particularmente para los niños.

Sin embargo, a diferencia de nuestros antepasados del siglo diecinueve, quienes tuvieron relativamente poco control sobre su ambiente y solo un entendimiento parcial de los cambios por los que estaban atravesando, en el siglo veintiuno contamos con la experiencia, la tecnología y los datos que nos ayuden a entender y pronosticar los beneficios y también los riesgos y peligros relacionados con la forma en que nuestras sociedades se están transformando.

Nosotros debemos usar este conocimiento y experiencia para salvaguardar a nuestros hijos de los peligros en línea, así como de los peligros del mundo fuera de línea que son permitidos o promovidos por la actividad en línea. Tenemos la oportunidad de salvar a millones de niños de un sufrimiento innecesario, y prevenir los daños que dejarán a nuestras sociedades incapaces de obtener el máximo beneficio de la transformación digital que están experimentando.

La buena noticia es que muchas de las herramientas necesarias para actuar en contra del flagelo de la violencia, la explotación y el abuso de los niños, existe. Pero con mucha frecuencia, el trabajo que se requiere para crear estas herramientas en una jurisdicción no se comparte en otra.

Todas las partes interesadas, abarcando desde gobiernos, agencias policiales, el sector privado y los expertos en la materia reconocen que también necesitamos herramientas nuevas y más efectivas que se pueden compartir, como las plataformas agnósticas, y/o abiertas.

El sector privado está en una buena posición para invertir en el desarrollo y la difusión de soluciones impulsadas por la tecnología con la cooperación de los gobiernos, las ONG (la comunidad de expertos), agencias policiales y otras partes interesadas. Pero también se requiere de más apoyo, fondos, participación y experiencia técnica del sector privado. Sin embargo, también existe la necesidad de promover y fortalecer el apoyo a las iniciativas globales, como el End Violence Fund (fondo para acabar con la violencia), el cual es actualmente la iniciativa global líder que invierte en el desarrollo de soluciones impulsadas por la tecnología.

El tiempo y los recursos que se emplean duplicando los esfuerzos pudieran usarse para la detección y aplicación de la ley, o en cualquier otra área de la protección de niños en línea. Es por eso que existe la urgencia de que los países cooperen para desarrollar estándares, sistemas y protocolos comunes. Solo de esta manera, la protección de nuestros hijos puede ser tan sólida, eficiente y de acción rápida como se necesita para prevenir el flagelo de la violencia contra los niños en línea, particularmente en los países en desarrollo donde viven hoy la mayoría de los niños y quienes estarán en línea en el futuro cercano.

La explotación y el abuso de niños endémicos pueden prevenirse, pero se requiere del compromiso de todos para proteger a los niños cuando usen el Internet. Debemos trabajar juntos para empoderar a los niños de todos los niveles y estilos de vida para que obtengan los beneficios de la conectividad, a la vez que evitamos o mitigamos los riesgos relacionados con la conectividad que enfrentan hoy día.

Reconocemos que para avanzar nuestra visión y metas en común se requiere de acciones individuales y colectivas. Por lo tanto, necesitamos:

- Incluir los derechos de los niños en nuestra estrategia de banda ancha y en todas las demás áreas relevantes de la política nacional.
- Cooperar a nivel transfronterizo para crear estándares y terminologías válidos a nivel internacional para definir y medir la condición de los derechos y la protección del menor en línea.
- Garantizar que los productos y servicios diseñados para niños de parte del sector público o privado o de las ONG, tengan los derechos de los niños en el centro de sus principios operativos.
- Trabajar con el sector privado, la sociedad civil, expertos en la materia y socios para desarrollar los estándares de los derechos de los niños en línea para nuestras respectivas jurisdicciones.
- Desarrollar maneras de involucrar a las partes interesadas locales relevantes en campañas en contra de los peligros como la explotación de los niños y otros temas de los derechos de los niños en línea.
- Emplear tecnologías nuevas e innovadoras como IA, análisis de datos y datos de diseño, para prevenir que los delincuentes usen las redes y los servicios.
- Realizar un progreso medible para bloquear el subir MASN y otro tipo de material que no sea de abuso sexual de niños o dañino para los niños en los servicios y productos bajo nuestras respectivas jurisdicciones.
- Comprometer a nuestras organizaciones a cooperar a lo largo de las fronteras con los socios de relevancia para detectar, detener y, donde sea posible, prevenir daños a los niños en línea.

Para ayudar a movilizar a todos los participantes en el ámbito de la seguridad en línea, el grupo de trabajo desarrolló una Declaración Universal para la Seguridad de los Niños en Línea. Basándose en las recomendaciones del informe, la declaración es una expresión de nuestro compromiso con los niños y con su bienestar.

El propósito de la declaración es ayudar a la movilización de las partes interesadas, como las compañías de tecnología y reguladores que estén en la posición de contribuir directa o indirectamente para mejorar la seguridad de los niños en línea.

Puede consultar la declaración en:
www.childonlinesafety.org

Le pedimos que comparta este informe con cualquier persona que usted sepa que tiene alguna influencia en asuntos concernientes a la seguridad de los niños en línea.

12 Casos de estudio y mejores prácticas



Caso de estudio 1: Convención sobre los Derechos del Niño de la Organización de las Naciones Unidas

Por 30 años, la Convención sobre los Derechos del Niño de la Organización de las Naciones Unidas (CDN) ha sido el estándar modelo por medio del cual interpretar los derechos de los niños en los diferentes medios. Sus más de 40 artículos clasifican los derechos de los niños y ofrecen una estructura con la cual los estados nacionales entienden sus responsabilidades con aquellos menores de 18 años. Este es el tratado más ratificado en la historia, y más de 190 estados son signatarios.

Desafío

Dentro de las naciones con una amplia conectividad, la niñez se ha ido transformando con la llegada y la adopción de las tecnologías que median, mejoran e interactúan con casi la mayor parte de las experiencias del niño: desde la educación, el juego y el entretenimiento, hasta la salud, la comunicación y la justicia. Por el contrario, la falta de la conectividad o el acceso a la misma tecnología tiene un impacto en las oportunidades de vida del menor.

Mientras fijamos la mirada en que la población mundial esté conectada en línea, debemos tomar en cuenta cómo hacer efectivos los derechos de los niños en el ambiente digital; tanto su derecho a estar conectados para poder participar en la sociedad y, una vez conectados, cómo mantener y ejercer sus derechos existentes ya por mucho tiempo, para asegurarnos que la adopción de la tecnología digital tome en cuenta el florecimiento de los niños desde su diseño y por defecto.

La Observación General sobre los derechos de los niños en cuanto al medio digital funge como un complemento para la convención, y expone la importancia de los derechos de los niños en el mundo digital.

Estrategia

La fundación 5Rights Foundation está dando su apoyo al Comité sobre los Derechos del Niño (CDN) para desarrollar la Observación General. Dirigido por la profesora Sonia Livingstone, el grupo de trabajo del comité ha emprendido una revisión profunda de la literatura, una consulta pública de tres meses y ha diseñado talleres con la participación de más de 400 niños provenientes de un amplio número de contextos alrededor del mundo.

Se llevará a cabo una consulta experta presentada por 5Rights Foundation en nombre del Comité, en Londres en el otoño del 2019. Este grupo de expertos representado por todo tipo de especialidades, diferentes sectores, naciones y contextos, llevará a cabo un análisis detallado de este primer boceto. Se dará a conocer un boceto con correcciones para consulta pública, y el Comité considerará la presentación durante su reunión en mayo del 2020.

Una vez que se llegue a un acuerdo, la Observación General será divulgada a un grupo amplio de partes interesadas; e incluirá la publicación de trabajo académico, recursos orientados a niños, webinars y contribuciones a encuentros en materia de políticas, plataformas y medios.

Resultados

En un mundo interconectado, si un niño no cuenta con la seguridad para gozar de sus derechos en un contexto determinado, no puede ejercer estos derechos en ningún otro contexto. La Observación General añadirá a lo que ya sabemos respecto a cómo diseñar el mundo digital tomando en cuenta a los niños, y de esta manera solidificar y asegurar los derechos de los niños en la era digital.

Caso de estudio 2: Protección al menor en línea en Ruanda (financiado por End Violence Fund)

Con el despliegue de la banda ancha y una mayor disponibilidad de teléfonos inteligentes, Ruanda decidió crear una infraestructura que garantizara la seguridad de los niños en línea.

Desafío

Ruanda necesitaba una política de seguridad de los niños en línea que reflejara las inquietudes de las partes interesadas del país, que incorporara las mejores prácticas dentro de la comunidad global, que siguiera los procesos y la documentación del gabinete, además de construir una capacidad a nivel institucional en una era de nuevas políticas.

Fue en este contexto positivo que el gobierno de Ruanda invitó a la 5Rights Foundation para desarrollar una Política de Protección de los Niños en Línea. Trabajando al lado de la profesora Julia Davidson de la University of East London, la 5Rights Foundation desarrolló una Política Nacional de Protección de los Niños en Línea y un Plan de Implementación.

Estrategia

Se formó en el Reino Unido un grupo de trabajo multidisciplinario, conformado por expertos en aplicación de la ley, abuso y trauma de los niños, desarrollo de los niños, leyes, protección de datos, telecomunicaciones, empresas, distribuidores de servicios del gobierno y de derechos del menor, para tomar en cuenta áreas clave para esta política.

Se identificaron disciplinas similares existentes en Ruanda y, con el apoyo del Ministerio de Tecnología de la información y comunicaciones e innovación de Ruanda, pudieron participar con colegas con experiencia en justicia, aplicación de la ley, educación, trabajo social y familia.

Por medio de un análisis de deficiencias amplio, incluyendo entrevistas con miembros del gobierno, mesas redondas, revisión de la literatura y talleres académicos, el equipo desarrolló un entendimiento de la capacidad digital existente en Ruanda.

Los problemas identificados por el análisis de deficiencias, aunado a los problemas de las políticas de los tratados y mejores prácticas internacionales existentes y por medio de las observaciones de los miembros expertos del grupo de trabajo, fueron incorporados en el documento final de política e implementación.

Resultados

La colaboración entre la 5Rights Foundation y el gobierno de Ruanda llevó a la creación de un documento de política de alto nivel, en el que se establecen ocho objetivos de la política. En este documento se presentaron las áreas claves, las responsabilidades, los facilitadores y el trabajo de las diversas partes interesadas que exige la Protección de los Niños en Línea.

Caso de estudio 3: Albania: Un Internet más seguro y mejor para los niños y jóvenes en Albania (financiado por el End Violence Fund)

El dominio de Internet de Albania ".al" aparece a menudo como uno de los principales servidores huéspedes de MASN. A pesar de que Albania ratificó cualquier legislación internacional central referente a MASN, entre el 2016 y el 2018 la policía solamente identificó 12 presuntos casos de abuso de niños y solo se detectó un posible delincuente.

Desafío

El análisis demostró que un marco legal pobremente desarrollado y confuso respecto a la protección de los

niños contra peligros en línea estaba contribuyendo a índices de detección bajos. Los convenios internacionales de relevancia no están codificados en la ley criminal, y como tal no se puede acceder a la ley internacional ni se puede hacer uso de ella.

Estrategia

La Ley Sobre Derechos y Protección del Menor de Albania de 2017 fue redactada con el apoyo técnico directo de UNICEF. Esta consagra el principio de la protección de los niños contra toda clase de abuso, daño y explotación (en línea y fuera de ella) y por tanto obliga al gobierno a implementarla.

A continuación, UNICEF estableció una plataforma de colaboración sólida para todas las instituciones gubernamentales clave, grupos de la sociedad civil, representantes del sector privado y los niños mismos, para consultar y dialogar sobre provisiones procesales concretas para la protección del menor contra los peligros en línea.

Trabajando al lado de una variedad de partes interesadas del sector público y privado, la plataforma de colaboración creó un boceto final de la legislación secundaria, desarrollando el tema de la implementación y la protección al menor contra los peligros en línea, la cual fue redactada dentro de los siguientes seis meses y enviada con éxito al Consejo de Ministros para ser adoptada.

Resultados

En julio del 2019, el Consejo de Ministros de Albania respaldó la decisión clave (por ley) respecto a "Medidas para proteger a los niños de materiales dañinos e ilegales en línea". Esta presenta por primera vez una provisión legal y las responsabilidades institucionales para la protección del menor de contenido en línea dañino e ilegal.

Por otra parte, establece los procedimientos para la remoción inmediata de contenido dañino e ilegal del Internet, así como para la denuncia y las vías de derivación para el abuso de niños en línea, el bullying y la explotación sexual. El impacto de este resultado de alto alcance afectará de manera positiva a casi todos los niños en Albania.

Caso de estudio 4: Filipinas: Acabando con la explotación sexual de niños en línea en Cebu (financiado por el End Violence Fund)

Filipinas se ha convertido en un centro de actividad, donde la explotación y el abuso sexual de niños (EASN) en línea está creciendo rápidamente. Su gobierno decidió que debía hacerse algo al respecto.

Desafío

En tan solo un mes en el 2015, Filipinas recibió más de 2600 notificaciones de los EE. UU., informándole de la detección de nuevos web filipinos de abuso a niños. Hasta que las leyes en Filipinas sean aplicadas con más eficiencia, estos números seguirán aumentando.

Estrategia

La International Justice Mission (Misión de justicia internacional), una ONG de derechos humanos, se asoció con el gobierno de Filipinas para fortalecer su capacidad de tratar la explotación y el abuso sexual de niños (EASN) en línea, en particular el intercambio de material de streaming en vivo de abuso sexual de niños y otro material de explotación de niños entre clientes y traficantes de niños.

La IJM trabajó con el sistema de justicia para rescatar y rehabilitar a las víctimas, hacer responsables a los delincuentes por los delitos, aumentar la capacidad de las autoridades locales y detectar los vacíos específicos en el sistema de justicia público que diera como resultado la impunidad.

La ONG también colaboró directamente con las agencias policiales locales e

internacionales, incluyendo los sistemas de policía y de tribunales, para identificar y rescatar a las víctimas, arrestar a los agresores y reunir suficiente evidencia para apoyar las acusaciones.

Resultados

Para julio del 2019, la IJM y las autoridades filipinas trabajando en equipo han rescatado a 123 niños de agresores sexuales. Además de rescatar a las víctimas, la IJM ha ayudado a la policía a arrestar y acusar a 20 presuntos responsables y a apoyar a los fiscales a presentar cargos contra los sospechosos, además de brindar apoyo a los fiscales a nivel nacional y local con sus casos en curso.

La IJM fortaleció aún más su capacidad entrenando a más de 50 oficiales de las agencias policiales y a 100 jueces y fiscales filipinos sobre las complejidades de investigar y juzgar estos delitos. La IJM sigue abogando con el congreso de Filipinas y con otras agencias para cumplir con el compromiso del gobierno de tres años para fortalecer al personal y para financiar la Unidad de protección de mujeres y niños a nivel nacional.

Caso de estudio 5: 'I Click Sensibly' (Hago clic con cuidado) — Educación digital en Polonia

La UKE es el órgano regulador responsable de supervisar el Internet en Polonia. Este sabía que niños muy pequeños estaban usando a menudo teléfonos inteligentes con poca o ninguna restricción ni orientación.

Desafío

Este cuerpo regulador necesitaba saber qué tipo de actividades estaban llevando a cabo los niños en línea y los riesgos que estas representaban. Aún más, necesitaba encontrar una manera de enseñar a los niños y a los padres a estar seguros en línea y a entender y manejar los riesgos.

Estrategia

En respuesta a estos desafíos, la UKE creó la campaña 'I click sensibly' (Hago clic con cuidado). Esta contiene dos partes. La primera fue una serie de clases sobre seguridad en Internet. Durante las clases especializadas, los entrenadores de la Oficina de Comunicaciones Electrónicas dialogaron sobre cómo navegar en línea de forma responsable, de lo que deben estar conscientes cuando naveguen en línea y cómo usar los dispositivos de telecomunicaciones de forma segura.

A los niños que asistieron a los talleres también se les enseñó a cómo lidiar con el cyberbullying o con la incitación al odio, cómo lidiar con la agresión en línea y cómo proteger sus datos. Con las clases también se enseñó a los padres cómo filtrar el contenido inapropiado y a controlar cómo los niños pasan su tiempo en Internet.

Al mismo tiempo, UKE encuestó a muchos de los niños que asistieron a las clases para averiguar cómo usaban el Internet y a qué riesgos y daños podrían estar expuestos. Las encuestas se llevaron a cabo usando entrevistas personales con ayuda de computadora.

Resultados

Más de 50.000 niños se beneficiaron directamente de las clases. Usando la encuesta, UKE también pudo reunir información detallada sobre cómo los niños pasaban su tiempo en línea, los riesgos a los que estaban expuestos y qué tan bien capacitados estaban sus padres para apoyarlos. En un tiempo donde muchas agencias nacionales e internacionales ni siquiera tienen datos sobre las vidas en línea de los niños, UKE tiene estadísticas detalladas sobre temas, tales como el porcentaje de niños que han sido ridiculizados o acosados en línea, qué tan bien pueden los niños evaluar la veracidad de la información que encuentran en Internet, y cuántos padres ejercen control sobre los que sus hijos hacen y ven en línea.

Caso de estudio 6: Perú: Colaboración interdisciplinaria y entre sectores para prevenir y responder a la realidad de la explotación sexual de niños en línea en Perú (financiada por el End Violence Fund)

De acuerdo con el Instituto de Estadísticas Nacionales, en Perú, cerca del 50 % de niños de 6 a 17 años usan el Internet. El ministro del interior del país afirmó que, entre el 2014 y el 2017, 22 % de los casos del tráfico para la explotación sexual se originó en línea. Esto es un reflejo de las conclusiones a las que llegó la Child Rights International Office (Oficina internacional para los derechos del niño) advirtiendo que la tecnología de la información y comunicaciones estaba siendo usada para acosar sexualmente a niños para poder luego traficarlos para ser explotados sexualmente.

Desafío

Perú cuenta ya con una política y un marco legal relativamente sólidos para el combate de la explotación sexual de niños, comparado con sus contrapartes en Latinoamérica. El país ya es signatario de los ODS, el CDN y el Model National Response Statement of Action (Declaración de acción del modelo de respuesta nacional) del WPGA, además del Convenio de Budapest contra la ciberdelincuencia. Sin embargo, el número de quejas y casos que llegan a los juzgados es bajo. Aún más, ninguna de estas políticas ni marcos legales menciona explícitamente cómo tratar o lidiar con el creciente problema de la EASN en línea. También existen enormes brechas en lo referente a la información de la EASN, las nuevas formas de explotación en línea, los recursos y mecanismos para proteger a los niños, la coordinación entre los diferentes sectores, el entrenamiento y la concientización.

Estrategia

Con el apoyo económico del End Violence Fund y Capital Humano y Social (CHS) Alternativo, una organización no gubernamental de derechos humanos con sede en Perú, el país llevó a cabo cambios al código penal peruano en el que extendió la definición de la explotación sexual de niños y criminalizó esta actividad en todos los ámbitos. La contribución más importante de CHS fue el apoyo técnico que dio a las comisiones de la Mujer y la Familia, y de Justicia y Derechos del Congreso de la República.

Gracias a los esfuerzos de CHS y de las organizaciones de apoyo, diez artículos del código penal están listos para ser modificados, y siete más serán añadidos. Los cambios propuestos crean delitos y sentencias que tienen que ver con la explotación sexual de niños, el recibir un beneficio por coordinar, promover o favorecer la explotación sexual de niños. Pagar para tener relaciones con un menor también está cubierto en el código actualizado.

Además de trabajar para un cambio sistémico, el CHS también ha creado conciencia de esta amenaza y ha educado a 400 niños y 600 miembros de la comunidad (maestros, padres y proveedores de servicios) directamente respecto a cómo responder a la explotación sexual de niños, tanto involucrándose en los principales medios de difusión como por medio de capacitación en persona.

Resultados

El congreso aprobó la propuesta de ley y la versión final fue firmada y convertida en ley por el presidente de Perú en junio de 2019.

Caso de estudio 7: Protección al menor en línea en Vietnam (financiado por End Violence Fund)

Al elevarse el número de jóvenes en línea en Vietnam, también se elevaron los riesgos. Para enfrentar el problema de la seguridad en línea, ChildFund Vietnam inició la iniciativa Swipe Safe (navega seguro).

Desafío

Para el 2018, los jóvenes de entre 15 y 24 años de edad conformaban más de una tercera parte de los 54.7 millones de usuarios de Internet en Vietnam. Este hecho ha aumentado su exposición a todo tipo de abuso sexual en línea y otros peligros que existen en línea, y ha llevado a uno de cada tres estudiantes a sufrir de cyberbullying.

Esto ha sido exacerbado por los bajos niveles de conocimiento digital tanto de niños como de padres. Con la falta de herramientas y material que promuevan la seguridad en línea, existe un precario entendimiento del comportamiento en línea riesgoso y poco o ningún consejo sobre cómo estar seguros en línea.

Estrategia

Con el fin de ayudar a los jóvenes a navegar el Internet de forma segura, ChildFund Vietnam estableció la iniciativa Swipe Safe (navega seguro). Este programa enseña los riesgos potenciales que hay en línea, como las estafas cibernéticas, el bullying o el abuso sexual, y presenta consejos y métodos para mantenerse seguros.

Swipe Safe motiva a padres, hijos, escuelas y el sector privado a tomar un papel más activo respecto a la seguridad en línea de los niños. El programa ofrece capacitaciones para padres y administradores de cafés de Internet para identificar y encarar los peligros para los niños. Además, este da apoyo a escuelas para que desarrollen políticas fáciles de entender para los niños y dirección sobre seguridad en línea.

Una innovación clave del programa es el hecho de involucrar a voluntarios jóvenes con un amplio conocimiento sobre tecnología para entrenar a otros miembros de sus comunidades locales. Estos entrenadores se identifican directamente con las experiencias de otros jóvenes y ayudan a mantener el plan de estudios actualizado.

Resultados

Para junio del 2019, más de 8700 adolescentes, 1100 padres y 1000 "socios para la seguridad en línea" (incluyendo funcionarios del gobierno, representantes de escuelas y miembros de la Unión de Jóvenes) han recibido capacitación sobre seguridad en línea por medio del programa.

Las encuestas indican que el 91 % de los niños a quienes se dirigió el programa demostró un aumento de conocimiento sobre seguridad en línea. Este incluyó habilidades tales como configuraciones de privacidad, revisión de la información, compartir de forma responsable, búsqueda en línea y denuncia de contenido dañino. De aquellos encuestados, el 89 % supo adónde acudir para recibir ayuda y el 30 % se sentían más seguros en línea.

Caso de estudio 8: Uso de la tecnología para mantener a los niños seguros: Colaboración de Facebook con el NCMEC

Desafío

El abuso sexual de niños es un delito aberrante que afecta a aproximadamente 9 a 19.7 % de las niñas y 3 a 7.9 % de los niños. A los expertos en seguridad, a las

ONG, a gobiernos y compañías les interesa prevenir y romper con la explotación sexual de niños en todas las tecnologías que existen en línea, y deben trabajar juntos cuando sea posible para ser más eficaces.

Estrategia

Por ser la oficina de información y de denuncia integral de la nación para todos los temas relacionados con la prevención y la recuperación de víctimas menores de edad, el National Center for Missing and Exploited Children (Centro nacional de niños extraviados y explotados, o NCMEC) lleva la delantera en la lucha contra el secuestro, el abuso y la explotación.

Desde el 2016 Facebook lleva a cabo el Child Safety Hackathon (maratón de hacking de seguridad de los niños) cros-sectorial para desarrollar nuevas herramientas y tecnología para seguridad de los niños de socios de compañías sin fines de lucro como el NCMEC. El evento de dos días reúne a ingenieros y científicos de la información de compañías socias de la Technology Coalition (coalición por la tecnología) y de otras para desarrollar nuevas tecnologías que ayuden a salvaguardar a los niños. Los *Hackathons* (maratones de hacking) son una gran oportunidad para reunir personas de diferentes organizaciones con una amplia experiencia en la construcción de herramientas y en enfrentar problemas como el de la explotación sexual de niños en línea. Todos los códigos y prototipos de acceso abierto desarrollados en el Child Safety Hackathon se donan de nuevo a la Technology Coalition y a los socios en seguridad como el NCMEC, para que los utilicen para avanzar en sus esfuerzos sobre seguridad de los niños.

Construyendo a partir de la generosa contribución de parte de Microsoft con el PhotoDNA para combatir la explotación de niños hace diez años, y con el más reciente lanzamiento de Google Content Safety API en el Child Safety Hackathon del 2019, Facebook también anunció sus dos tecnologías de acceso abierto que detectan fotos y videos idénticos o casi idénticos, compartiendo alguna de la tecnología que utilizan para combatir el abuso en su plataforma con otros que también trabajan para un Internet seguro. Estos algoritmos son de acceso abierto en GitHub para que los socios de la industria, desarrolladores pequeños y organizaciones sin ánimo de lucro puedan usarlos para identificar más fácilmente contenido de abuso y compartir los resúmenes criptográficos, o huella digital, de los diferentes tipos de contenido dañino. Para aquellos quienes usan ya su propia tecnología u otra tecnología de comparación de contenido, estas tecnologías son otra línea de defensa y permiten a los sistemas de resumen criptográfico comunicarse entre sí, logrando que los sistemas sean mucho más poderosos.

Resultados

Entre los prototipos desarrollados en el *hackathon* se encuentran proyectos que mejoran la eficiencia para quienes trabajan en la identificación y el rescate de niños al hacer más fácil el ordenar rápidamente imágenes y datos y darle así prioridad a los casos. Por ejemplo, en el 2019 los equipos desarrollaron el prototipo de una función que permitiera a la herramienta de gestión de casos CyberTipline del NCMEC indagar y comparar elementos dentro de las bases de datos de otras organizaciones sin ánimo de lucro para encontrar resúmenes criptográficos y otra información clave. Esto ayudará a identificar a los niños que están en riesgo y destacar reportes de alto valor. El prototipo ganador del 2018, nombrado "Spotting Trends" (tendencias de detección), hace uso de análisis en grupo e información que está relacionada con traficantes sexuales de niños para ayudar a asegurar que esos individuos no puedan resurgir en ningún otro lugar en Internet. Además, el éxito y la aplicación en el mundo real del prototipo que se llevó a casa el primer premio del 2016, un localizador de niños que compara fotos en línea con aquellas disponibles en la base de datos del NCMEC, confirma el beneficio de emplear tecnología para ayudar a afrontar estos asuntos desafiantes. La tecnología de esta índole tiene el potencial de reducir el tiempo de respuesta de las agencias policiales, llevando a los niños que pueden estar más vulnerables una ayuda más rápida y más eficiente.

Glosario

13



Glosario

AP — Agencia policial

CDN — Convención sobre los Derechos del Niño de la Organización de las Naciones Unidas

COPPA — Ley de Privacidad del Niño en Internet de los EE. UU.

Cyberbullying — bullying (acoso) que se lleva acabo a través de canales electrónicos, tales como servicios de mensajería de chat, redes sociales, correo electrónico y SMS

Deepfake (ultrafalso) — fotografía o simulación en video realista que luce como una persona real

EASN — Explotación y abuso sexual de niños

Grooming — proceso mediante el cual un adulto construye una relación con un menor para facilitar el contacto en línea o fuera de ella para propósitos que ocasionarán daño al menor (por ejemplo, radicalización o abuso sexual)

GT — Grupo de trabajo

IA — Inteligencia artificial

MAN — Material de abuso de niños

MASN — Material de abuso sexual de niños

ODS — Objetivos de Desarrollo Sostenible

OMS — Organización Mundial de la Salud

ONU — Organización de las Naciones Unidas

PIB — Producto Interno Bruto

Red oscura (darknet) — sitios web y servicios que están cifrados para prevenir que los usuarios o publicadores sean rastreados

Resumen criptográfico (hashing) — tecnología que crea una firma única para un archivo digital, empleado en la detección automatizada de MASN

UIT — Unión Internacional de Telecomunicaciones

UNICEF — United Nations Children's Fund (Fondo para la niñez de la ONU)

WPGA — WePROTECT Global Alliance

Referencias bibliográficas

14



Referencias bibliográficas

1. Datos de la UNICEF. (2019). The State of the World's Children 2017 Statistical Tables. [en línea] Disponible en: https://data.unicef.org/resources/state-worlds-children-2017-statistical-tables/ [ingresado agosto 5, 2019].

2. Loritz, M. (2019). UK-based Cyan Forensics partners with major US nonprofit to stop child sexual abuse | EU-Startups. [en línea] Eu-startups.com. Disponible en: https://www.eu-startups.com/2019/08/uk-based-cyan-forensics-partners-with-major-us-nonprofit-to-stop-child-sexual-abuse/ [Ingresado agosto 25, 2019].

3. Comparitech. (2019). Cyberbullying Statistics and Facts for 2016 - 2019 | Comparitech. [en línea] Disponible en: https://www.comparitech.com/internet-providers/cyberbullying-statistics/ [Ingresado agosto 8, 2019].

4. Dqinstitute.org. (2019). Outsmart Cyber-Pandemic. [en línea] Disponible en: https://www.dqinstitute.org/2018DQ_Impact_Report/ [Ingresado sep. 6 2019].

5. The Prevalence of Unwanted Online Sexual Exposure and Solicitation Among Youth: A Meta-Analysis, Madigan, Sheri et al. Journal of Adolescent Health, Volume 63, Issue 2, 133 – 141

6. Benoliel, Uri y Becher, Shmuel I., The Duty to Read the Unreadable (11 de enero, 2019). 60 Boston College Law Review, Forthcoming. Disponible en SSRN: https://ssrn.com/abstract=3313837 o http://dx.doi.org/10.2139/ssrn.3313837

7. Lu, J. (2019). Here's How Every Country Ranks When it Comes to Child Abuse and Child Safety | UN Dispatch. [en línea] UN Dispatch. Disponible en: https://www.undispatch.com/here-is-how-every-country-ranks-on-child-safety/ [Ingresado agosto 8, 2019].

8. Generation Unlimited: Business Plan for Digital Connectivity, UNICEF, 2019.

9. Itu.int. (2019). Comunicado de prensa. [en línea] Disponible en: https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx [Ingresado agosto 3, 2019].

10. Provider, S., Forecasts, V. and Papers, W. (2019). Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. [en línea] Cisco. Disponible en: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html [Ingresado agosto 3, 2019].

11. Katoa 'Utoikamanu, F. y Sanou, B. (2019). CTs, LDCs and the SDGs Achieving universal and affordable Internet in the least developed countries. [en línea] Unohrlls.org. Disponible en: http://unohrlls.org/custom-content/uploads/2018/01/D-LDC-ICTLDC-2018-PDF-E.pdf [Ingresado agosto 3, 2019].

12. Banco Mundial. (2019). Ganancias en la inclusión financiera, ganancias para un mundo sostenible. [en línea] Disponible en: https://www.worldbank.org/en/news/immersive-story/2018/05/18/gains-in-financial-inclusion-gains-for-a-sustainable-world [Ingresado agosto 3, 2019].

13. Uis.unesco.org. (2019). Sudan | UNESCO UIS. [en línea] Disponible en: http://uis.unesco.org/en/country/sd?theme=education-and-literacy [Ingresado agosto 3, 2019].

14. 5rightsfoundation.com. (2019). The Internet On Our Own Terms. [en línea] Disponible en: https://5rightsfoundation.com/static/Internet-On-Our-Own-Terms.pdf [Ingresado sept. 6, 2019].

15. Iwf.org.uk. (2019). Once Upon A Year: The Internet Watch Foundation Annual Report 2018. [en línea] Disponible en: https://www.iwf.org.uk/sites/default/files/reports/2019-04/Once%20upon%20a%20year%20-%20IWF%20Annual%20Report%202018.pdf [Ingresado agosto 5, 2019].

16. Reyes, I., Wijesekera, P., Reardon, J., Elazari Bar On, A., Razaghpanah, A., Vallina-Rodriguez, N. y Egelman, S. (2019). "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. [online] Petsymposium.org. Disponible en: https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf [Ingresado agosto 5, 2019].

17. Patchin, J. (2019). 2016 Cyberbullying Data - Cyberbullying Research Center. [en línea] Cyberbullying Research Center. Disponible en: https://cyberbullying.org/2019-cyberbullying-data [Ingresado agosto 5, 2019].

18. Atchoarena, D., Selwyn, N., Chakroun, B. y Fengchun, M. (2019). Working Group on Education: Digital skills for life and work - September 2017. [en línea] Unesdoc.unesco.org. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000259013 [Ingresado sept. 6, 2019].

19. Foro Económico Mundial. (2019). Cyber-risk exposure among 8-12-year olds drops by 15%. [en línea] Disponible en: https://www.weforum.org/our-impact/helping-young-people-safely-navigate-the-digital-world [Ingresado agosto 6, 2019].

20. Byrne, J. y Burton, P. (2019). Children as Internet users: how can evidence better inform policy debate? [en línea] Taylor y Francis. Disponible en: https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1291698?hootPostID=1753d7ca474ab7a748bcee5f22ffe65e [Ingresado agosto 7, 2019].

21. Mascheroni, G. y Ólafsson, K. (2019). Access and use, risksand opportunities of the internet for Italian children. [en línea] Globalkidsonline.net. Disponible en: http://globalkidsonline.net/wp-content/uploads/2017/10/Executive-summary-Italy-june-2018.pdf [Ingresado agosto 7, 2019].

22. Globalkidsonline.net. (2019). GLOBAL KIDS ONLINE SERBIA: Balancing between Opportunities and Risks: Results from the Pilot Study. [en línea] Disponible en: http://globalkidsonline.net/wp-content/uploads/2016/05/Country-report_Serbia-final-26-Oct-2016.pdf [Ingresado agosto 7, 2019].

23. 5rightsfoundation.com. (2019). Towards An Internet Safety Strategy. [online] Disponible en: https://5rightsfoundation.com/static/5rights_Towards_an_Internet_Safety_Strategy_FINAL.pdf [Ingresado sept. 6, 2019].

24. Ico.org.uk. (2019). Age appropriate design: a code of practice for online services. [online] Disponible en: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services [Ingresado sept. 6, 2019].

25. Office of the eSafety Commissioner. (2019). Safety by Design. [en línea] Disponible en: https://www.esafety.gov.au/esafety-information/safety-by-design [Ingresado sept. 6, 2019].

26. Courtland, R. (2019). Bias detectives: the researchers striving to make algorithms fair. [en línea] Nature.com. Disponible en: https://www.nature.com/articles/d41586-018-05469-3 [Ingresado agosto 8, 2019].

27. Andrew K. Przybylski and Victoria Nash. Cyberpsychology, Behavior, and Social Networking. Jul 2018. Publicado antes de su impresión. http://doi.org/10.1089/cyber. 2017.0466

28. Unicef.org. (2019). The State of The World's Children 2017: Children In A Digital World. [en línea] Disponible en: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf [Ingresado agosto 8, 2019].

29. Itu.int. (2019). ICT Facts and Figures 2017. [en línea] Disponible en: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx [Ingresado agosto 8, 2019].

30. Unicef.org. (2019). The State of The World's Children 2017: Children In A Digital World. [en línea] Disponible en: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf [Ingresado agosto 8, 2019].

31. Africanews. (2019). Digital in 2018: Africa's internet users increase by 20% | Africanews. [en línea] Disponible en: https://www.africanews.com/2018/02/06/digital-in-2018-africa-s-internet-users-increase-by-20-percent// [Ingresado agosto 8, 2019].

32. Quartz Africa. (2019). Gender inequality in tech starts with teenagers on their cellphones. [en línea] Disponible en: https://qz.com/africa/1420938/girls-have-less-access-to-mobile-phones-than-boys-study-shows/ [Ingresado agosto 25, 2019].

33. IWF. (2019). Exposing child victims: The catastrophic impact of DNS-over-HTTPs. [en línea] Disponible en: https://www.iwf.org.uk/news/exposing-child-victims-catastrophic-impact-of-dns-over-https [Ingresado sept. 7, 2019].

34. Fox News. (2019). Hany Farid: Facebook's plan for end-to-end encryption sacrifices a lot of security for just a little bit of privacy. [en línea] Disponible en: https://www.foxnews.com/opinion/hany-farid-facebook-end-to-end-encryption-security-privacy [Ingresado sept. 7, 2019].

35. Interpol.int. (2019). Base de datos internacional sobre explotación sexual de niños. [en línea] Disponible en: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database [Ingresado agosto 8, 2019].

36. Thorn (2019). The Intersection of Technology and Child Sexual Abuse | Thorn. [en línea] Disponible en: https://www.thorn.org/child-sexual-exploitation-and-technology/ [Ingresado agosto 8, 2019].

37. Puddephatt, A. and Hargreaves, S. (2019). 2018 Annual Report. [online] iwf.org.uk/. Disponible en: https://www.iwf.org.uk/report/2018-annual-report [Ingresado agosto 8, 2019].

38. protectchildren.ca. (2019). Recursos adicionales e investigación: International Survivors' Survey. [en línea] Disponible en: https://protectchildren.ca/en/resources-research/survivors-survey-results/ [Ingresado agostot 25, 2019].

39. Ecpat.org. (2019). Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material. [en línea] Disponible en: https://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf [Ingresado sept. 6, 2019].

40. NetClean.com. (2019). The NetClean Report 2018. [en línea] Disponible en: https://www.netclean.com/netclean-report-2018/ [Ingresado agosto 12, 2019].

41. Rachel Young & Melissa Tully (2019) 'Nobody wants the parents involved': Social norms in parent and adolescent responses to cyberbullying, Journal of Youth Studies, 22:6, 856-872, DOI: 10.1080/13676261.2018.1546838

42. Childnet.com. (2019). Young people's experiences of online sexual harassment: A cross-country report from Project Deshame. [en línea] Disponible en: https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf [Ingresado agosto 8, 2019].

43. Icmec.org. (2019). Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review. [en línea] Disponible en: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf [Ingresado agosto 8, 2019].

44. Teliacompany.com. (2019). CHILDREN AND ONLINE PRIVACY: FINDINGS FROM THE CHILDREN'S ADVISORY PANEL 2017/18. [en línea] Disponible en: https://www.teliacompany.com/globalassets/telia-company/documents/sustainability/children-and-online-privacy.pdf [Ingresado agosto 12, 2019].

45. Brumfield, B. (2019). 3 girls skipped school to sneak off and join ISIS - CNN. [online] CNN. Disponible en: https://edition.cnn.com/2014/10/22/us/colorado-teens-syria-odyssey/index.html [Ingresado agosto 8, 2019].

46. Martelozzo, E. (2019). A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, belief sand behaviours of children and young people. [en línea] Mdx.ac.uk. Disponible en: https://www.mdx.ac.uk/__data/assets/pdf_file/0021/223266/MDX-NSPCC-OCC-pornography-report.pdf [Ingresado agosto 9, 2019].

47. ITV News. (2019). Children report feeling unprotected from inappropriate content on social media sites. [en línea] Disponible en: https://www.itv.com/news/utv/2017-04-27/children-warn-social-media-sites-are-failing-to-shield-them-from-inappropriate-and-dangerous-content/ [Ingresado agosto 9, 2019].

48. Shieber, J. (2019). 2018 really was more of a dumpster fire for online hate and harassment, ADL study finds – TechCrunch. [en línea] TechCrunch. Disponible en: https://techcrunch.com/2019/02/13/2018-really-was-more-of-a-dumpster-fire-for-online-hate-and-harassment-adl-study-finds/ [Ingresado agosto 9, 2019].

49. Kardefelt-Winther, D. CHILD RIGHTS AND ONLINE GAMING: OPPORTUNITIES & CHALLENGES FOR CHILDREN AND THE INDUSTRY – ECPAT International. [Ingresado sept. 9, 2019].

50. Fitzpatrick, C. (2019). Watching violence on screens makes children more emotionally distressed. [en línea] The Conversation. Disponible en: https://theconversation.com/watching-violence-on-screens-makes-children-more-emotionally-distressed-106757 [Ingresada agosto 9, 2019].

51. Livingstone, S., Kirwil, L., Ponte, C. y Staksrud, E. (2019). In their own words: What bothers children online? [en línea] Lse.ac.uk. Disponible en: https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf [Ingresado agosto 9, 2019].

52. Calado, F., Alexandre, J. & Griffiths, M.D. J Gambl Stud (2017) 33: 397. https://doi.org/10.1007/s10899-016-9627-5

53. Valentine, G. (2019). Children and Young People's Gambling: Research Review: Report by Professor Gill Valentine for the Responsible Gambling Trust. [en línea] About.gambleaware.org. Disponible en: https://about.gambleaware.org/media/1274/1-june-update-children-young-people-literature-review.pdf [Ingresado agosto 9, 2019].

54. Karlsson, Anna & Hakansson, Anders. (2018). Gambling disorder, increased mortality, suicidality, and associated comorbidity: A longitudinal nationwide register study. Journal of Behavioral Addictions. 7. 1-9. 10.1556/2006.7.2018.112.

55. Howard, J. (2019). What's the age when kids start social media? [en línea] CNN. Disponible en: https://edition.cnn.com/2018/06/22/health/social-media-for-kids-parent-curve/index.html [Ingresado agosto 9, 2019].

56. BBC News. (2019). Under-age social media use 'on the rise'. [en línea] Disponible en: https://www.bbc.co.uk/news/technology-42153694 [Ingresado agosto 9, 2019].

57. Publications.parliament.uk. (2019). Impact of social media and screen-use on young people's health. [en línea] Disponible en: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/822/822.pdf [Ingresado agosto 9, 2019].

58. Sally Power, Chris Taylor & Kim Horton (2017) Sleepless in school? The social dimensions of young people's bedtime rest and routines, Journal of Youth Studies, 20:8, 945-958, DOI: 10.1080/13676261.2016.1273522

59. Cramer, S. e Inkster, B. (2019). #Status Of Mind: Social media and young people's mental health and wellbeing. [en línea] Rsph.org.uk. Disponible en: https://www.rsph.org.uk/uploads/assets/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf [Ingresado agosto 9, 2019].

60. Marisa Meyer, Victoria Adkins, Nalingna Yuan, Heidi M. Weeks, Yung-Ju Chang, Jenny Radesky. Advertising in Young Children's Apps. Journal of Developmental & Behavioral Pediatrics, 2018; 1 DOI: 10.1097/DBP.0000000000000622

61. Binns, Reuben & Lyngs, Ulrik & Van Kleek, Max & Zhao, Jun & Libert, Timothy & Shadbolt, Nigel. (2018). Third Party Tracking in the Mobile Ecosystem. 10.31235/osf.io/u7qmz.

62. Todorovic, N. y Chaudhuri, A. (2019). Using AI to help organizations detect and report child sexual abuse material online. [en línea] Google. Disponible en: https://www.blog.google/around-the-globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online/ [Ingresado agosto 10, 2019].

63. Richter, I. (2019). Automatische Bilderkennung hilft im Einsatz gegen Kinderpornografie | News Center Microsoft. [en línea] News Center Microsoft Deutschland. Disonible en: https://news.microsoft.com/de-de/ki-im-einsatz-gegen-kinderpornografie/ [Ingresado agosto 10, 2019].

64. Vleugels, A. (2019). AI-algorithms identify pedophiles for the police — here's how it works. [en línea] The Next Police | The Next Web. Disponible en: https://thenextweb.com/the-next-police/2018/11/08/ai-algorithms-identify-sexual-child-abuse-for-the-police/ [Ingresado agosto 10, 2019].

65. Griffeye. (2019). Griffeye releases new AI technology trained to aid child abuse investigations. [en línea] Disponible en: https://www.griffeye.com/griffeye-releases-new-ai-technology-press/ [Ingresado agosto 10, 2019].

66. Burgess, M. (2019). AI is helping UK police tackle child abuse way quicker than before. [en linea] Wired.co.uk. Disponible en: https://www.wired.co.uk/article/uk-police-child-abuse-images-ai [Ingresado agosto 10, 2019].

67. Griffeye. (2019). New AI technology trained to aid child abuse investigations. [en línea] Disponible en: https://www.griffeye.com/new-ai-technology-trained-to-aid-child-abuse-investigations/ [Ingresado sept. 6, 2019].

68. Ward, M. y Balian, S. (2019). Combating online radicalisation with expanded AI capabilities. [en línea] Faculty. Disponible en: https://faculty.ai/blog/combating-online-radicalisation-with-expanded-ai-capabilities/ [Ingresado agosto 10, 2019].

69. Boyce, J. (2019). Facebook touts use of artificial intelligence to fight child exploitation. [en línea] NBC News. Disponible en: https://www.nbcnews.com/tech/tech-news/facebook-touts-use-artificial-intelligence-fight-child-exploitation-n923906 [Ingresado agosto 10, 2019].

70. Publications.parliament.uk. (2019). Impact of social media and screen-use on young people's health: Government Response to the Committee's Fourteenth Report - Science and Technology Committee - House of Commons. [en línea] Disponible en: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/2120/212002.htm [Ingresado agosto 25, 2019].

71. https://www.marinusanalytics.com

72. ComputerWeekly.com. (2019). Thorn CEO on using machine learning and tech partnerships to tackle online child sex abuse. [en línea] Disponible en: https://www.computerweekly.com/news/450415609/Thorn-CEO-on-using-machine-learning-and-tech-partnerships-to-tackle-online-child-sex-abuse [Ingresado sept. 6, 2019].

73. Minton, L. (2019). What is human trafficking, and how can technology combat it? [en línea] ASU Now: Access, Excellence, Impact. Disponible en: https://asunow.asu.edu/20190313-what-human-trafficking-and-how-can-technology-combat-it [Ingresado agosto 10, 2019].

74. Phys.org. (2019). Instagram rolls out new features to counter bullying with AI. [en línea] Disponible en: https://phys.org/news/2019-07-instagram-features-counter-bullying-ai.html [Ingresado agosto 10, 2019].

75. http://creep-project.eu

76. Simonite, T., Simonite, T., Matsakis, L., Martineau, P., Tiku, N., Matsakis, L., Schwartz, O. y Martineau, P. (2019). How Facial Recognition Is Fighting Child Sex Trafficking. [en línea] WIRED. Disponible en: https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/ [Ingresado agosto 25, 2019].

77. Eandt.theiet.org. (2019). Child abuse targeted with upgraded police tech, limiting officer exposure to images. [en línea] Disponible en: https://eandt.theiet.org/content/articles/2019/07/child-abuse-targeted-with-upgraded-police-tech-limiting-officer-exposure-to-indecent-images/ [Ingresado agosto 25, 2019].

78. McIntyre, N. y Pegg, D. (2019). Councils use 377,000 people's data in efforts to predict child abuse. [en línea] the Guardian. Disponible en: https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse [Ingresado agosto 25, 2019].

79. Europol. (2019). Global action tackles distribution of child sexual exploitation images via WhatsApp: 39 arrested so far. [en línea] Available at: https://www.europol.europa.eu/newsroom/news/global-action-tackles-distribution-of-child-sexual-exploitation-images-whatsapp-39-arrested-so-far [Ingresado agosto 25, 2019].

80. (www.dw.com), D. (2019). Interpol busts international pedophilia ring | DW | 23.05.2019. [en línea] DW.COM. Disponible en: https://www.dw.com/en/interpol-busts-international-pedophilia-ring/a-48841717 [Ingresado agosto 25, 2019].

81. Estadísticas provistas por INHOPE

82. Niels Nagelhus Schia (2018) The cyber frontier and digital pitfalls in the Global South, Third World Quarterly, 39:5, 821-837, DOI: 10.1080/01436597.2017.1408403}

83. Out of the Shadows. (2019). Out the Shadows - Shining light on the response to child sexual abuse and exploitation. [en línea] Disponible en: https://outoftheshadows.eiu.com [Ingresado agosto 25, 2019].

84. Childrenandbusiness.org. (2019). Children's Rights and Business Principles. [en línea] Disponible en: http://childrenandbusiness.org/ [Ingresado agosto 25, 2019].

85. Unctad.org. (2019). UNCTAD | Cybercrime Legislation Worldwide. [en línea] Disponible en: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx [Ingresado agosto 11, 2019].

86. Unicef.org. (2019). COP Guidelines for Industry. [en línea] Disponible en: https://www.unicef.org/csr/COPguidelines.htm [Ingresado sept. 7, 2019].

87. Out of the Shadows. (2019). Out the Shadows - Shining light on the response to child sexual abuse and exploitation. [en línea] Disponible en: https://outoftheshadows.eiu.com [Ingresado agosto 25, 2019].

88. Publicsafety.gc.ca. (2019). Child Pornography Offenders: A Review. [en línea] Disponible en: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2018-s001/index-en.aspx [Ingresad agosto 25, 2019].

89. Thorn.org. (2019). Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims. [en línea] Disponible en: https://www.thorn.org/wp-content/uploads/2018/03/Production-and-Active-Trading-of-CSAM_FullReport_FINAL.pdf [Ingresada agosto 13, 2019].

90. NetClean.com. (2019). The NetClean Report 2017 - There is no such thing as a typical offender (The consumer of child sexual abuse material). [en línea] Disponible en: https://www.netclean.com/netclean-report-2017/insight-3/ [Ingresado agosto 25, 2019].

91. Stop It Now (2006) Let's talk: speaking up to prevent child sexual abuse. [en línea] Disponible en: https://www.stopitnow.org/sites/default/files/documents/files/lets_talk.pdf

92. Stone, J. y Stone, J. (2019). The dark web isn't as big as you think. [en línea] CyberScoop. Disponible en: https://www.cyberscoop.com/dark-web-marketplaces-research-recorded-future/ [Ingresado agosto 25, 2019].

93. Ecpat.org. (2019). Emerging Global Threats Related To The Online Sexual Exploitation Of Children. [en línea] Disponible en: https://www.ecpat.org/wp-content/uploads/2018/08/Briefing-Paper-Emerging-Issues-and-Global-Threats-Children-online-_06.06.17.pdf [Ingresado agosto 10, 2019].

94. Stop It Now. (2019). Understanding What Makes Kids Vulnerable to Being Sexually Abused. [en línea] Disponible en: https://www.stopitnow.org/ohc-content/understanding-what-makes-kids-vulnerable-to-being-sexually-abused [Ingresado agosto 11, 2019].

95. Nice.org.uk. (2019). NICE Guideline NG76: Child abuse and neglect: recognising, assessing and responding to abuse and neglect of children and young people. [en línea] Disponible en: https://www.nice.org.uk/guidance/ng76/evidence/full-guideline-pdf-4607478261 [Ingresado agosto 25, 2019].

96. Who.int. (2019). Child abuse and neglectby parents and other caregivers. [en línea] Disponible en: https://www.who.int/violence_injury_prevention/violence/global_campaign/en/chap3.pdf [Ingresado agosto 25, 2019].

97. Unicef.org. (2019). 'Shame and pain': Vietnam starts to grapple with child abuse epidemic. [en línea] Disponible en: https://www.unicef.org/vietnam/stories/shame-and-pain-vietnam-starts-grapple-child-abuse-epidemic [Ingresado agosto 11, 2019].

98. BBC News. (2019). Instagram 'biggest for child grooming online'. [en línea] Disponible en: https://www.bbc.co.uk/news/uk-47410520 [Ingresado agosto 12, 2019].

99. The Conversation. (2019). YouTube's paedophile problem is only a small part of the internet's issue with child sexual abuse. [en línea] Disponible en: https://theconversation.com/youtubes-paedophile-problem-is-only-a-small-part-of-the-internets-issue-with-child-sexual-abuse-94126 [Ingresado agosto 12, 2019].

100. Ditchthelabel.org. (2019). Anti-Bullying Survey 2017. [en línea] Disponible en: https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf [Ingresado agosto 12, 2019].

101. Economicgraph.linkedin.com. (2019). LinkedIn Workforce Report | United States | August 2018. [en línea] Disponible en: https://economicgraph.linkedin.com/resources/linkedin-workforce-report-august-2018 [Ingresado agosto 25, 2019].

102. Digital Single Market - European Commission. (2019). Final results of the European Data Market study measuring the size and trends of the EU data economy - Digital Single Market - European Commission. [en línea] Disponible en: https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy [Ingresado agosto 25, 2019].

103. Anon, (2019). Data Science and Analytics Skills Shortage: Equipping the APEC Workforce with the Competencies Demanded by Employers. [en línea] Disponible en: https://www.apec.org/Publications/2017/11/Data-Science-and-Analytics-Skills-Shortage [Ingresado agosto 25, 2019].

104. Thorn (2019). Sound Practices Guide to Stopping Child Sexual Abuse | Thorn. [en línea] Disponible en: https://www.thorn.org/sound-practices-guide-stopping-child-abuse/ [Ingresado sept. 7, 2019].

105. NetClean.com. (2019). Benchmarking Index on the response to child sexual abuse and exploitation. [en línea] Disponible en: https://www.netclean.com/2019/01/11/benchmarking-index-response-to-child-sexual-abuse-and-exploitation/ [Ingresado setp. 7, 2019].

106. Legislation.gov.uk. (2019). Data Protection Act 2018. [en línea] Disponible en: http://www.legislation.gov.uk/ukpga/2018/12/section/123/enacted [Ingresado sept. 7, 2019].

107. INHOPE Annual Report 2017: http://88.208.218.79/libraries/annual_reports/inhope_annual_report_2017.sflb.ashx\

Materiales adicionales

15



Materiales adicionales

Contigo Conectados Online Safety Resources
https://contigoconectados.com/resultados/riesgos/

Economist Intelligence Unit: Out of the Shadows
https://outoftheshadows.eiu.com/

End Violence Against Children: Keeping Children Safe Online
https://www.end-violence.org/keeping-children-safe-online

Facebook: Photo Video Matching
https://newsroom.fb.com/news/2019/08/open-source-photo-video-matching/

Facebook: New technology to fight child exploitation
https://newsroom.fb.com/news/2018/10/fighting-child-exploitation/

Griffeye
https://www.griffeye.com/

GSMA European Framework for Safer Mobile Use by Younger Teenagers and Children
https://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/myouth

IMEC Child Sexual Abuse Material: Model Legislation & Global Review
https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf

Inhope Global Internet Hotlines
http://www.inhope.org

ITU Guidelines for Policy Makers on Child Protection
https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf

Luxembourg Terminology Guidelines for The Protection of Children from Sexual Exploitation and Sexual Abuse
http://luxembourgguidelines.org/english-version/

Microsoft Digital Skills
https://www.microsoft.com/en-us/digital-skills/online-safety

Microsoft Online Safety Resources
https://www.microsoft.com/en-us/digital-skills/online-safety-resources

Microsoft PhotoDNA
https://www.microsoft.com/en-us/photodna

NetClean
https://www.netclean.com/

OECD: The Future of Education and Skills
https://www.oecd.org/education/2030/E2030%20Position%20Paper%20(05.04.2018).pdf

The #ENDviolence Youth Manifesto
https://www.unicef.org/end-violence/youth-manifesto

Thorn
https://www.thorn.org

UK Online Harms White Paper
https://www.gov.uk/government/consultations/online-harms-white-paper

UN Convention on the Rights of the Child
https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

UNICEF & GSMA: NOTICE AND TAKEDOWN — Company policies and practices to remove online child sexual abuse material
https://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/notice_and_takedown_gsma_unicef_april_2016.pdf

WeProtect Model National Response Guidance Document
https://www.weprotect.org/the-model-national-response

The ITU Global Cybersecurity Index.
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

NOTAS

NOTAS

NOTAS

BROADBAND COMMISSION
FOR SUSTAINABLE DEVELOPMENT